

# Enterasys® B5

Stackable Switches

---

## CLI Reference

Firmware Version 6.42.xx.xxxx or Higher



## Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.  
50 Minuteman Road  
Andover, MA 01810

© 2011 Enterasys Networks, Inc. All rights reserved.

Part Number: 9034525-02 January 2011

ENTERASYS, ENTERASYS NETWORKS, ENTERASYS SECURE NETWORKS, ENTERASYS NETSIGHT, WEBVIEW, and any logos associated therewith, are trademarks or registered trademarks of Enterasys Networks, Inc. in the United States and other countries. For a complete list of Enterasys trademarks, see <http://www.enterasys.com/company/trademarks.aspx>.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

**Documentation URL:** <https://extranet.enterasys.com/downloads/>

<b>Version:</b> Information in this guide refers to Enterasys B5 firmware version 6.42.xx.xxxx or higher.
---

# Enterasys Networks, Inc. Firmware License Agreement

## BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement (“Agreement”) between the end user (“You”) and Enterasys Networks, Inc., on behalf of itself and its Affiliates (as hereinafter defined) (“Enterasys”) that sets forth Your rights and obligations with respect to the Enterasys software program/firmware (including any accompanying documentation, hardware or media) (“Program”) in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. “Affiliate” means any person, partnership, corporation, limited liability company, other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. This Agreement constitutes the entire understanding between the parties, with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, “YOU” AND “YOUR” SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, LEGAL DEPARTMENT AT (978) 684-1000.

### You and Enterasys agree as follows:

1. **LICENSE.** You have the non-exclusive and non-transferable right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.
2. **RESTRICTIONS.** Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:
  - (a) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and upon payment of Enterasys’ applicable fee.
  - (b) Incorporate the Program in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.
  - (c) Publish, disclose, copy reproduce or transmit the Program, in whole or in part.
  - (d) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part.
  - (e) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.
3. **APPLICABLE LAW.** This Agreement shall be interpreted and governed under the laws and in the state and federal courts of the Commonwealth of Massachusetts without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the Commonwealth of Massachusetts courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.
4. **EXPORT RESTRICTIONS.** You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Section 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Cambodia, Cuba, Georgia, Iraq, Kazakhstan, Laos, Libya, Macau, Moldova, Mongolia, North Korea, the People's Republic of China, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

**5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

**6. DISCLAIMER OF WARRANTY.** EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED TO YOU IN WRITING BY ENTERASYS, ENTERASYS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.

**7. LIMITATION OF LIABILITY.** IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

**8. AUDIT RIGHTS.** You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys, and, accordingly, You hereby agree to maintain complete books, records and accounts showing (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such audit discovers non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly pay to Enterasys the appropriate license fees. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

**9. OWNERSHIP.** This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its suppliers. All rights not specifically granted to You shall be reserved to Enterasys.

**10. ENFORCEMENT.** You acknowledge and agree that any breach of Sections 2, 4, or 9 of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.

**11. ASSIGNMENT.** You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except that You may assign this Agreement to any person or entity which acquires substantially all of Your stock assets. Enterasys may assign this Agreement in its sole discretion. This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors and assigns as permitted by this Agreement. Any attempted assignment, transfer or sublicense in violation of the terms of this Agreement shall be void and a breach of this Agreement.

**12. WAIVER.** A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.

**13. SEVERABILITY.** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality, or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.

**14. TERMINATION.** Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

---

# Contents

## About This Guide

Using This Guide .....	xxix
Structure of This Guide .....	xxix
Related Documents .....	xxx
Conventions Used in This Guide .....	xxxi
Getting Help .....	xxxii

## Chapter 1: Introduction

Enterasys B5 CLI Overview .....	1-1
Switch Management Methods .....	1-1
Factory Default Settings .....	1-2
Using the Command Line Interface .....	1-6
Starting a CLI Session .....	1-6
Logging In .....	1-7
Navigating the Command Line Interface .....	1-8

## Chapter 2: Configuring Switches in a Stack

About Enterasys B5 Switch Operation in a Stack .....	2-1
Installing a New Stackable System of Up to Eight Units .....	2-2
Installing Previously-Configured Systems in a Stack .....	2-3
Adding a New Unit to an Existing Stack .....	2-3
Creating a Virtual Switch Configuration .....	2-3
Considerations About Using Clear Config in a Stack .....	2-4
Stacking Configuration and Management Commands .....	2-5
Purpose .....	2-5
Commands .....	2-5
show switch .....	2-5
show switch switchtype .....	2-6
show switch stack-ports.....	2-7
set switch.....	2-8
set switch copy-fw .....	2-9
set switch description .....	2-9
set switch movemanagement.....	2-10
set switch member.....	2-10
clear switch member.....	2-11

## Chapter 3: Basic Configuration

Quick Start Setup Commands .....	3-1
Setting User Accounts and Passwords .....	3-2
Purpose .....	3-2
Commands .....	3-2
show system login .....	3-3
set system login.....	3-4
clear system login.....	3-4
set password .....	3-5
set system password length .....	3-6
set system password aging .....	3-6
set system password history .....	3-7
show system lockout .....	3-7
set system lockout.....	3-8

Setting Basic Switch Properties .....	3-9
Purpose .....	3-9
Commands .....	3-9
show ip address.....	3-10
set ip address .....	3-10
clear ip address .....	3-11
show ip protocol.....	3-12
set ip protocol .....	3-12
show ip route .....	3-13
show system.....	3-13
show system hardware.....	3-15
show system utilization.....	3-16
set system utilization .....	3-17
clear system utilization .....	3-17
set system temperature .....	3-18
clear system temperature .....	3-19
show time .....	3-20
set time .....	3-20
show summertime .....	3-21
set summertime .....	3-21
set summertime date .....	3-22
set summertime recurring.....	3-22
clear summertime .....	3-23
set prompt.....	3-24
show banner motd .....	3-24
set banner motd.....	3-25
clear banner motd.....	3-25
show version.....	3-26
set system name .....	3-27
set system location .....	3-27
set system contact.....	3-28
set width .....	3-28
set length .....	3-29
show logout .....	3-29
set logout .....	3-30
show console.....	3-30
set console baud .....	3-31
Downloading a Firmware Image .....	3-31
Downloading from a TFTP Server .....	3-32
Downloading via the Serial Port .....	3-32
Reverting to a Previous Image .....	3-33
Reviewing and Selecting a Boot Firmware Image .....	3-34
Purpose .....	3-34
Commands .....	3-34
show boot system.....	3-34
set boot system .....	3-35
Starting and Configuring Telnet .....	3-36
Purpose .....	3-36
Commands .....	3-36
show telnet .....	3-36
set telnet.....	3-37
telnet.....	3-37
Managing Switch Configuration and Files .....	3-38
Configuration Persistence Mode .....	3-38
Purpose .....	3-38
Commands .....	3-38



show snmp persistmode.....	3-39
set snmp persistmode .....	3-40
save config .....	3-40
dir.....	3-41
show file.....	3-42
show config.....	3-43
configure.....	3-44
copy .....	3-44
delete.....	3-45
show tftp settings.....	3-45
set tftp timeout .....	3-46
clear tftp timeout .....	3-47
set tftp retry.....	3-47
clear tftp retry.....	3-48
Clearing and Closing the CLI .....	3-48
Purpose .....	3-48
Commands .....	3-48
cls (clear screen) .....	3-48
exit .....	3-49
Resetting the Switch .....	3-49
Purpose .....	3-49
Commands .....	3-49
reset.....	3-50
clear config .....	3-50
Using and Configuring WebView .....	3-51
Purpose .....	3-51
Commands .....	3-51
show webview .....	3-52
set webview .....	3-52
show ssl.....	3-53
set ssl .....	3-53
Gathering Technical Support Information .....	3-54
Purpose .....	3-54
Command .....	3-54
show support.....	3-54

## Chapter 4: Configuring System Power and PoE

Power Management .....	4-1
Management of PoE Power to PDs .....	4-1
Commands .....	4-2
show inlinepower .....	4-2
set inlinepower threshold.....	4-3
set inlinepower trap .....	4-4
set inlinepower detectionmode .....	4-4
show port inlinepower.....	4-5
set port inlinepower .....	4-6
set inlinepower management.....	4-7

## Chapter 5: Transmit Queue Monitoring Configuration

Transmit Queue Monitoring Overview .....	5-1
Commands .....	5-1
set txqmonitor .....	5-2
set txqmonitor downtime.....	5-2
set txqmonitor minrate .....	5-3
set txqmonitor threshold .....	5-3

clear txqmonitor .....	5-4
show txqmonitor .....	5-5
show txqmonitor flowcontrol .....	5-6
show txqmonitor port .....	5-6

## Chapter 6: Discovery Protocol Configuration

Configuring CDP .....	6-1
Purpose .....	6-1
Commands .....	6-1
show cdp .....	6-2
set cdp state .....	6-3
set cdp auth .....	6-4
set cdp interval .....	6-4
set cdp hold-time .....	6-5
clear cdp .....	6-5
show neighbors .....	6-6
Configuring Cisco Discovery Protocol .....	6-7
Purpose .....	6-7
Commands .....	6-7
show ciscodep .....	6-7
show ciscodep port info .....	6-8
set ciscodep status .....	6-9
set ciscodep timer .....	6-9
set ciscodep holdtime .....	6-10
set ciscodep port .....	6-10
clear ciscodep .....	6-12
Configuring Link Layer Discovery Protocol and LLDP-MED .....	6-13
Overview .....	6-13
Configuration Tasks .....	6-13
Commands .....	6-14
show lldp .....	6-15
show lldp port status .....	6-15
show lldp port trap .....	6-16
show lldp port tx-tlv .....	6-17
show lldp port location-info .....	6-17
show lldp port local-info .....	6-18
show lldp port remote-info .....	6-21
show lldp port network-policy .....	6-22
set lldp tx-interval .....	6-23
set lldp hold-multiplier .....	6-24
set lldp trap-interval .....	6-24
set lldp med-fast-repeat .....	6-25
set lldp port status .....	6-25
set lldp port trap .....	6-26
set lldp port med-trap .....	6-26
set lldp port location-info .....	6-27
set lldp port tx-tlv .....	6-28
set lldp port network-policy .....	6-29
clear lldp .....	6-31
clear lldp port status .....	6-31
clear lldp port trap .....	6-32
clear lldp port med-trap .....	6-32
clear lldp port location-info .....	6-33
clear lldp port network-policy .....	6-33
clear lldp port tx-tlv .....	6-34

## Chapter 7: Port Configuration

Port Configuration Summary .....	7-1
Port String Syntax Used in the CLI .....	7-1
Reviewing Port Status .....	7-2
Purpose .....	7-2
Commands .....	7-2
show port .....	7-3
show port status .....	7-3
show port counters .....	7-4
clear port counters .....	7-6
show port cablestatus .....	7-6
Disabling / Enabling and Naming Ports .....	7-7
Purpose .....	7-7
Commands .....	7-7
set port disable .....	7-8
set port enable .....	7-8
show port alias .....	7-9
set port alias .....	7-9
Setting Speed and Duplex Mode .....	7-11
Purpose .....	7-11
Commands .....	7-11
show port speed .....	7-11
set port speed .....	7-12
show port duplex .....	7-12
set port duplex .....	7-13
Enabling / Disabling Jumbo Frame Support .....	7-14
Purpose .....	7-14
Commands .....	7-14
show port jumbo .....	7-14
set port jumbo .....	7-15
clear port jumbo .....	7-15
Setting Auto-Negotiation and Advertised Ability .....	7-16
Purpose .....	7-16
Commands .....	7-16
show port negotiation .....	7-16
set port negotiation .....	7-17
show port advertise .....	7-17
set port advertise .....	7-18
clear port advertise .....	7-19
show port mdix .....	7-20
set port mdix .....	7-20
Setting Flow Control .....	7-22
Purpose .....	7-22
Commands .....	7-22
show flowcontrol .....	7-22
set flowcontrol .....	7-22
Setting Port Link Traps and Link Flap Detection .....	7-24
Purpose .....	7-24
Commands .....	7-24
show port trap .....	7-24
set port trap .....	7-25
show linkflap .....	7-25
set linkflap globalstate .....	7-28
set linkflap portstate .....	7-28
set linkflap interval .....	7-29

set linkflap action .....	7-29
clear linkflap action .....	7-30
set linkflap threshold .....	7-30
set linkflap downtime .....	7-31
clear linkflap down .....	7-31
clear linkflap .....	7-32
show newaddrtrap .....	7-33
set newaddrtrap .....	7-33
Configuring Broadcast Suppression .....	7-35
Purpose .....	7-35
Commands .....	7-35
show port broadcast .....	7-35
set port broadcast .....	7-36
clear port broadcast .....	7-36
Port Mirroring .....	7-38
Mirroring Features .....	7-38
Remote Port Mirroring .....	7-38
Configuring SMON MIB Port Mirroring .....	7-39
Purpose .....	7-40
Commands .....	7-40
show port mirroring .....	7-40
set port mirroring .....	7-41
clear port mirroring .....	7-42
set mirror vlan .....	7-42
clear mirror vlan .....	7-43
Link Aggregation Control Protocol (LACP) .....	7-44
LACP Operation .....	7-44
LACP Terminology .....	7-45
Enterasys B5 Usage Considerations .....	7-45
Commands .....	7-46
show lacp .....	7-47
set lacp .....	7-48
set lacp asypri .....	7-49
set lacp aadminkey .....	7-49
clear lacp .....	7-50
set lacp static .....	7-50
clear lacp static .....	7-51
set lacp singleportlag .....	7-52
clear lacp singleportlag .....	7-52
show port lacp .....	7-53
set port lacp .....	7-54
clear port lacp .....	7-56
Configuring Protected Ports .....	7-58
Protected Port Operation .....	7-58
Commands .....	7-58
set port protected .....	7-58
show port protected .....	7-59
clear port protected .....	7-59
set port protected name .....	7-60
show port protected name .....	7-60
clear port protected name .....	7-61

## Chapter 8: SNMP Configuration

SNMP Configuration Summary .....	8-1
SNMPv1 and SNMPv2c .....	8-2

SNMPv3 .....	8-2
About SNMP Security Models and Levels .....	8-2
Using SNMP Contexts to Access Specific MIBs .....	8-3
Configuration Considerations .....	8-3
Reviewing SNMP Statistics .....	8-3
Purpose .....	8-3
Commands .....	8-4
show snmp engineid .....	8-4
show snmp counters .....	8-5
Configuring SNMP Users, Groups, and Communities .....	8-8
Purpose .....	8-8
Commands .....	8-8
show snmp user .....	8-8
set snmp user .....	8-9
clear snmp user .....	8-11
show snmp group .....	8-11
set snmp group .....	8-12
clear snmp group .....	8-13
show snmp community .....	8-13
set snmp community .....	8-14
clear snmp community .....	8-15
Configuring SNMP Access Rights .....	8-15
Purpose .....	8-15
Commands .....	8-16
show snmp access .....	8-16
set snmp access .....	8-18
clear snmp access .....	8-19
Configuring SNMP MIB Views .....	8-19
Purpose .....	8-19
Commands .....	8-19
show snmp view .....	8-20
show snmp context .....	8-21
set snmp view .....	8-21
clear snmp view .....	8-22
Configuring SNMP Target Parameters .....	8-23
Purpose .....	8-23
Commands .....	8-23
show snmp targetparams .....	8-23
set snmp targetparams .....	8-24
clear snmp targetparams .....	8-25
Configuring SNMP Target Addresses .....	8-26
Purpose .....	8-26
Commands .....	8-26
show snmp targetaddr .....	8-26
set snmp targetaddr .....	8-27
clear snmp targetaddr .....	8-28
Configuring SNMP Notification Parameters .....	8-29
About SNMP Notify Filters .....	8-29
Purpose .....	8-29
Commands .....	8-29
show snmp notify .....	8-30
set snmp notify .....	8-31
clear snmp notify .....	8-31
show snmp notifyfilter .....	8-32
set snmp notifyfilter .....	8-33
clear snmp notifyfilter .....	8-33

show snmp notifyprofile .....	8-34
set snmp notifyprofile.....	8-35
clear snmp notifyprofile.....	8-35
Creating a Basic SNMP Trap Configuration .....	8-36
Example .....	8-37
Configuring the SNMP Management Interface .....	8-38
Purpose .....	8-38
Commands .....	8-38
show snmp interface.....	8-38
set snmp interface .....	8-38
clear snmp interface .....	8-40

## Chapter 9: Spanning Tree Configuration

Spanning Tree Configuration Summary .....	9-1
Overview: Single, Rapid, and Multiple Spanning Tree Protocols .....	9-1
Spanning Tree Features .....	9-2
Loop Protect .....	9-2
Configuring Spanning Tree Bridge Parameters .....	9-3
Purpose .....	9-3
Commands .....	9-4
show spantree stats.....	9-5
set spantree .....	9-7
show spantree version.....	9-7
set spantree version .....	9-8
clear spantree version .....	9-9
show spantree bpdu-forwarding .....	9-9
set spantree bpdu-forwarding.....	9-10
show spantree bridgeprioritymode .....	9-10
set spantree bridgeprioritymode .....	9-11
clear spantree bridgeprioritymode .....	9-11
show spantree mstlist .....	9-12
set spantree msti .....	9-12
clear spantree msti .....	9-13
show spantree mstmap .....	9-13
set spantree mstmap .....	9-14
clear spantree mstmap .....	9-14
show spantree vlanlist .....	9-15
show spantree mstcfgid.....	9-15
set spantree mstcfgid .....	9-16
clear spantree mstcfgid .....	9-16
set spantree priority .....	9-17
clear spantree priority .....	9-17
set spantree hello .....	9-18
clear spantree hello .....	9-18
set spantree maxage .....	9-19
clear spantree maxage .....	9-20
set spantree fwddelay.....	9-20
clear spantree fwddelay.....	9-21
show spantree backuproot .....	9-21
set spantree backuproot.....	9-22
clear spantree backuproot .....	9-22
show spantree tctrapsuppress.....	9-23
set spantree tctrapsuppress .....	9-23
clear spantree tctrapsuppress .....	9-24
set spantree protomigration .....	9-24

show spantree spanguard	9-25
set spantree spanguard	9-25
clear spantree spanguard	9-26
show spantree spanguardtimeout	9-27
set spantree spanguardtimeout	9-27
clear spantree spanguardtimeout	9-28
show spantree spanguardlock	9-28
clear / set spantree spanguardlock	9-29
show spantree spanguardtrapeivable	9-29
set spantree spanguardtrapeivable	9-30
clear spantree spanguardtrapeivable	9-30
show spantree legacypathcost	9-31
set spantree legacypathcost	9-31
clear spantree legacypathcost	9-32
show spantree autoedge	9-32
set spantree autoedge	9-32
clear spantree autoedge	9-33
Configuring Spanning Tree Port Parameters	9-34
Purpose	9-34
Commands	9-34
set spantree portadmin	9-34
clear spantree portadmin	9-35
show spantree portadmin	9-35
show spantree portpri	9-36
set spantree portpri	9-36
clear spantree portpri	9-37
show spantree adminpathcost	9-38
set spantree adminpathcost	9-38
clear spantree adminpathcost	9-39
show spantree adminedge	9-39
set spantree adminedge	9-40
clear spantree adminedge	9-40
show spantree operedge	9-41
Configuring Spanning Tree Loop Protect Parameters	9-42
Purpose	9-42
Commands	9-42
set spantree lp	9-43
show spantree lp	9-43
clear spantree lp	9-44
show spantree lpbloc	9-44
clear spantree lpbloc	9-45
set spantree lpcapablepartner	9-46
show spantree lpcapablepartner	9-46
clear spantree lpcapablepartner	9-47
set spantree lpthreshold	9-47
show spantree lpthreshold	9-48
clear spantree lpthreshold	9-48
set spantree lpwindow	9-49
show spantree lpwindow	9-49
clear spantree lpwindow	9-50
set spantree lptrapeivable	9-50
show spantree lptrapeivable	9-51
clear spantree lptrapeivable	9-51
set spantree disputedbpduthreshold	9-52
show spantree disputedbpduthreshold	9-53
clear spantree disputedbpduthreshold	9-53

show spantree nonforwardingreason .....	9-54
---	------

## Chapter 10: 802.1Q VLAN Configuration

VLAN Configuration Summary .....	10-1
Port String Syntax Used in the CLI .....	10-1
Creating a Secure Management VLAN .....	10-2
Viewing VLANs .....	10-3
Purpose .....	10-3
Command .....	10-3
show vlan .....	10-3
Creating and Naming Static VLANs .....	10-5
Purpose .....	10-5
Commands .....	10-5
set vlan .....	10-5
set vlan name .....	10-6
clear vlan .....	10-6
clear vlan name .....	10-7
Assigning Port VLAN IDs (PVIDs) and Ingress Filtering .....	10-8
Purpose .....	10-8
Commands .....	10-8
show port vlan .....	10-8
set port vlan .....	10-9
clear port vlan .....	10-9
show port ingress-filter .....	10-10
set port ingress-filter .....	10-11
show port discard .....	10-11
set port discard .....	10-12
Configuring the VLAN Egress List .....	10-13
Purpose .....	10-13
Commands .....	10-13
show port egress .....	10-13
set vlan forbidden .....	10-14
set vlan egress .....	10-15
clear vlan egress .....	10-15
show vlan dynamic egress .....	10-16
set vlan dynamic egress .....	10-17
Setting the Host VLAN .....	10-18
Purpose .....	10-18
Commands .....	10-18
show host vlan .....	10-18
set host vlan .....	10-18
clear host vlan .....	10-19
Enabling/Disabling GVRP (GARP VLAN Registration Protocol) .....	10-20
About GARP VLAN Registration Protocol (GVRP) .....	10-20
Purpose .....	10-21
Commands .....	10-21
show gvrp .....	10-22
show garp timer .....	10-22
set gvrp .....	10-23
clear gvrp .....	10-24
set garp timer .....	10-25
clear garp timer .....	10-25



## Chapter 11: Policy Classification Configuration

Policy Classification Configuration Summary .....	11-1
Configuring Policy Profiles .....	11-2
Purpose .....	11-2
Commands .....	11-2
show policy profile .....	11-2
set policy profile .....	11-4
clear policy profile .....	11-5
Configuring Classification Rules .....	11-6
Purpose .....	11-6
Commands .....	11-6
show policy rule .....	11-6
show policy capability .....	11-8
set policy rule .....	11-10
clear policy rule .....	11-12
clear policy all-rules .....	11-13
Assigning Ports to Policy Profiles .....	11-14
Purpose .....	11-14
Commands .....	11-14
set policy port .....	11-14
clear policy port .....	11-15
Configuring Policy Class of Service (CoS) .....	11-16
About Policy-Based CoS Configurations .....	11-16
About CoS-Based Flood Control .....	11-18
Commands .....	11-19
set cos state .....	11-19
show cos state .....	11-20
clear cos state .....	11-20
set cos settings .....	11-21
clear cos settings .....	11-22
show cos settings .....	11-22
set cos port-config .....	11-23
show cos port-config .....	11-24
clear cos port-config .....	11-25
set cos port-resource irl .....	11-26
set cos port-resource flood-ctrl .....	11-27
show cos port-resource .....	11-28
clear cos port-resource irl .....	11-29
clear cos port-resource flood-ctrl .....	11-30
set cos reference .....	11-30
show cos reference .....	11-31
clear cos reference .....	11-32
show cos unit .....	11-33
clear cos all-entries .....	11-33
show cos port-type .....	11-34

## Chapter 12: Port Priority Configuration

Port Priority Configuration Summary .....	12-1
Configuring Port Priority .....	12-2
Purpose .....	12-2
Commands .....	12-2
show port priority .....	12-2
set port priority .....	12-3
clear port priority .....	12-3

Configuring Priority to Transmit Queue Mapping .....	12-4
Purpose .....	12-4
Commands .....	12-4
show port priority-queue .....	12-4
set port priority-queue .....	12-5
clear port priority-queue .....	12-6
Configuring Quality of Service (QoS) .....	12-7
Purpose .....	12-7
Commands .....	12-7
show port txq .....	12-7
set port txq .....	12-8
clear port txq .....	12-8

## Chapter 13: IGMP Configuration

IGMP Overview .....	13-1
About IP Multicast Group Management .....	13-1
About Multicasting .....	13-2
Configuring IGMP at Layer 2 .....	13-2
Purpose .....	13-2
Commands .....	13-2
show igmpsnooping .....	13-3
set igmpsnooping adminmode .....	13-3
set igmpsnooping interfacemode .....	13-4
set igmpsnooping groupmembershipinterval .....	13-4
set igmpsnooping maxresponse .....	13-5
set igmpsnooping mcrtrexpiretime .....	13-6
set igmpsnooping add-static .....	13-6
set igmpsnooping remove-static .....	13-7
show igmpsnooping static .....	13-7
show igmpsnooping mfdb .....	13-8
clear igmpsnooping .....	13-9
Configuring IGMP on Routing Interfaces .....	13-10
Purpose .....	13-10
Commands .....	13-10
ip igmp .....	13-10
ip igmp enable .....	13-11
ip igmp version .....	13-11
show ip igmp interface .....	13-12
show ip igmp groups .....	13-13
ip igmp query-interval .....	13-13
ip igmp query-max-response-time .....	13-14
ip igmp startup-query-interval .....	13-14
ip igmp startup-query-count .....	13-15
ip igmp last-member-query-interval .....	13-15
ip igmp last-member-query-count .....	13-16
ip igmp robustness .....	13-16

## Chapter 14: Logging and Network Management

Configuring System Logging .....	14-1
Purpose .....	14-1
Commands .....	14-1
show logging server .....	14-2
set logging server .....	14-3
clear logging server .....	14-4
show logging default .....	14-4

set logging default .....	14-5
clear logging default .....	14-6
show logging application .....	14-6
set logging application .....	14-7
clear logging application .....	14-9
show logging local .....	14-9
set logging local .....	14-10
clear logging local .....	14-10
show logging buffer .....	14-11
show logging interface .....	14-11
set logging interface .....	14-12
clear logging interface .....	14-13
Monitoring Network Events and Status .....	14-14
Purpose .....	14-14
Commands .....	14-14
history .....	14-14
show history .....	14-15
set history .....	14-15
ping .....	14-16
show users .....	14-16
disconnect .....	14-17
show netstat .....	14-17
Managing Switch Network Addresses and Routes .....	14-19
Purpose .....	14-19
Commands .....	14-19
show arp .....	14-19
set arp .....	14-20
clear arp .....	14-21
traceroute .....	14-21
show mac .....	14-22
show mac agetime .....	14-23
set mac agetime .....	14-24
clear mac agetime .....	14-24
set mac algorithm .....	14-25
show mac algorithm .....	14-25
clear mac algorithm .....	14-26
set mac multicast .....	14-26
clear mac address .....	14-27
show mac unreserved-flood .....	14-28
set mac unreserved-flood .....	14-28
Configuring Simple Network Time Protocol (SNTP) .....	14-29
Purpose .....	14-29
Commands .....	14-29
show sntp .....	14-29
set sntp client .....	14-31
clear sntp client .....	14-31
set sntp server .....	14-32
clear sntp server .....	14-32
set sntp poll-interval .....	14-33
clear sntp poll-interval .....	14-33
set sntp poll-retry .....	14-34
clear sntp poll-retry .....	14-34
set sntp poll-timeout .....	14-35
clear sntp poll-timeout .....	14-35
set timezone .....	14-36
show sntp interface .....	14-37

set snmp interface .....	14-37
clear snmp interface .....	14-38
Configuring Node Aliases .....	14-39
Purpose .....	14-39
Commands .....	14-39
show nodealias config .....	14-39
set nodealias .....	14-40
clear nodealias config .....	14-41

## Chapter 15: RMON Configuration

RMON Monitoring Group Functions .....	15-1
Design Considerations .....	15-2
Statistics Group Commands .....	15-3
Purpose .....	15-3
Commands .....	15-3
show rmon stats .....	15-4
set rmon stats .....	15-4
clear rmon stats .....	15-5
History Group Commands .....	15-6
Purpose .....	15-6
Commands .....	15-6
show rmon history .....	15-6
set rmon history .....	15-7
clear rmon history .....	15-7
Alarm Group Commands .....	15-9
Purpose .....	15-9
Commands .....	15-9
show rmon alarm .....	15-9
set rmon alarm properties .....	15-10
set rmon alarm status .....	15-11
clear rmon alarm .....	15-12
Event Group Commands .....	15-13
Purpose .....	15-13
Commands .....	15-13
show rmon event .....	15-13
set rmon event properties .....	15-14
set rmon event status .....	15-15
clear rmon event .....	15-15
Filter Group Commands .....	15-17
Commands .....	15-17
show rmon channel .....	15-17
set rmon channel .....	15-18
clear rmon channel .....	15-19
show rmon filter .....	15-19
set rmon filter .....	15-20
clear rmon filter .....	15-21
Packet Capture Commands .....	15-22
Purpose .....	15-22
Commands .....	15-22
show rmon capture .....	15-22
set rmon capture .....	15-23
clear rmon capture .....	15-24

## Chapter 16: DHCP Server Configuration

DHCP Overview .....	16-1
DHCP Relay Agent .....	16-1
DHCP Server .....	16-1
Configuring a DHCP Server .....	16-2
Configuring General DHCP Server Parameters .....	16-3
Purpose .....	16-3
Commands .....	16-3
set dhcp .....	16-4
set dhcp bootp .....	16-4
set dhcp conflict logging .....	16-5
show dhcp conflict .....	16-5
clear dhcp conflict .....	16-6
set dhcp exclude .....	16-7
clear dhcp exclude .....	16-7
set dhcp ping .....	16-8
clear dhcp ping .....	16-8
show dhcp binding .....	16-9
clear dhcp binding .....	16-9
show dhcp server statistics .....	16-10
clear dhcp server statistics .....	16-11
Configuring IP Address Pools .....	16-12
Manual Pool Configuration Considerations .....	16-12
Purpose .....	16-12
Commands .....	16-12
set dhcp pool .....	16-13
clear dhcp pool .....	16-14
set dhcp pool network .....	16-14
clear dhcp pool network .....	16-15
set dhcp pool hardware-address .....	16-15
clear dhcp pool hardware-address .....	16-16
set dhcp pool host .....	16-16
clear dhcp pool host .....	16-17
set dhcp pool client-identifier .....	16-17
clear dhcp pool client-identifier .....	16-18
set dhcp pool client-name .....	16-19
clear dhcp pool client-name .....	16-19
set dhcp pool bootfile .....	16-20
clear dhcp pool bootfile .....	16-20
set dhcp pool next-server .....	16-21
clear dhcp pool next-server .....	16-21
set dhcp pool lease .....	16-22
clear dhcp pool lease .....	16-22
set dhcp pool default-router .....	16-23
clear dhcp pool default-router .....	16-23
set dhcp pool dns-server .....	16-24
clear dhcp pool dns-server .....	16-24
set dhcp pool domain-name .....	16-25
clear dhcp pool domain-name .....	16-25
set dhcp pool netbios-name-server .....	16-26
clear dhcp pool netbios-name-server .....	16-26
set dhcp pool netbios-node-type .....	16-27
clear dhcp pool netbios-node-type .....	16-27
set dhcp pool option .....	16-28
clear dhcp pool option .....	16-29

show dhcp pool configuration .....	16-29
------------------------------------	-------

## Chapter 17: DHCP Snooping and Dynamic ARP Inspection

DHCP Snooping Overview .....	17-1
DHCP Message Processing .....	17-1
Building and Maintaining the Database .....	17-2
Rate Limiting .....	17-3
Basic Configuration .....	17-3
DHCP Snooping Commands .....	17-4
set dhcpsnooping .....	17-4
set dhcpsnooping vlan .....	17-5
set dhcpsnooping database write-delay .....	17-5
set dhcpsnooping trust .....	17-6
set dhcpsnooping binding .....	17-7
set dhcpsnooping verify .....	17-7
set dhcpsnooping log-invalid .....	17-8
set dhcpsnooping limit .....	17-9
show dhcpsnooping .....	17-10
show dhcpsnooping database .....	17-11
show dhcpsnooping port .....	17-11
show dhcpsnooping binding .....	17-12
show dhcpsnooping statistics .....	17-13
clear dhcpsnooping binding .....	17-14
clear dhcpsnooping statistics .....	17-14
clear dhcpsnooping database .....	17-14
clear dhcpsnooping limit .....	17-15
Dynamic ARP Inspection Overview .....	17-16
Functional Description .....	17-16
Basic Configuration .....	17-18
Example Configuration .....	17-19
Dynamic ARP Inspection Commands .....	17-20
set arpinspection vlan .....	17-20
set arpinspection trust .....	17-21
set arpinspection validate .....	17-22
set arpinspection limit .....	17-23
set arpinspection filter .....	17-24
show arpinspection access-list .....	17-24
show arpinspection ports .....	17-25
show arpinspection vlan .....	17-26
show arpinspection statistics .....	17-26
clear arpinspection validate .....	17-27
clear arpinspection vlan .....	17-28
clear arpinspection filter .....	17-29
clear arpinspection limit .....	17-30
clear arpinspection statistics .....	17-31

## Chapter 18: Preparing for Router Mode

Pre-Routing Configuration Tasks .....	18-1
Example .....	18-2
Enabling Router Configuration Modes .....	18-2

## Chapter 19: IP Configuration

Configuring Routing Interface Settings .....	19-1
Purpose .....	19-1
Commands .....	19-1

show interface .....	19-2
interface .....	19-2
show ip interface.....	19-4
ip address .....	19-5
no shutdown .....	19-6
no ip routing .....	19-6
show running-config .....	19-7
Reviewing and Configuring the ARP Table .....	19-8
Purpose .....	19-8
Commands .....	19-8
show ip arp .....	19-8
arp .....	19-9
ip proxy-arp.....	19-10
arp timeout.....	19-11
clear arp-cache.....	19-11
Configuring Broadcast Settings .....	19-12
Purpose .....	19-12
Commands .....	19-12
ip directed-broadcast .....	19-12
ip forward-protocol.....	19-13
ip helper-address.....	19-14
Reviewing IP Traffic and Configuring Routes .....	19-15
Purpose .....	19-15
Commands .....	19-15
show ip route .....	19-15
ip route.....	19-16
ping.....	19-17
tracert.....	19-17
Configuring ICMP Redirects .....	19-18
Purpose .....	19-18
Commands .....	19-18
ip icmp redirect enable .....	19-18
show ip icmp redirect.....	19-19

## Chapter 20: IPv4 Routing Protocol Configuration

Configuring RIP .....	20-1
RIP Configuration Task List and Commands .....	20-1
Router Configuration Commands .....	20-2
router rip .....	20-2
distance .....	20-3
no auto-summary.....	20-4
split-horizon poison.....	20-4
passive-interface .....	20-5
receive-interface .....	20-6
redistribute .....	20-6
Interface Configuration Commands .....	20-7
ip rip enable .....	20-7
ip rip send version .....	20-8
ip rip receive version.....	20-8
ip rip authentication-key.....	20-9
ip rip message-digest-key.....	20-9
Configuring IRDP .....	20-11
Purpose .....	20-11
Commands .....	20-11
ip irdp enable .....	20-11

ip irdp maxadvertinterval .....	20-12
ip irdp minadvertinterval .....	20-12
ip irdp holdtime .....	20-13
ip irdp preference.....	20-13
ip irdp broadcast .....	20-14
show ip irdp .....	20-14

## Chapter 21: IPv6 Management

Purpose .....	21-1
Commands .....	21-1
show ipv6 status .....	21-1
set ipv6 .....	21-2
set ipv6 address .....	21-3
show ipv6 address .....	21-4
clear ipv6 address .....	21-4
set ipv6 gateway .....	21-5
clear ipv6 gateway .....	21-6
show ipv6 neighbors .....	21-7
show ipv6 netstat .....	21-7
ping ipv6 .....	21-8
traceroute ipv6 .....	21-9

## Chapter 22: Authentication and Authorization Configuration

Overview of Authentication and Authorization Methods .....	22-1
RADIUS Filter-ID Attribute and Dynamic Policy Profile Assignment .....	22-3
Setting the Authentication Login Method .....	22-4
Purpose .....	22-4
Commands .....	22-4
show authentication login .....	22-4
set authentication login .....	22-5
clear authentication login .....	22-5
Configuring RADIUS .....	22-6
Purpose .....	22-6
Commands .....	22-6
show radius .....	22-6
set radius .....	22-8
clear radius .....	22-9
show radius accounting .....	22-10
set radius accounting .....	22-11
clear radius accounting .....	22-12
show radius interface .....	22-12
set radius interface .....	22-13
clear radius interface .....	22-14
Configuring 802.1X Authentication .....	22-15
Purpose .....	22-15
Commands .....	22-15
show dot1x .....	22-15
show dot1x auth-config .....	22-17
set dot1x .....	22-18
set dot1x auth-config .....	22-19
clear dot1x auth-config .....	22-20
show eapol .....	22-21
set eapol .....	22-23
clear eapol .....	22-23



Configuring MAC Authentication .....	22-25
Purpose .....	22-25
Commands .....	22-25
show macauthentication .....	22-25
show macauthentication session .....	22-27
set macauthentication .....	22-28
set macauthentication password .....	22-28
clear macauthentication password .....	22-29
set macauthentication port .....	22-29
set macauthentication portinitialize .....	22-30
set macauthentication portquietperiod .....	22-30
clear macauthentication portquietperiod .....	22-31
set macauthentication macinitialize .....	22-31
set macauthentication reauthentication .....	22-32
set macauthentication portreauthenticate .....	22-32
set macauthentication macreauthenticate .....	22-33
set macauthentication reauthperiod .....	22-33
clear macauthentication reauthperiod .....	22-34
set macauthentication significant-bits .....	22-35
clear macauthentication significant-bits .....	22-35
Configuring Multiple Authentication Methods .....	22-37
About Multiple Authentication Types .....	22-37
About Multi-User Authentication .....	22-37
Commands .....	22-37
show multiauth .....	22-38
set multiauth mode .....	22-39
clear multiauth mode .....	22-39
set multiauth precedence .....	22-40
clear multiauth precedence .....	22-40
show multiauth port .....	22-41
set multiauth port .....	22-41
clear multiauth port .....	22-42
show multiauth station .....	22-43
show multiauth session .....	22-43
show multiauth idle-timeout .....	22-44
set multiauth idle-timeout .....	22-45
clear multiauth idle-timeout .....	22-46
show multiauth session-timeout .....	22-46
set multiauth session-timeout .....	22-47
clear multiauth session-timeout .....	22-48
Configuring User + IP Phone Authentication .....	22-48
Configuring VLAN Authorization (RFC 3580) .....	22-49
Purpose .....	22-49
Commands .....	22-49
set vlanauthorization .....	22-50
set vlanauthorization egress .....	22-50
clear vlanauthorization .....	22-51
show vlanauthorization .....	22-51
Configuring Policy Mappable Response .....	22-52
Operational Description .....	22-53
Commands .....	22-54
show policy mactable .....	22-54
set policy mactable .....	22-55
clear policy mactable .....	22-56
Configuring MAC Locking .....	22-57
Purpose .....	22-57

Commands .....	22-58
show maclock .....	22-58
show maclock stations.....	22-59
set maclock enable .....	22-60
set maclock disable .....	22-61
set maclock.....	22-61
clear maclock.....	22-62
set maclock static .....	22-63
clear maclock static .....	22-63
set maclock firstarrival .....	22-64
clear maclock firstarrival .....	22-65
set maclock agefirstarrival .....	22-65
clear maclock agefirstarrival .....	22-66
set maclock move.....	22-66
set maclock trap .....	22-67
Configuring Port Web Authentication (PWA) .....	22-68
About PWA .....	22-68
Purpose .....	22-68
Commands .....	22-68
show pwa.....	22-69
set pwa .....	22-70
show pwa banner .....	22-71
set pwa banner .....	22-71
clear pwa banner .....	22-72
set pwa displaylogo .....	22-72
set pwa ipaddress.....	22-73
set pwa protocol .....	22-73
set pwa guestname .....	22-74
clear pwa guestname .....	22-74
set pwa guestpassword .....	22-75
set pwa gueststatus .....	22-75
set pwa initialize .....	22-76
set pwa quietperiod .....	22-76
set pwa maxrequest .....	22-77
set pwa portcontrol .....	22-77
show pwa session .....	22-78
set pwa enhancedmode .....	22-79
Configuring Secure Shell (SSH) .....	22-80
Purpose .....	22-80
Commands .....	22-80
show ssh status .....	22-80
set ssh .....	22-80
set ssh hostkey .....	22-81
Configuring Access Lists .....	22-82
Purpose .....	22-82
Commands .....	22-82
show access-lists.....	22-82
access-list (standard) .....	22-83
access-list (extended).....	22-84
ip access-group .....	22-86

## Chapter 23: TACACS+ Configuration

show tacacs .....	23-2
set tacacs .....	23-3
show tacacs server .....	23-3

set tacacs server .....	23-4
clear tacacs server .....	23-5
show tacacs session .....	23-6
set tacacs session .....	23-7
clear tacacs session .....	23-8
show tacacs command .....	23-9
set tacacs command .....	23-9
show tacacs singleconnect .....	23-10
set tacacs singleconnect .....	23-10
show tacacs interface .....	23-11
set tacacs interface .....	23-11
clear tacacs interface .....	23-12

## Chapter 24: sFlow Configuration

Overview .....	24-1
Using sFlow in Your Network .....	24-1
Definitions .....	24-2
sFlow Agent Functionality .....	24-2
Sampling Mechanisms .....	24-2
Example Configuration .....	24-4
Commands .....	24-4
show sflow receivers .....	24-5
set sflow receiver owner .....	24-7
set sflow receiver ip .....	24-7
set sflow receiver maxdatagram .....	24-8
set sflow receiver port .....	24-9
clear sflow receiver .....	24-9
set sflow port poller .....	24-10
show sflow pollers .....	24-11
clear sflow port poller .....	24-12
set sflow port sampler .....	24-12
show sflow samplers .....	24-13
clear sflow port sampler .....	24-14
set sflow interface .....	24-14
show sflow interface .....	24-15
clear sflow interface .....	24-16
show sflow agent .....	24-17

## Appendix A: Policy and Authentication Capacities

Policy Capacities .....	A-1
Authentication Capacities .....	A-2

## Index

### Figures

1-1	Enterasys B5 Startup Screen .....	1-6
1-2	Sample CLI Defaults Description .....	1-8
1-3	Performing a Keyword Lookup .....	1-8
1-4	Performing a Partial Keyword Lookup .....	1-9
1-5	Scrolling Screen Output .....	1-9
1-6	Abbreviating a Command .....	1-10
10-1	Example of VLAN Propagation via GVRP .....	10-21

## Tables

1-1	Default Settings for Basic Switch Operation .....	1-2
1-2	Default Settings for Router Operation .....	1-4
1-3	Basic Line Editing Commands.....	1-10
3-1	Required CLI Setup Commands.....	3-1
3-2	Optional CLI Setup Commands.....	3-2
3-3	show system lockout Output Details.....	3-8
3-4	show system Output Details .....	3-14
3-5	show version Output Details .....	3-26
4-1	PoE Powered Device Classes .....	4-1
4-2	show inlinepower Output Details .....	4-3
4-3	show port inlinepower Output Details .....	4-5
6-1	show cdp Output Details.....	6-2
6-2	show ciscodp Output Details .....	6-8
6-3	show ciscodp port info Output Details .....	6-9
6-4	show lldp port local-info Output Details .....	6-19
6-5	show lldp port remote-info Output Display.....	6-22
7-1	show port status Output Details.....	7-4
7-2	show port counters Output Details .....	7-5
7-3	show port cablestatus Output Details .....	7-7
7-4	show linkflap parameters Output Details .....	7-27
7-5	show linkflap metrics Output Details.....	7-27
7-6	LACP Terms and Definitions .....	7-45
7-7	show lacp Output Details.....	7-48
8-1	SNMP Security Levels.....	8-3
8-2	show snmp engineid Output Details .....	8-4
8-3	show snmp counters Output Details.....	8-6
8-4	show snmp user Output Details.....	8-9
8-5	show snmp group Output Details .....	8-12
8-6	show snmp access Output Details .....	8-17
8-7	show snmp view Output Details .....	8-21
8-8	show snmp targetparams Output Details .....	8-24
8-9	show snmp targetaddr Output Details .....	8-27
8-10	show snmp notify Output Details.....	8-30
8-11	Basic SNMP Trap Configuration.....	8-36
9-1	show spantree Output Details .....	9-6
10-1	Command Set for Creating a Secure Management VLAN .....	10-2
10-2	show vlan Output Details.....	10-4
10-3	show gvrp configuration Output Details.....	10-23
11-1	show policy profile Output Details .....	11-3
11-2	show policy rule Output Details .....	11-8
11-3	Valid Values for Policy Classification Rules .....	11-11
14-1	show logging server Output Details.....	14-3
14-2	show logging application Output Details.....	14-7
14-3	Mnemonic Values for Logging Applications.....	14-8
14-4	show netstat Output Details.....	14-18
14-5	show arp Output Details .....	14-20
14-6	show mac Output Details.....	14-23
14-7	show snmp Output Details.....	14-30
14-8	show nodealias config Output Details .....	14-40
15-1	RMON Monitoring Group Functions and Commands.....	15-1
15-2	show rmon alarm Output Details .....	15-10
15-3	show rmon event Output Details .....	15-14
18-1	Enabling the Switch for Routing .....	18-2
18-2	Router CLI Configuration Modes.....	18-2

19-1	show ip interface Output Details .....	19-4
19-2	show ip arp Output Details .....	19-9
20-1	RIP Configuration Task List and Commands .....	20-1
22-1	show radius Output Details.....	22-7
22-2	show eapol Output Details.....	22-22
22-3	show macauthentication Output Details .....	22-26
22-4	show macauthentication session Output Details .....	22-27
22-5	show vlanauthorization Output Details .....	22-52
22-6	show maclock Output Details .....	22-59
22-7	show maclock stations Output Details.....	22-60
22-8	show pwa Output Details.....	22-69
23-1	show tacacs Output Details .....	23-2
24-1	sFlow Definitions .....	24-2
24-2	show sflow receivers Output Descriptions.....	24-6
A-1	Policy Capacities .....	A-1
A-2	Authentication Capacities .....	A-2



---

# About This Guide

Welcome to the Enterasys B5 CLI Reference. This manual explains how to access the device's Command Line Interface (CLI) and how to use it to configure Enterasys B5 switch devices.

---

## Important Notice

Depending on the firmware version used in your Enterasys B5 device, some features described in this document may not be supported. Refer to the Release Notes for your device to determine which features are supported.

---

## Using This Guide

A general working knowledge of basic network operations and an understanding of CLI management applications is helpful before configuring the device.

This manual describes how to do the following:

- Access the switch CLI.
- Use CLI commands to perform network management and device configuration operations
- Establish and manage Virtual Local Area Networks (VLANs).
- Establish and manage static and dynamically-assigned policy classifications.
- Establish and manage priority classification.
- Configure security protocols, including 802.1X and RADIUS, SSHv2, MAC locking, and MAC authentication.

## Structure of This Guide

The guide is organized as follows:

[Chapter 1, Introduction](#), provides an overview of the tasks that can be accomplished using the CLI interface, an overview of local management requirements, an overview of the device's factory default settings, and information about using the Command Line Interface (CLI).

[Chapter 2, Configuring Switches in a Stack](#), provides information about how to configure and manage stacked switches.

[Chapter 3, Basic Configuration](#), provides how to set basic system properties, how to download a firmware image, how to configure WebView and Telnet, how to manage configuration files, how to set the login password, and how to exit the CLI.

[Chapter 4, Configuring System Power and PoE](#), describes the commands used to review and set system power and PoE parameters on devices that offer Power over Ethernet.

[Chapter 5, Transmit Queue Monitoring Configuration](#), describes the commands used to monitor transmit queues and, if a queue is found to be stalled, to take corrective action.

[Chapter 6, Discovery Protocol Configuration](#) provides how to configure discovery protocols supported by the device.

**Chapter 7, Port Configuration**, describes how to review and configure console port settings, and how to enable or disable switch ports and configure switch port settings, including port speed, duplex mode, auto-negotiation, flow control, port mirroring, link aggregation and broadcast suppression.

**Chapter 8, SNMP Configuration**, describes how to configure SNMP users and user groups, access rights, target addresses, and notification parameters.

**Chapter 9, Spanning Tree Configuration**, describes how to review and set Spanning Tree bridge parameters for the device, including bridge priority, hello time, maximum aging time and forward delay; and how to review and set Spanning Tree port parameters, including port priority and path costs. Configuring the SpanGuard and Loop Protect functions is also described.

**Chapter 10, 802.1Q VLAN Configuration**, describes how to create static VLANs, select the mode of operation for each port, establish VLAN forwarding (egress) lists, route frames according to VLAN ID, display the current ports and port types associated with a VLAN and protocol, create a secure management VLAN, and configure ports on the device as GVRP-aware ports.

**Chapter 11, Policy Classification Configuration**, describes how to create, change or remove user roles or profiles based on business-specific use of network services; how to permit or deny access to specific services by creating and assigning classification rules which map user profiles to frame filtering policies; how to classify frames to a VLAN or Class of Service (CoS); and how to assign or unassign ports to policy profiles so that only ports activated for a profile will be allowed to transmit frames accordingly.

**Chapter 12, Port Priority Configuration**, describes how to set the transmit priority of each port and configure a rate limit for a given port and list of priorities.

**Chapter 13, IGMP Configuration**, describes how to configure Internet Group Management Protocol (IGMP) settings for multicast filtering.

**Chapter 14, Logging and Network Management**, describes how to configure Syslog, how to manage general switch settings, how to monitor network events and status, and how to configure SNMP and node aliases.

**Chapter 15, RMON Configuration**, describes how to use RMON (Remote Network Monitoring), which provides comprehensive network fault diagnosis, planning, and performance tuning information and allows for interoperability between SNMP management stations and monitoring agents.

**Chapter 16, DHCP Server Configuration**, describes how to review and configure DHCP server parameters, how to review and configure DHCP address pools, and how to display DHCP server information.

**Chapter 17, DHCP Snooping and Dynamic ARP Inspection**, describes two security features — DHCP snooping, which monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP messages and to build a database of authorized address bindings, and Dynamic ARP inspection, which uses the bindings database created by the DHCP snooping feature to reject invalid and malicious ARP packets.

**Chapter 18, Preparing for Router Mode**, provides information about router modes and how to activate a license.

**Chapter 19, IP Configuration**, describes how to enable IP routing for router mode operation, how to configure IP interface settings, how to review and configure the routing ARP table, how to review and configure routing broadcasts, and how to configure IP routes.

**Chapter 20, IPv4 Routing Protocol Configuration**, describes how to configure IPv4 routing and routing protocols, including RIP and IRDP.

**Chapter 21, IPv6 Management**, describes how to manage IPv6 at Layer 2. These switch level commands allow you to enable or disable the IPv6 management function, to configure and display the IPv6 host address and IPv6 gateway for the switch, and to display IPv6 status information.



[Chapter 22, Authentication and Authorization Configuration](#), describes how to configure the authentication and authorization features provided on the Enterasys B5.

[Chapter 23, TACACS+ Configuration](#), provides information about the commands used to configure and monitor TACACS+ (Terminal Access Controller Access-Control System Plus).

[Chapter 24, sFlow Configuration](#), provides information about the commands used to configure and monitor the sFlow system.

[Appendix A, Policy and Authentication Capacities](#), lists the policy and authentication capacities of the Enterasys B5 as of the date this document was published.

## Related Documents

The following Enterasys Networks documents may help you to set up, control, and manage the device:

- *Enterasys Firmware Feature Guides*
- *Enterasys B5 Hardware Installation Guide*
- Redundant Power System Quick References

Documents listed above, can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following web site:

<https://extranet.enterasys.com/downloads/>

## Conventions Used in This Guide

The following conventions are used in the text of this document:

Convention	Description
<b>Bold font</b>	Indicates mandatory keywords, parameters or keyboard keys.
<i>italic font</i>	Indicates complete document titles.
<code>Courier font</code>	Used for examples of information displayed on the screen.
<i>Courier font in italics</i>	Indicates a user-supplied value, either required or optional.
[ ]	Square brackets indicate an optional value.
{ }	Braces indicate required values. One or more values may be required.
	A vertical bar indicates a choice in values.
[x   y   z]	Square brackets with a vertical bar indicate a choice of a value.
{x   y   z}	Braces with a vertical bar indicate a choice of a required value.
[x {y   z}]	A combination of square brackets with braces and vertical bars indicates a required choice of an optional value.

The following icons are used in this guide:



**Note:** Calls the reader's attention to any item of information that may be of special importance.



**Caution:** Contains information essential to avoid damage to the equipment.

**Precaución:** Contiene información esencial para prevenir dañar el equipo.

**Achtung:** Verweist auf wichtige Informationen zum Schutz gegen Beschädigungen.

## Getting Help

For additional support related to this switch or document, contact Enterasys Networks using one of the following methods:

---

World Wide Web	<a href="http://www.enterasys.com/support">http://www.enterasys.com/support</a>
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-978-684-1000  For the Enterasys Networks Support toll-free number in your country: <a href="http://www.enterasys.com/support">http://www.enterasys.com/support</a>
Internet mail	<a href="mailto:support@enterasys.com">support@enterasys.com</a>  To expedite your message, type <b>[SWITCHING]</b> in the subject line.

---

To send comments or suggestions concerning this document to the Technical Publications Department:  
[techpubs@enterasys.com](mailto:techpubs@enterasys.com)

---

Make sure to include the document Part Number in the email message.

---

### Before calling Enterasys Networks, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (for example, layout, cable type)
- Network load and frame size at the time of trouble (if known)
- The switch history (for example, have you returned the switch before, is this a recurring problem?)
- Any previous Return Material Authorization (RMA) numbers

## Introduction

This chapter provides an overview of the Enterasys B5's unique features and functionality, an overview of the tasks that may be accomplished using the CLI interface, an overview of ways to manage the switch, factory default settings, and information about how to use the Command Line Interface to configure the switch.

For information about...	Refer to page...
<a href="#">Enterasys B5 CLI Overview</a>	1-1
<a href="#">Switch Management Methods</a>	1-1
<a href="#">Factory Default Settings</a>	1-2
<a href="#">Using the Command Line Interface</a>	1-6

## Enterasys B5 CLI Overview

The Enterasys Networks Enterasys B5 CLI interface allows you to perform a variety of network management tasks, including the following:

- Use CLI commands to perform network management and switch configuration operations.
- Download a new firmware image.
- Assign IP address and subnet mask.
- Select a default gateway.
- Establish and manage Virtual Local Area Networks (VLANs).
- Establish and manage policy profiles and classifications.
- Establish and manage priority classification.
- Configure security protocols, including 802.1X and RADIUS, SSHv2, PWA, MAC locking, and MAC authentication.

## Switch Management Methods

The Enterasys B5 switch can be managed using the following methods:

- Locally using a VT type terminal connected to the console port.
- Remotely using a VT type terminal connected through a modem.
- Remotely using an SNMP management station.
- In-band through a Telnet connection.
- In-band using the Enterasys NetSight® management application.

- Remotely using WebView™, Enterasys Networks' embedded web server application.

The *Installation Guide* for your Enterasys B5 device provides setup instructions for connecting a terminal or modem to the switch.

## Factory Default Settings

The following tables list factory default settings available on the Enterasys B5 switch.

**Table 1-1 Default Settings for Basic Switch Operation**

Feature	Default Setting
<b>Switch Mode Defaults</b>	
CDP discovery protocol	Auto enabled on all ports.
CDP authentication code	Set to 00-00-00-00-00-00-00-00
CDP hold time	Set to 180 seconds.
CDP interval	Transmit frequency of CDP messages set to 60 seconds.
Cisco discovery protocol	Auto enabled on all ports.
Cisco DP hold time	Set to 180 seconds.
Cisco DP interval timer	Set to 60 seconds.
Community name	Public.
Console (serial) port required settings	Baud rate: 9600 Data bits: 8 Flow control: disabled Stop bits: 1 Parity: none
DHCP server	Disabled.
EAPOL	Disabled.
EAPOL authentication mode	When enabled, set to auto for all ports.
GARP timer	Join timer set to 20 centiseconds; leave timer set to 60 centiseconds; leaveall timer set to 1000 centiseconds.
GVRP	Globally enabled. Disabled per port.
History buffer size	20 lines.
IEEE 802.1 authentication	Disabled.
IGMP snooping	Disabled. When enabled, query interval is set to 260 seconds and response time is set to 10 seconds.
IP mask and gateway	Subnet mask set to 0.0.0.0; default gateway set to 0.0.0.0.
IP routes	No static routes configured.
Jumbo frame support	Enabled on all ports.
Link aggregation control protocol (LACP)	Globally enabled. Disabled per port.
Link aggregation admin key	Set to 32768 for all ports.

**Table 1-1 Default Settings for Basic Switch Operation (Continued)**

Feature	Default Setting
Link aggregation flow regeneration	Disabled.
Link aggregation system priority	Set to 32768 for all ports.
Link aggregation outport algorithm	Set to DIP-SIP.
Lockout	Set to disable Read-Write and Read-Only users, and to lockout the default admin (Super User) account for 15 minutes, after 3 failed login attempts.
Logging	Syslog port set to UDP port number 514. Logging severity level set to 6 (significant conditions) for all applications.
MAC aging time	Set to 300 seconds.
MAC locking	Disabled (globally and on all ports).
Passwords	Set to an empty string for all default user accounts. User must press ENTER at the password prompt to access CLI.
Password aging	Disabled.
Password history	No passwords are checked for duplication.
Policy classification	Classification rules are automatically enabled when created.
Port auto-negotiation	Enabled on all ports.
Port advertised ability	Maximum ability advertised on all ports.
Port broadcast suppression	Enabled and set to limit broadcast packets to 14,881 per second on all switch ports.
Port duplex mode	Set to half duplex, except for 100BASE-FX and 1000BASE-X, which is set to full duplex.
Port enable/disable	Enabled.
Port priority	Set to 0.
Port speed	Set to 10 Mbps, except for 1000BASE-X, which is set to 1000 Mbps, and 100BASE-FX, which is set to 100 Mbps.
Port trap	All ports are enabled to send link traps.
Power over Ethernet port admin state	Administrative state is on (auto).
Priority classification	Classification rules are automatically enabled when created.
RADIUS client	Disabled.
RADIUS last resort action	When the client is enabled, set to Challenge.
RADIUS retries	When the client is enabled, set to 3.
RADIUS timeout	When the client is enabled, set to 20 seconds.
Rate limiting	Disabled (globally and on all ports).
SNMP	Enabled.
SNTP	Disabled.
Spanning Tree	Globally enabled and enabled on all ports.

**Table 1-1 Default Settings for Basic Switch Operation (Continued)**

Feature	Default Setting
Spanning Tree edge port administrative status	Edge port administrative status begins with the value set to <b>false</b> initially after the device is powered up. If a Spanning Tree BPDU is not received on the port within a few seconds, the status setting changes to <b>true</b> .
Spanning Tree edge port delay	Enabled.
Spanning Tree forward delay	Set to 15 seconds.
Spanning Tree hello interval	Set to 2 seconds.
Spanning Tree ID (SID)	Set to 0.
Spanning Tree maximum aging time	Set to 20 seconds.
Spanning Tree port priority	All ports with bridge priority are set to 128 (medium priority).
Spanning Tree priority	Bridge priority is set to 32768.
Spanning Tree topology change trap suppression	Enabled.
Spanning Tree version	Set to mstp (Multiple Spanning Tree Protocol).
SSH	Disabled.
System baud rate	Set to 9600 baud.
System contact	Set to empty string.
System location	Set to empty string.
System name	Set to empty string.
Terminal	CLI display set to 80 columns and 24 rows.
Timeout	Set to 5 minutes.
User names	Login accounts set to <b>ro</b> for Read-Only access; <b>rw</b> for Read-Write access; and <b>admin</b> for Super User access.
VLAN dynamic egress	Disabled on all VLANs.
VLAN ID	All ports use a VLAN identifier of 1.
Host VLAN	Default host VLAN is 1.

Not all of the following routing features are available on all platforms. Check the Release Notes for your specific platforms for details.

**Table 1-2 Default Settings for Router Operation**

Output...	What it displays...
Access groups (IP security)	None configured.
Access lists (IP security)	None configured.
Area authentication (OSPF)	Disabled.
Area default cost (OSPF)	Set to 1.
Area NSSA (OSPF)	None configured.

**Table 1-2 Default Settings for Router Operation (Continued)**

Output...	What it displays...
Area range (OSPF)	None configured.
ARP table	No permanent entries configured.
ARP timeout	Set to 14,400 seconds.
Authentication key (RIP and OSPF)	None configured.
Authentication mode (RIP and OSPF)	None configured.
Dead interval (OSPF)	Set to 40 seconds.
Disable triggered updates (RIP)	Triggered updates allowed.
Distribute list (RIP)	No filters applied.
DVMRP	Disabled. Metric set to 1.
Hello interval (OSPF)	Set to 10 seconds for broadcast and point-to-point networks. Set to 30 seconds for non-broadcast networks.
ICMP	Enabled for echo-reply and mask-reply modes.
IP-directed broadcasts	Disabled.
IP forward-protocol	Enabled with no port specified.
IP interfaces	Disabled with no IP addresses specified.
IRDP	Disabled on all interfaces. When enabled, maximum advertisement interval is set to 600 seconds, minimum advertisement interval is set to 450 seconds, holdtime is set to 1800 seconds, and address preference is set to 0.
MD5 authentication (OSPF)	Disabled with no password set.
MTU size	Set to 1500 bytes on all interfaces.
OSPF	Disabled.
OSPF cost	Set to 10 for all interfaces.
OSPF network	None configured.
OSPF priority	Set to 1.
Passive interfaces (RIP)	None configured.
Proxy ARP	Enabled on all interfaces.
Receive interfaces (RIP)	Enabled on all interfaces.
Retransmit delay (OSPF)	Set to 1 second.
Retransmit interval (OSPF)	Set to 5 seconds.
RIP receive version	Set to accept both version 1 and version 2.
RIP send version	Set to version 1.
RIP offset	No value applied.
SNMP	Enabled.
Split horizon	Enabled for RIP packets without poison reverse.
Stub area (OSPF)	None configured.
Telnet	Enabled.

**Table 1-2 Default Settings for Router Operation (Continued)**

Output...	What it displays...
Telnet port (IP)	Set to port number 23.
Timers (OSPF)	SPF delay set to 5 seconds. SPF holdtime set to 10 seconds.
Transmit delay (OSPF)	Set to 1 second.
VRRP	Disabled.

## Using the Command Line Interface

### Starting a CLI Session

#### Connecting Using the Console Port

Connect a terminal to the local console port as described in your *Enterasys B5 Installation Guide*. The startup screen, [Figure 1-1](#), will display on the terminal. You can now start the Command Line Interface (CLI) by

- using a default user account, as described in [“Using a Default User Account”](#) on page 1-7, or
- using an administratively-assigned user account as described in [“Using an Administratively Configured User Account”](#) on page 1-7.

**Figure 1-1 Enterasys B5 Startup Screen**

```

Username:admin
Password:

Enterasys Enterasys B5
Command Line Interface

Enterasys Networks, Inc.
50 Minuteman Rd.
Andover, MA 01810-1008 U.S.A.

Phone: +1 978 684 1000
E-mail: support@enterasys.com
WWW: http://www.enterasys.com

(c) Copyright Enterasys Networks, Inc. 2011

Chassis Serial Number:      041800249041
Chassis Firmware Revision:  6.42.xx.xxxx

B5(su)->

```

#### Connecting Using Telnet

Once the Enterasys B5 device has a valid IP address, you can establish a Telnet session from any TCP/IP based node on the network. For information about setting the switch’s IP address, refer to [“set ip address”](#) on page 3-10.

To establish a Telnet session:



1. Telnet to the switch's IP address.
2. Enter login (user name) and password information in one of the following ways:
  - If the switch's default login and password settings have not been changed, follow the steps listed in [“Using a Default User Account”](#) on page 1-7, or
  - Enter an administratively-configured user name and password.

The notice of authorization and the prompt displays as shown in [Figure 1-1](#).

For information about configuring Telnet settings, refer to [“Starting and Configuring Telnet”](#) on page 3-36.

Refer to the instructions included with the Telnet application for information about establishing a Telnet session.

## Logging In

By default, the Enterasys B5 switch is configured with three user login accounts—**ro** for Read-Only access, **rw** for Read-Write access, and **admin** for super-user access to all modifiable parameters. The default password is set to a blank string. For information on changing these default settings, refer to [“Setting User Accounts and Passwords”](#) on page 3-2.

### Using a Default User Account

If this is the first time you are logging in to the Enterasys B5 switch, or if the default user accounts have not been administratively changed, proceed as follows:

1. At the login prompt, enter one of the following default user names:
  - **ro** for Read-Only access.
  - **rw** for Read-Write access.
  - **admin** for Super User access.
2. Press ENTER. The Password prompt displays.
3. Leave this string blank and press ENTER. The switch information and prompt displays as shown in [Figure 1-1](#).

### Using an Administratively Configured User Account

If the switch's default user account settings have been changed, proceed as follows:

1. At the login prompt, enter your administratively-assigned user name and press ENTER.
2. At the Password prompt, enter your password and press ENTER.

The notice of authorization and the prompt displays as shown in [Figure 1-1](#).



**Note:** Users with Read-Write (rw) and Read-Only access can use the [set password](#) command (page 3-5) to change their own passwords. Administrators with Super User (su) access can use the [set system login](#) command (page 3-4) to create and change user accounts, and the [set password](#) command to change any local account password.

## Navigating the Command Line Interface

### Getting Help with CLI Syntax

The Enterasys B5 switch allows you to display usage and syntax information for individual commands by typing **help** or **?** after the command.

### CLI Command Defaults Descriptions

Each command description in this guide includes a section entitled “Defaults” which contains different information from the factory default settings on the switch described in [Table 1-1](#). The section defines CLI behavior if the user enters a command without typing optional parameters (indicated by square brackets [ ]). For commands without optional parameters, the defaults section lists “None”. For commands with optional parameters, this section describes how the CLI responds if the user opts to enter only the keywords of the command syntax. [Figure 1-2](#) provides an example.

**Figure 1-2 Sample CLI Defaults Description**

<p><b>Syntax</b></p> <pre>show port status [port-string]</pre> <p><b>Defaults</b></p> <p>If <i>port-string</i> is not specified, status information for all ports will be displayed.</p>
--

### CLI Command Modes

Each command description in this guide includes a section entitled “Mode” which states whether the command is executable in Admin (Super User), Read-Write, or Read-Only mode. Users with Read-Only access will only be permitted to view Read-Only (**show**) commands. Users with Read-Write access will be able to modify all modifiable parameters in **set** and **show** commands, as well as view Read-Only commands. Administrators or Super Users will be allowed all Read-Write and Read-Only privileges, and will be able to modify local user accounts. The Enterasys B5 switch indicates which mode a user is logged in as by displaying one of the following prompts:

- Admin: B5(su)->
- Read-Write: B5(rw)->
- Read-Only: B5(ro)->

### Performing Keyword Lookups

Entering a space and a question mark (?) after a keyword will display all commands beginning with the keyword. [Figure 1-3](#) shows how to perform a keyword lookup for the **show snmp** command. In this case, four additional keywords are used by the **show snmp** command. Entering a space and a question mark (?) after any of these parameters (such as **show snmp community**) will display additional parameters nested within the syntax.

**Figure 1-3 Performing a Keyword Lookup**

B5(su)->show snmp ?	
community	SNMP v1/v2c community name configuration
notify	SNMP notify configuration
targetaddr	SNMP target address configuration
targetparams	SNMP target parameters configuration

Entering a question mark (?) without a space after a partial keyword will display a list of commands that begin with the partial keyword. [Figure 1-4](#) shows how to use this function for all commands beginning with **co**:

**Figure 1-4 Performing a Partial Keyword Lookup**

```
B5 (rw) ->co?
configure                copy
B5 (su) ->co
```



**Note:** At the end of the lookup display, the system will repeat the command you entered without the ?.

## Displaying Scrolling Screens

If the CLI screen length has been set using the **set length** command as described on page 3-29, CLI output requiring more than one screen will display `--More--` to indicate continuing screens. To display additional screen output:

- Press any key other than ENTER to advance the output one screen at a time.
- Press ENTER to advance the output one line at a time.

The example in [Figure 1-5](#) shows how the **show mac** command indicates that output continues on more than one screen.

**Figure 1-5 Scrolling Screen Output**

```
B5 (su) ->show mac

MAC Address           FID      Port      Type
-----
00-00-1d-67-68-69    1        host      Management
00-00-02-00-00-00    1        ge.1.2    Learned
00-00-02-00-00-01    1        ge.1.3    Learned
00-00-02-00-00-02    1        ge.1.4    Learned
00-00-02-00-00-03    1        ge.1.5    Learned
00-00-02-00-00-04    1        ge.1.6    Learned
00-00-02-00-00-05    1        ge.1.7    Learned
00-00-02-00-00-06    1        ge.1.8    Learned
00-00-02-00-00-07    1        ge.1.9    Learned
00-00-02-00-00-08    1        ge.1.10   Learned
--More--
```

## Abbreviating and Completing Commands

The Enterasys B5 switch allows you to abbreviate CLI commands and keywords down to the number of characters that will allow for a unique abbreviation. [Figure 1-6](#) shows how to abbreviate the **show netstat** command to **sh net**.

**Figure 1-6 Abbreviating a Command**

```

B5(su)->sh net
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
-----
TCP        0      0 10.21.73.13.23         134.141.190.94.51246   ESTABLISHED
TCP        0     275 10.21.73.13.23         134.141.192.119.4724  ESTABLISHED
TCP        0      0 *.80                   *.*                     LISTEN
TCP        0      0 *.23                   *.*                     LISTEN
UDP        0      0 10.21.73.13.1030      134.141.89.113.514    *.*
UDP        0      0 *.161                  *.*                     *.*
UDP        0      0 *.1025                 *.*                     *.*
UDP        0      0 *.123                  *.*                     *.*

```

## Basic Line Editing Commands

The CLI supports EMACS-like line editing commands. [Table 1-3](#) lists some commonly used commands.

**Table 1-3 Basic Line Editing Commands**

Key Sequence	Command
Ctrl+A	Move cursor to beginning of line.
Ctrl+B	Move cursor back one character.
Ctrl+D	Delete a character.
Ctrl+E	Move cursor to end of line.
Ctrl+F	Move cursor forward one character.
Ctrl+H	Delete character to left of cursor.
Ctrl+I or TAB	Complete word.
Ctrl+K	Delete all characters after cursor.
Ctrl+N	Scroll to next command in command history (use the CLI history command to display the history).
Ctrl+P	Scroll to previous command in command history.
Ctrl+Q	Resume the CLI process.
Ctrl+S	Pause the CLI process (for scrolling).
Ctrl+T	Transpose characters.
Ctrl+U or Ctrl+X	Delete all characters before cursor.
Ctrl+W	Delete word to the left of cursor.
Ctrl+Y	Restore the most recently deleted item.

## Configuring Switches in a Stack

This chapter provides information about configuring Enterasys B5 switches in a stack.

For information about ...	Refer to page ...
<a href="#">About Enterasys B5 Switch Operation in a Stack</a>	2-1
<a href="#">Installing a New Stackable System of Up to Eight Units</a>	2-2
<a href="#">Installing Previously-Configured Systems in a Stack</a>	2-3
<a href="#">Adding a New Unit to an Existing Stack</a>	2-3
<a href="#">Creating a Virtual Switch Configuration</a>	2-3
<a href="#">Considerations About Using Clear Config in a Stack</a>	2-4
<a href="#">Stacking Configuration and Management Commands</a>	2-5

### About Enterasys B5 Switch Operation in a Stack

The Enterasys B5 products are stackable switches that can be adapted and scaled to help meet your network needs. These switches provide a management platform and uplink to a network backbone for a stacked group of up to eight Enterasys B5 switches.



**Note:** B5 switches can only be stacked with other B5 switches.

Once installed in a stack, the switches behave and perform as a single switch product. As such, you can start with a single unit and add more units as your network expands. You can also mix different products in the family in a single stack to provide a desired combination of port types and functions to match the requirements of individual applications. In all cases, a stack of units performs as one large product, and is managed as a single network entity.

When switches are installed and connected as described in your Enterasys B5 Installation Guide, the following occurs during initialization:

- The switch that will manage the stack is automatically established. This is known as the manager switch.
- All other switches are established as members in the stack.
- The hierarchy of the switches that will assume the function of backup manager is also determined in case the current manager malfunctions, is powered down, or is disconnected from the stack.
- The console port on the manager switch remains active for out-of-band (local) switch management, but the console port on each member switch is deactivated. This enables you to

set the IP address and system password using a single console port. Now each switch can be configured locally using only the manager's console port, or inband using a remote device and the CLI set of commands described in this section.

Once a stack is created (more than one switch is interconnected), the following procedure occurs:

1. By default, unit IDs are arbitrarily assigned on a first-come, first-served basis.
2. Unit IDs are saved against each module. Then, every time a board is power-cycled, it will initialize with the same unit ID. This is important for port-specific information (for example: ge.4.12 is the 12th Gigabit Ethernet port on Unit # 4).
3. The management election process uses the following precedence to assign a management switch:
  - a. Previously assigned / elected management unit
  - b. Management assigned priority (values 1-15)
  - c. Hardware preference level
  - d. Highest MAC Address

Use the following recommended procedures when installing a new stackable system or adding a new unit to an existing stack.

---

### Important

The following procedures assume that all units have a clean configuration from manufacturing. When adding a new unit to an already running stack, it is also assumed that the new unit is using the same firmware image version as other units in the stack.

---

## Installing a New Stackable System of Up to Eight Units

Use the following procedure for installing a new stack of up to eight units out of the box.

1. Before applying power, make **all** physical connections with the stack cables as described in your Enterasys B5 Installation Guide.
2. Once all of the stack cables have been connected, individually power on each unit from top to bottom.



**Notes:** Ensure that each switch is fully operational before applying power to the next switch. Since unit IDs are assigned on a first-come, first-served basis, this will ensure that unit IDs are ordered sequentially.

Once unit IDs are assigned, they are persistent and will be retained during a power cycle to any or all of the units.

3. (Optional) If desired, change the management unit using the **set switch movemanagement** command as described in “[set switch movemanagement](#)” on page 2-10.
4. Once the desired master unit has been selected, reset the system using the **reset** command (page 3-50).
5. After the stack has been configured, you can use the **show switch unit** command (page 2-5) to physically identify each unit. When you enter the command with a unit number, the MGR LED of the specified switch will blink for 10 seconds. The normal state of this LED is off for member units and steady green for the manager unit.

## Installing Previously-Configured Systems in a Stack

If member units in a stack have been previous members of a different stack, you may need to configure the renumbering of the stack as follows:

1. Stack the units in the method desired, and connect the stack cables.
2. Power up only the unit you wish to be manager.
3. Once the management unit is powered up, log into the CLI, and use the **show switch** command as described in “[show switch](#)” on page 2-5 to display stacking information.
4. Clear any switches which are listed as “unassigned” using the **clear switch member** command as described in “[clear switch member](#)” on page 2-11.
5. Power up the member of the stack you wish to become unit 2. Once the second unit is fully powered, the COM session of the CLI will state that a new CPU was added.
6. Use the **show switch** command to redisplay stacking information.
  - a. If the new member displays as unit 2, you can proceed to repeat this step with the next unit.
  - b. If the new member displays a different unit number, you must:
    - (1) Renumber the stack using the **set switch renumber** command as described in “[set switch](#)” on page 2-8, then
    - (2) Clear the original unit number using the **clear switch member** command.
7. Repeat Step 6 until all members have been renumbered in the order you desire.
8. After the stack has been reconfigured, you can use the **show switch unit** command (“[show switch](#)” on page 2-5) to physically confirm the identity of each unit. When you enter the command with a unit number, the MGR LED of the specified switch will blink for 10 seconds. The normal state of this LED is off for member units and steady green for the manager unit.

## Adding a New Unit to an Existing Stack

Use the following procedure for installing a new unit to an existing stack configuration. This procedure assumes that the new unit being added has a clean configuration from manufacturing and is running the same firmware image version as other units in the stack.

1. Ensure that power is off on the new unit being installed.
2. Use one of the following methods to complete stack cable connections:
  - If the running stack uses a daisy chain topology, make the stack cable connections from the bottom of the stack to the new unit (that is, STACK DOWN port from the bottom unit of the running stack to the STACK UP port on the new unit).
  - If the running stack uses a ring stack topology, break the ring and make the stack cable connections to the new unit to close the ring.
3. Apply power to the new unit.

## Creating a Virtual Switch Configuration

You can create a configuration for a Enterasys B5 switch before adding the actual physical device to a stack. This preconfiguration feature includes configuring protocols on the ports of the “virtual switch.”

To create a virtual switch configuration in a stack environment:

1. Display the types of switches supported in the stack, using the **show switch swichtype** command (page 2-6).
2. Using the output of the **show switch swichtype** command, determine the switch index (SID) of the model of switch being configured.
3. Add the virtual switch to the stack using the **set switch member** command (page 2-10). Use the SID of the switch model, determined in the previous step, and the unit ID that you want to assign to this switch member.
4. Proceed to configure the ports of the virtual switch as you would do for physically present devices.

```
B5(su)->set vlan create 555
B5(su)->clear vlan egress 1 ge.2.1
B5(su)->set port vlan ge.2.1 555 untagged
B5(su)->show port vlan ge.2.1
ge.2.1 is set to 555
```



**Note:** If you preconfigure a virtual switch and then add a physical switch of a different type to the stack as that unit number, any configured functionality that cannot be supported on the physical switch will cause a configuration mismatch status for that device and the ports of the new device will join detached. You must clear the mismatch before the new device will properly join the stack.

## Considerations About Using Clear Config in a Stack

When using the **clear config** command (page 3-50) to clear configuration parameters in a stack, it is important to remember the following:

- Use **clear config** to clear config parameters without clearing stack unit IDs. This command WILL NOT clear stack parameters or the IP address and avoids the process of renumbering the stack.
- Use **clear config all** when it is necessary to clear all config parameters, including stack unit IDs and switch priority values. This command will not clear the IP address nor will it remove an applied advanced feature license.
- Use **clear ip address** to remove the IP address of the stack.
- Use **clear license** to remove an applied license from a switch.

Configuration parameters and stacking information can also be cleared **on the master unit only** by selecting the “restore configuration to factory defaults” option from the boot menu on switch startup. This selection will leave stacking priorities on all other units.



# Stacking Configuration and Management Commands

## Purpose

To review, individually configure and manage switches in a Enterasys B5 stack.

## Commands

For information about...	Refer to page...
<a href="#">show switch</a>	<a href="#">2-5</a>
<a href="#">show switch switchtype</a>	<a href="#">2-6</a>
<a href="#">show switch stack-ports</a>	<a href="#">2-7</a>
<a href="#">set switch</a>	<a href="#">2-8</a>
<a href="#">set switch copy-fw</a>	<a href="#">2-9</a>
<a href="#">set switch description</a>	<a href="#">2-9</a>
<a href="#">set switch movemanagement</a>	<a href="#">2-10</a>
<a href="#">set switch member</a>	<a href="#">2-10</a>
<a href="#">clear switch member</a>	<a href="#">2-11</a>

## show switch

Use this command to display information about one or more units in the stack.

### Syntax

```
show switch [status] [unit]
```

### Parameters

<b>status</b>	(Optional) Displays power and administrative status information for one or more units in the stack.
<i>unit</i>	(Optional) Specifies the unit(s) for which information will display.

### Defaults

If not specified, status and other configuration information about all units will be displayed.

### Mode

Switch command, read-only.

### Usage

After a stack has been configured, you can use this command to physically confirm the identity of each unit. When you enter the command with a unit number, the MGR LED of the specified switch will blink for 10 seconds. The normal state of this LED is off for member units and steady green for the manager unit.

## Examples

This example shows how to display information about all switch units in the stack:

```
B5(rw)->show switch
      Management   Preconfig   Plugged-in   Switch   Code
Switch  Status     Model ID     Model ID     Status   Version
-----
1      Mgmt Switch  B5G124-24   B5G124-24   OK       06.42.xx.xxxx
2      Stack Member B5G124-24   B5G124-24   OK       06.42.xx.xxxx
3      Stack Member B5G124-24   B5G124-24   OK       06.42.xx.xxxx
4      Stack Member B5G124-24   B5G124-24   OK       06.42.xx.xxxx
5      Stack Member B5G124-24   B5G124-24   OK       06.42.xx.xxxx
6      Stack Member B5G124-24   B5G124-24   OK       06.42.xx.xxxx
7      Stack Member B5G124-24   B5G124-24   OK       06.42.xx.xxxx
8      Stack Member B5G124-24   B5G124-24   OK       06.42.xx.xxxx
```

This example shows how to display information about switch unit 1 in the stack:

```
B5(ro)->show switch 1
Switch                               1
Management Status                   Management Switch
Hardware Management Preference       Unassigned
Admin Management Preference          Unassigned
Switch Type                           B5G124-24
Preconfigured Model Identifier        B5G124-24
Plugged-in Model Identifier           B5G124-24
Switch Status                          OK
Switch Description                    Enterasys Networks, Inc. B5 -- Model
                                       B5G124-24
Detected Code Version                 06.42.xx.xxxx
Detected Code in Flash                 03.01.20
Detected Code in Back Image            02.01.37
Up Time                               0 days 6 hrs 37 mins 54 secs
```

This example shows how to display status information for switch unit 1 in the stack:

```
B5(ro)->show switch status 1
Switch                               1
Switch Status                         Full
Admin State
Power State
Inserted Switch:
  Model Identifier                     B5G124-24
  Description                           Enterasys Networks, Inc. B5 -- Model
                                       B5G124-24
Configured Switch:
  Model Identifier                     B5G124-24
  Description                           Enterasys Networks, Inc. B5 -- Model
                                       B5G124-24
```

## show switch switchtype

Use this command to display information about supported switch types in the stack.

### Syntax

```
show switch switchtype [switchindex]
```

## Parameters

---

<i>switchindex</i>	(Optional) Specifies the switch index (SID) of the switch type to display.
--------------------	--

---

## Defaults

None.

## Mode

Switch command, read-only.

## Examples

This example shows how to display switch type information about all switches in the stack:

```
B5(su)->show switch switchtype
```

SID	Switch Model ID	Mgmt Pref	Code Version
1	B5G124-24	1	0xa08378
2	B5G124-24P2	1	0xa08378
3	B5G124-48	1	0xa08378
4	B5G124-48P2	1	0xa08378
5	B5K125-24	1	0xa08378
6	B5K125-24P2	1	0xa08378
7	B5K125-48	1	0xa08378
8	B5K125-48P2	1	0xa08378

This example shows how to display switch type information about SID1:

```
B5(su)->show switch switchtype 1
```

Switch Type	0xb5121001
Model Identifier	B5G124-24
Switch Description	Enterasys Networks, Inc. B5 -- Model B5G124-24
Management Preference	1
Expected Code Version	0xa08378

Supported Cards:

Slot	0
Card Index (CID)	1
Model Identifier	B5G124-24

## show switch stack-ports

Use this command to display various data flow and error counters on stack ports.

### Syntax

```
show switch stack-ports [unit]
```

### Parameters

---

<i>unit</i>	(Optional) Specifies the switch unit ID, an integer ranging from 1 to 8.
-------------	--

---

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to display data and error information on stack ports:

```
B5(ro)->show switch stack-ports
-----TX-----RX-----
          Data   Error          Data   Error
Switch   Stacking Rate   Rate   Total   Rate   Rate   Total
         Port   (Mb/s) (Errors/s) Errors (Mb/s) (Errors/s) Errors
-----
1        Up      0       0       0       0       0       0
         Down    0       0       0       0       0       0
```

## set switch

Use this command to assign a switch ID, to set a switch's priority for becoming the management switch if the previous management switch fails, or to change the switch unit ID for a switch in the stack.

## Syntax

```
set switch {unit [priority value / renumber newunit]}
```

## Parameters

<i>unit</i>	Specifies a unit number for the switch. Value can range from 1 to 8.
<b>priority</b> <i>value</i>	Specifies a priority value for the unit. Valid values are 1 to 15 with higher values assigning higher priority.
<b>renumber</b> <i>newunit</i>	Specifies a new number for the unit. <b>Note:</b> This number must be a previously unassigned unit ID number.

## Defaults

None.

## Mode

Switch command, read-write.

## Examples

This example shows how to assign priority 3 to switch 5:

```
B5(su)->set switch 5 priority 3
```

This example shows how to renumber switch 5 to switch 7:

```
B5(su)->set switch 5 renumber 7
```

## set switch copy-fw

Use this command to replicate the code image file from the management switch to other switch(es) in the stack.

### Syntax

```
set switch copy-fw [destination-system unit]
```

### Parameters

<b>destination-system</b> <i>unit</i>	(Optional) Specifies the unit number of unit on which to copy the management image file.
--	--

### Defaults

If **destination-system** is not specified, the management image file will be replicated to all switches in the stack.

### Mode

Switch command, read-write.

### Example

This example shows how to replicate the management image file to all switches in the stack:

```
B5(su)->set switch copy-fw
Are you sure you want to copy firmware? (y/n) y

Code transfer completed successfully.
```

## set switch description

Use this command to assign a name to a switch in the stack.

### Syntax

```
set switch description unit description
```

### Parameters

<i>unit</i>	Specifies a unit number for the switch.
<i>description</i>	Specifies a text description for the unit.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to assign the name "FirstUnit" to switch unit 1 in the stack:

```
B5(su)->set switch description 1 FirstUnit
```

## set switch movemanagement

Use this command to move management switch functionality from one switch to another.

### Syntax

```
set switch movemanagement fromunit tounit
```

### Parameters

<i>fromunit</i>	Specifies the unit number of the current management switch.
<i>tounit</i>	Specifies the unit number of the newly-designated management switch.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to move management functionality from switch 1 to switch 2:

```
B5(su)->set switch movemanagement 1 2
Moving stack management will unconfigure entire stack including all interfaces.
Are you sure you want to move stack management? (y/n) y
```

## set switch member

Use this command to add a virtual member to a stack. This allows you to preconfigure a switch before the physical device is actually added to the stack.

### Syntax

```
set switch member unit switch-id
```

### Parameters

<i>unit</i>	Specifies a unit number for the switch.
<i>switch-id</i>	Specifies a switch ID (SID) for the switch. SIDs can be displayed with the <a href="#">show switch switchtype</a> command.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

Refer to “[Creating a Virtual Switch Configuration](#)” on page 2-3 for more information about how to add a virtual switch to a stack.

## Example

This example shows how to specify a switch as unit 1 with a switch ID of 1:

```
B5(su)->set switch member 1 1
```

## clear switch member

Use this command to remove a member entry from the stack.

### Syntax

```
clear switch member unit
```

### Parameters

---

<i>unit</i>	Specifies the unit number of the switch.
-------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to remove the switch 5 entry from the stack:

```
B5(su)->clear switch member 5
```





## Basic Configuration

At startup, the Enterasys B5 switch is configured with many defaults and standard features. This chapter describes how to customize basic system settings to adapt to your work environment.

For information about...	Refer to page...
<a href="#">Quick Start Setup Commands</a>	<a href="#">3-1</a>
<a href="#">Setting User Accounts and Passwords</a>	<a href="#">3-2</a>
<a href="#">Setting Basic Switch Properties</a>	<a href="#">3-9</a>
<a href="#">Downloading a Firmware Image</a>	<a href="#">3-31</a>
<a href="#">Reviewing and Selecting a Boot Firmware Image</a>	<a href="#">3-34</a>
<a href="#">Starting and Configuring Telnet</a>	<a href="#">3-36</a>
<a href="#">Managing Switch Configuration and Files</a>	<a href="#">3-38</a>
<a href="#">Clearing and Closing the CLI</a>	<a href="#">3-48</a>
<a href="#">Resetting the Switch</a>	<a href="#">3-49</a>
<a href="#">Using and Configuring WebView</a>	<a href="#">3-51</a>
<a href="#">Gathering Technical Support Information</a>	<a href="#">3-54</a>

### Quick Start Setup Commands

The tables in this section provide a quick reference for the CLI commands needed to begin basic B5 switch operation. [Table 3-1](#) lists tasks and their associated CLI commands required for setting up the switch with the latest firmware. [Table 3-2](#) lists optional CLI commands that will help you perform additional basic configuration on the switch. Refer to the pages listed for more information about each command.

**Table 3-1 Required CLI Setup Commands**

Step	Task	CLI commands	Refer to page...
1	Set a new password.	<code>set password [username]</code>	<a href="#">3-5</a>
2	Set the switch IP address.	<code>set ip address ip-address [mask ip-mask] [gateway ip-gateway]</code>	<a href="#">3-10</a>
3	Download, activate, and verify new firmware on the switch using TFTP copy.	<code>copy tftp://tftp_server_ip_address/ filename system:image</code>	<a href="#">3-44</a>
		<code>set boot system filename</code>	<a href="#">3-35</a>
		<code>show version</code>	<a href="#">3-26</a>

**Table 3-2 Optional CLI Setup Commands**

Task	CLI commands	Refer to page...
Save the active configuration.	<code>save config</code>	3-40
Enable or disable SSH.	<code>set ssh enable   disable</code>	15-52
Enable or disable Telnet.	<code>set telnet {enable   disable} [inbound   outbound   all]</code>	3-37
Enable or disable HTTP management (WebView).	<code>set webview {enable   disable}</code>	3-52
Enable or disable SNMP port link traps.	<code>set port trap port-string {enable   disable}</code>	7-25
Set the per port broadcast limit	<code>set port broadcast port-string threshold-value</code>	7-36
Configure a VLAN.	<code>set vlan create vlan-id</code>	10-5
	<code>set port vlan port-string vlan-id modify-egress</code>	10-9
Set a Syslog server IP and severity	<code>set logging server index ip-addr ip-addr severity severity state enable</code>	10-9
Configure and enable a RADIUS server.	<code>set radius server index ip-addr port [secret-value]{realm {management-access   any   network-access}}</code>	15-4
	<code>set radius enable</code>	15-4

## Setting User Accounts and Passwords

### Purpose

To change the switch's default user login and password settings, and to add new user accounts and passwords.

### Commands

For information about...	Refer to page...
show system login	3-3
set system login	3-4
clear system login	3-4
set password	3-5
set system password length	3-6
set system password aging	3-6
set system password history	3-7
show system lockout	3-7
set system lockout	3-8

## show system login

Use this command to display user login account information.

### Syntax

```
show system login
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, super user.

### Example

This example shows how to display login account information. In this case, switch defaults have not been changed:

```
B5(su)->show system login
Password history size: 0
Password aging       : disabled

Username           Access      State
-----
admin              super-user  enabled
ro                  read-only   enabled
rw                  read-write  enabled
```

[Table 3-1](#) provides an explanation of the command output.

**Table 3-1 show system login Output Details**

Output Field	What It Displays...
Password history size	Number of previously used user login passwords that will be checked for duplication when the set password command is executed. Configured with <a href="#">set system password history (page 3-7)</a> .
Password aging	Number of days user passwords will remain valid before aging out. Configured with <a href="#">set system password aging (page 3-6)</a> .
Username	Login user names.
Access	Access assigned to this user account: super-user, read-write or read-only.
State	Whether this user account is enabled or disabled.

## set system login

Use this command to create a new user login account, or to disable or enable an existing account. The Enterasys B5 switch supports up to 16 user accounts, including the **admin** account, which cannot be deleted.

### Syntax

```
set system login username {super-user | read-write | read-only} {enable | disable}
```

### Parameters

<i>username</i>	Specifies a login name for a new or existing user. This string can be a maximum of 80 characters, although a maximum of 16 characters is recommended for proper viewing in the <b>show system login</b> display.
<b>super-user</b>   <b>read-write</b>   <b>read-only</b>	Specifies the access privileges for this user.
<b>enable</b>   <b>disable</b>	Enables or disables the user account.

### Defaults

None.

### Mode

Switch command, super user.

### Usage

Login accounts, including the **admin** user account, can be locked out after multiple failed attempts to log in to the system. Refer to “[show system lockout](#)” on page 3-7 and “[set system lockout](#)” on page 3-8 for more information about lockout parameters.

If the **admin** user account has been locked out, you must wait until the configured lockout time period has expired or you can power cycle the switch to reboot it, which will re-enable the **admin** user account.

### Example

This example shows how to enable a new user account with the login name “netops” with super user access privileges:

```
B5(su)->set system login netops super-user enable
```

## clear system login

Use this command to remove a local login user account.

### Syntax

```
clear system login username
```

### Parameters

<i>username</i>	Specifies the login name of the account to be cleared. <b>Note:</b> The default admin (su) account cannot be deleted.
-----------------	--

## Defaults

None.

## Mode

Switch command, super user.

## Example

This example shows how to remove the “netops” user account:

```
B5(su)->clear system login netops
```

# set password

Use this command to change system default passwords or to set a new login password on the CLI.

## Syntax

```
set password [username]
```

## Parameters

---

<i>username</i>	(Only available to users with super-user access.) Specifies a system default or a user-configured login account name. By default, the Enterasys B5 switch provides the following account names:  <b>ro</b> for Read-Only access.  <b>rw</b> for Read-Write access.  <b>admin</b> for Super User access. (This access level allows Read-Write access to all modifiable parameters, including user accounts.)
-----------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

Switch command, super-user.

## Usage

Read-Write users can change their own passwords.

Super Users (Admin) can change any password on the system.

If you forget the password for the **admin** user account, you can reset the password to the default password value by pressing the password reset button on the switch.

## Examples

This example shows how a super-user would change the Read-Write password from the system default (blank string):

```
B5(su)->set password rw
Please enter new password: *****
Please re-enter new password: *****
```

```
Password changed.  
B5(su)->
```

This example shows how a user with Read-Write access would change his password:

```
B5(rw)->set password  
Please enter old password: *****  
Please enter new password: *****  
Please re-enter new password: *****  
Password changed.  
B5(rw)->
```

## set system password length

Use this command to set the minimum user login password length.

### Syntax

```
set system password length characters
```

### Parameters

---

<i>characters</i>	Specifies the minimum number of characters for a user account password. Valid values are 0 to 40.
-------------------	---

---

### Defaults

None.

### Mode

Switch command, super user.

### Example

This example shows how to set the minimum system password length to 8 characters:

```
B5(su)->set system password length 8
```

## set system password aging

Use this command to set the number of days user passwords will remain valid before aging out, or to disable user account password aging.

### Syntax

```
set system password aging {days | disable}
```

### Parameters

---

<i>days</i>	Specifies the number of days user passwords will remain valid before aging out. Valid values are 1 to 365.
<b>disable</b>	Disables password aging.

---

### Defaults

None.

## Mode

Switch command, super user.

## Example

This example shows how to set the system password age time to 45 days:

```
B5(su)->set system password aging 45
```

# set system password history

Use this command to set the number of previously used user login passwords that will be checked for password duplication. This prevents duplicate passwords from being entered into the system with the **set password** command.

## Syntax

```
set system password history size
```

## Parameters

---

<i>size</i>	Specifies the number of passwords checked for duplication. Valid values are 0 to 10.
-------------	--

---

## Defaults

None.

## Mode

Switch command, super user.

## Example

This example shows how to configure the system to check the last 10 passwords for duplication

```
B5(su)->set system password history 10
```

# show system lockout

Use this command to display settings for locking out users after failed attempts to log in to the system.

## Syntax

```
show system lockout
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, super user.

## Example

This example shows how to display user lockout settings. In this case, switch defaults have not been changed:

```
B5(su)->show system lockout
Lockout attempts: 3
Lockout time:      15 minutes.
```

[Table 3-3](#) provides an explanation of the command output. These settings are configured with the **set system lockout** command (“[set system lockout](#)” on page 3-8).

**Table 3-3 show system lockout Output Details**

Output Field	What It Displays...
Lockout attempts	Number of failed login attempts allowed before a read-write or read-only user's account will be disabled.
Lockout time	Number of minutes the default admin user account will be locked out after the maximum login attempts.

## set system lockout

Use this command to set the number of failed login attempts before locking out (disabling) a read-write or read-only user account, and the number of minutes to lockout the default admin super user account after maximum login attempts.

### Syntax

```
set system lockout {[attempts attempts] [time time]}
```

### Parameters

<b>attempts</b> <i>attempts</i>	Specifies the number of failed login attempts allowed before a read-write or read-only user's account will be disabled. Valid values are 1 to 10. The default value is 3 attempts.
<b>time</b> <i>time</i>	Specifies the number of minutes the default admin user account will be locked out after the maximum login attempts. Valid values are 0 to 60. The default value is 15 minutes.

### Defaults

- 3 attempts
- 15 minutes

### Mode

Switch command, super user.

### Usage

Once a user account is locked out, it can only be re-enabled by a super user with the **set system login** command ([page 3-4](#)).

If the default admin super user account has been locked out, you can wait until the lock out time has expired or you can reset the switch in order to re-enable the admin account.



## Example

This example shows how to set login attempts to 5 and lockout time to 30 minutes:

```
B5(su)->set system lockout attempts 5 time 30
```

# Setting Basic Switch Properties

## Purpose

To display and set the system IP address and other basic system (switch) properties.

## Commands

For information about...	Refer to page...
show ip address	<a href="#">3-10</a>
set ip address	<a href="#">3-10</a>
clear ip address	<a href="#">3-11</a>
show ip protocol	<a href="#">3-12</a>
set ip protocol	<a href="#">3-12</a>
show ip route	<a href="#">3-13</a>
show system	<a href="#">3-13</a>
show system hardware	<a href="#">3-15</a>
show system utilization	<a href="#">3-16</a>
set system utilization	<a href="#">3-17</a>
clear system utilization	<a href="#">3-17</a>
set system temperature	<a href="#">3-18</a>
clear system temperature	<a href="#">3-19</a>
show time	<a href="#">3-20</a>
set time	<a href="#">3-20</a>
show summertime	<a href="#">3-21</a>
set summertime	<a href="#">3-21</a>
set summertime date	<a href="#">3-22</a>
set summertime recurring	<a href="#">3-22</a>
clear summertime	<a href="#">3-23</a>
set prompt	<a href="#">3-24</a>
show banner motd	<a href="#">3-24</a>
set banner motd	<a href="#">3-25</a>
clear banner motd	<a href="#">3-25</a>
show version	<a href="#">3-26</a>

For information about...	Refer to page...
set system name	<a href="#">3-27</a>
set system location	<a href="#">3-27</a>
set system contact	<a href="#">3-28</a>
set width	<a href="#">3-28</a>
set length	<a href="#">3-29</a>
show logout	<a href="#">3-29</a>
set logout	<a href="#">3-30</a>
show console	<a href="#">3-30</a>
set console baud	<a href="#">3-31</a>

## show ip address

Use this command to display the system IP address and subnet mask.

### Syntax

```
show ip address
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the system IP address and subnet mask:

```
B5(su)->show ip address
```

Name	Address	Mask
-----	-----	-----
host	10.42.13.20	255.255.0.0

## set ip address

Use this command to set the system IP address, subnet mask and default gateway.



**Note:** The B5 does not support the ability for a user to configure the host's gateway to be a local routed interface IP. The host's gateway must exist on a different device in the network if one is configured.

### Syntax

```
set ip address ip-address [mask ip-mask] [gateway ip-gateway]
```

## Parameters

<i>ip-address</i>	Sets the IP address for the system. For Enterasys B5 systems, this is the IP address of the management switch as described in <a href="#">“About Enterasys B5 Switch Operation in a Stack”</a> on page 2-1.
<b>mask</b> <i>ip-mask</i>	(Optional) Sets the system’s subnet mask.
<b>gateway</b> <i>ip-gateway</i>	(Optional) Sets the system’s default gateway (next-hop device).

## Defaults

If not specified, *ip-mask* will be set to the natural mask of the *ip-address* and *ip-gateway* will be set to the *ip-address*.

## Mode

Switch command, read-write.

## Usage

Parameters must be entered in the order shown (host IP, then mask, then gateway) for the command to be accepted.

## Example

This example shows how to set the system IP address to 10.1.10.1 with a mask of 255.255.128.0:

```
B5(su)->set ip address 10.1.10.1 mask 255.255.128.0
```

# clear ip address

Use this command to clear the system IP address.

## Syntax

```
clear ip address
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear the system IP address:

```
B5(rw)->clear ip address
```

## show ip protocol

Use this command to display the method used to acquire a network IP address for switch management.

### Syntax

```
show ip protocol
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the method used to acquire a network IP address:

```
B5(su)->show ip protocol
System IP address acquisition method: dhcp
```

## set ip protocol

Use this command to specify the protocol used to acquire a network IP address for switch management.

### Syntax

```
set ip protocol {bootp | dhcp | none}
```

### Parameters

<b>bootp</b>	Selects BOOTP as the protocol to use to acquire the system IP address.
<b>dhcp</b>	Selects DHCP as the protocol to use to acquire the system IP address.
<b>none</b>	No protocol will be used to acquire the system IP address.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the method used to acquire a network IP address to DHCP.

```
B5(su)->set ip protocol dhcp
```

## show ip route

Use this command to display the IP route table.

### Syntax

```
show ip route
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read only.

### Example

This example shows the output of this command.

```
B5(ro)->show ip route
```

```

INET route table
Destination                Gateway                Flags    Use    If    Metric
0.0.0.0/0                  192.168.0.1           UG       13    host    5
127.0.0.1                  127.0.0.1             UH       0     lo0     5
192.168.0.0/24             127.0.0.1             UC       2     host    5
192.168.0.101              127.0.0.1             UH       0     lo0     5

```

## show system

Use this command to display system information, including contact information, power and fan tray status and uptime.

### Syntax

```
show system
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display system information:

```
B5(su)->show system
```

```

System contact:
System location:
System name:

Switch 1
-----
PS1-Status                PS2-Status
-----
Ok                        Not Installed and/or Not Operating

Fan Group 1-Status        Fan Group 2-Status
-----
Ok                        Ok

Fan Group 3-Status        Fan Group 4-Status
-----
Ok                        Not Installed

Temp-Alarm
-----
off
Temp alarm max threshold: 100%
Temp alarm trap: disabled
Temp alarm syslog: disabled

Thermal Sensor            Thermal Threshold
-----
Power Supply              92%
System                    91%

Uptime d,h:m:s  Logout
-----
1,0:18:54      0 min
    
```

**Table 3-4 show system Output Details**

Output	What It Displays...
System contact	Contact person for the system. Default of a blank string can be changed with the <b>set system contact</b> command (" <a href="#">set system contact</a> " on page 3-28).
System location	Where the system is located. Default of a blank string can be changed with the <b>set system location</b> command (" <a href="#">set system location</a> " on page 3-27).
System name	Name identifying the system. Default of a blank string can be changed with the <b>set system name</b> command (" <a href="#">set system name</a> " on page 3-27).
Switch x	Indicates the switch position in the stack. When multiple switches are in a stack, information for each switch is displayed.
PS1-Status	Operational status for the primary power supply.
PS2-Status	Operational status for the secondary power supply, if installed.
Fanx-Status	Operational status of the fan(s).
Temp-Alarm	Indicates status of temperature alarm — on, off. The status will show NA (not available) on switches that do not support this functionality.
Temp alarm max threshold	The temperature alarm threshold expressed as a percentage of the maximum rated. The default value is 100%.
Temp alarm trap	Indicates whether the sending of temperature alarm traps is enabled or disabled. The default is disabled.

**Table 3-4 show system Output Details (Continued)**

Output	What It Displays...
Temp alarm syslog	Indicates whether temperature alarm syslog messages are enabled or disabled. The default is disabled.
Thermal Sensor/Thermal Threshold	Lists the type of thermal sensor (power supply, system) and the percentage of thermal threshold reached for that sensor. The status will show NA (not available) on switches that do not support this functionality.
Uptime d,h:m:s	System uptime.
Logout	Time an idle console or Telnet CLI session will remain connected before timing out. Default of 5 minutes can be changed with the <b>set logout</b> command (“ <a href="#">set logout</a> ” on page 3-30).

## show system hardware

Use this command to display the system’s hardware configuration.

### Syntax

```
show system hardware
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the system’s hardware configuration. Please note that the information you see displayed may differ from this example.

```
B5(su)->show system hardware
  SLOT 1 HARDWARE INFORMATION
  -----
  Model:
  Serial Number:          777777777777
  Vendor ID:              0xbc00
  Base MAC Address:      00:11:88:B1:76:C0
  Hardware Version:      BCM56514 REV 1
  FirmWare Version:      01.00.00.0052
  Boot Code Version:     01.00.42
```

## show system utilization

Use this command to display detailed information about the processor running on the switch, or the overall memory usage of the Flash and SDRAM storage devices on the unit, or the processes running on the switch. Only the memory usage in the master unit of a stack is shown.

### Syntax

```
show system utilization {cpu | storage | process}
```

### Parameters

<b>cpu</b>	Display information about the processor running on the switch.
<b>storage</b>	Display information about the overall memory usage on the switch.
<b>process</b>	Display information about the processes running on the switch.

### Defaults

None.

### Mode

Switch command, read-only.

### Examples

This example shows how to display the system's CPU utilization:

```
B5(ro)->show system utilization cpu
```

```
CPU Utilization Threshold Traps enable: Threshold = 80.0%
```

```
Total CPU Utilization:
```

Switch	CPU	5 sec	1 min	5 min
1	1	50%	49%	49%

This example shows how to display the system's overall memory usage:

```
B5(ro)->show system utilization storage
```

```
Storage Utilization:
```

Type	Description	Size(Kb)	Available (Kb)
RAM	RAM device	262144	97173
Flash	Images, Config, Other	31095	8094

This example shows how to display information about the processes running on the system. Only partial output is shown.

```
B5(ro)->show system utilization process
```

```
Switch:1 CPU:1
```

TID	Name	5Sec	1Min	5Min
c157930	ipMapForwardingTask	3.60%	3.02%	3.48%
cc70000	RMONTask	0.00%	0.00%	0.00%
ccb0b60	SNMPTask	34.80%	34.06%	31.78%
d4847a0	tEmWeb	0.00%	0.03%	0.01%



d4ca360	hapiRxTask	3.20%	4.80%	5.00%
dec8600	lvl7TaskUtilMonitorTas	0.40%	0.40%	0.40%
eb74120	bcmRX	2.00%	2.91%	4.48%
eb7fbc8	bcmLINK.0	0.40%	0.22%	0.32%
f00c9a0	bcmTX	0.00%	0.33%	0.53%
f027648	bcmCNTR.0	0.00%	0.00%	0.03%
f034858	bcmL2X.0	0.00%	0.02%	0.04%

## set system utilization

Use this command to set the threshold for sending CPU utilization notification messages.

### Syntax

```
set system utilization threshold threshold
```

### Parameters

---

<b>threshold</b> <i>threshold</i>	Specifies a threshold value in 1/10 of a percent. Valid range is 1 to 1000. A value of 0 disables utilization notification messages.
-----------------------------------	--

---

### Defaults

The default threshold value is 80%.

### Mode

Switch command, read-write.

### Usage

This command sets the percentage of system CPU utilization that will cause a trap notification to be sent. After the threshold has been exceeded, additional notifications will be sent once a minute until the utilization has dropped back below the threshold.

### Example

This example sets the CPU utilization threshold to 75%.

```
B5(rw)->set system utilization threshold 750
```

## clear system utilization

Use this command to reset the CPU utilization threshold to the default of 80%.

### Syntax

```
clear system utilization
```

### Parameters

None.

### Defaults

The default threshold value is 80%.

## Mode

Switch command, read-write.

## Example

This example resets the CPU utilization threshold to the default.

```
B5(rw)->show system utilization cpu
```

```
CPU Utilization Threshold Traps enable: Threshold = 75.0%
```

```
Total CPU Utilization:
```

Switch	CPU	5 sec	1 min	5 min
1	1	10%	10%	10%

```
B5(rw)->clear system utilization
```

```
B5(rw)->show system utilization cpu
```

```
CPU Utilization Threshold Traps enable: Threshold = 80.0%
```

```
Total CPU Utilization:
```

Switch	CPU	5 sec	1 min	5 min
1	1	14%	11%	10%

# set system temperature

Use this command to set the system high temperature threshold limit and the high temperature alert parameters, on the platforms that support this feature.

## Syntax

```
set system temperature {[syslog enable | disable] [trap enable | disable]
[overtemp-threshold value]}
```

## Parameters

<b>syslog enable   disable</b>	Enables or disables logging high temperature alerts to the system log when the system transitions into an alarm state.
<b>trap enable   disable</b>	Enables or disables sending high temperature alerts by means of SNMP traps when the system transitions into an alarm state.
<b>overtemp-threshold value</b>	Sets the thermal threshold as a percentage of the maximum rated for the specific platform. Value can range from 0 to 100%.

## Defaults

Syslog alerts are disabled by default.

Trap alerts are disabled by default.

Overtemp threshold is 100% by default.

## Mode

Switch command, read-write.

## Usage

On the platforms that support this feature, temperature sensors are located in several different locations within the device. Threshold calibrations have been calculated separately for each platform. The thermal overtemp threshold is the high-water mark that, when reached, triggers an alert to warn the system administrator that the device is operating at high temperatures.

When a high temperature alert condition occurs, the CPU LED on the front panel of the switch will flash red. In addition, if enabled, a syslog message will be logged and/or an SNMP trap will be sent.

The values set with this command can be viewed with the **show system** command.

## Example

The following example enables sending SNMP traps and sets the overtemp threshold to 60%.

```
B5(su)->set system temperature trap enable overtemp-threshold 60
```

# clear system temperature

Use this command to reset system high temperature parameters to their default values, on the platforms that support this feature.

## Syntax

```
clear system temperature
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command resets all the high temperature parameters to their default values:

- Syslog alerts are disabled by default.
- Trap alerts are disabled by default.
- Overtemp threshold is 100% by default.

## Example

This example resets all high temperature parameters to their defaults.

```
B5(su)->clear system temperature
```

## show time

Use this command to display the current time of day in the system clock.

### Syntax

```
show time
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the current time. The output shows the day of the week, month, day, and the time of day in hours, minutes, and seconds and the year:

```
B5(su)->show time
THU SEP 05 09:21:57 2002
```

## set time

Use this command to change the time of day on the system clock.

### Syntax

```
set time [mm/dd/yyyy] [hh:mm:ss]
```

### Parameters

---

[mm/dd/yyyy]	Sets the time in:
[hh:mm:ss]	month, day, year and/or
	24-hour format
	At least one set of time parameters must be entered.

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the system clock to 7:50 a.m:

```
B5(su)->set time 7:50:00
```

## show summertime

Use this command to display daylight savings time settings.

### Syntax

```
show summertime
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display daylight savings time settings:

```
B5(su)->show summertime
Summertime is Enabled and set to ''
Start : SUN MAR 14 02:00:00
End   : SUN NOV  7 02:00:00
Offset: 60 minutes (1 hours 0 minutes)
Recurring: yes, starting at 2:00 of the second Sunday of March and ending at 2:00
of the first Sunday of November
```

## set summertime

Use this command to enable or disable the daylight savings time function.

### Syntax

```
set summertime {enable | disable} [zone]
```

### Parameters

<b>enable   disable</b>	Enables or disables the daylight savings time function.
<i>zone</i>	(Optional) Applies a name to the daylight savings time settings.

### Defaults

If a *zone* name is not specified, none will be applied.

### Mode

Switch command, read-only.

### Example

This example shows how to enable daylight savings time function:

```
B5(su)->set summertime enable
```

## set summertime date

Use this command to configure specific dates to start and stop daylight savings time. These settings will be non-recurring and will have to be reset annually.

### Syntax

```
set summertime date start_month start_date start_year start_hr_min end_month
end_date end_year end_hr_min [offset_minutes]
```

### Parameters

<i>start_month</i>	Specifies the month of the year to start daylight savings time.
<i>start_date</i>	Specifies the day of the month to start daylight savings time.
<i>start_year</i>	Specifies the year to start daylight savings time.
<i>start_hr_min</i>	Specifies the time of day to start daylight savings time. Format is hh:mm.
<i>end_month</i>	Specifies the month of the year to end daylight savings time.
<i>end_date</i>	Specifies the day of the month to end daylight savings time.
<i>end_year</i>	Specifies the year to end daylight savings time.
<i>end_hr_min</i>	Specifies the time of day to end daylight savings time. Format is hh:mm.
<i>offset_minutes</i>	(Optional) Specifies the amount of time in minutes to offset daylight savings time from the non-daylight savings time system setting. Valid values are 1 - 1440.

### Defaults

If an *offset* is not specified, none will be applied.

### Mode

Switch command, read-write.

### Example

This example shows how to set a daylight savings time start date of April 4, 2004 at 2 a.m. and an ending date of October 31, 2004 at 2 a.m. with an offset time of one hour:

```
B5(su)->set summertime date April 4 2004 02:00 October 31 2004 02:00 60
```

## set summertime recurring

Use this command to configure recurring daylight savings time settings. These settings will start and stop daylight savings time at the specified day of the month and hour each year and will not have to be reset annually.

### Syntax

```
set summertime recurring start_week start_day start_month start_hr_min end_week
end_day end_month end_hr_min [offset_minutes]
```

## Parameters

<i>start_week</i>	Specifies the week of the month to restart daylight savings time. Valid values are: first, second, third, fourth, and last.
<i>start_day</i>	Specifies the day of the week to restart daylight savings time.
<i>start_hr_min</i>	Specifies the time of day to restart daylight savings time. Format is hh:mm.
<i>end_week</i>	Specifies the week of the month to end daylight savings time.
<i>end_day</i>	Specifies the day of the week to end daylight savings time.
<i>end_hr_min</i>	Specifies the time of day to end daylight savings time. Format is hh:mm.
<i>offset_minutes</i>	(Optional) Specifies the amount of time in minutes to offset daylight savings time from the non-daylight savings time system setting. Valid values are 1 - 1440.

## Defaults

If an *offset* is not specified, none will be applied.

## Mode

Switch command, read-write.

## Example

This example shows how set daylight savings time to recur starting on the first Sunday of April at 2 a.m. and ending the last Sunday of October at 2 a.m. with an offset time of one hour:

```
B5(su)->set summertime recurring first Sunday April 02:00 last Sunday October
02:00 60
```

## clear summertime

Use this command to clear the daylight savings time configuration.

## Syntax

```
clear summertime
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear the daylight savings time configuration:

```
B5(su)->clear summertime
```

## set prompt

Use this command to modify the command prompt.

### Syntax

```
set prompt prompt_string
```

### Parameters

---

<i>prompt_string</i>	Specifies a text string for the command prompt.
----------------------	---

**Note:** A prompt string containing a space in the text must be enclosed in quotes as shown in the example below.

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the command prompt to Switch 1:

```
B5(su)->set prompt "Switch 1"  
Switch 1(su)->
```

## show banner motd

Use this command to show the banner message of the day that will display at session login.

### Syntax

```
show banner motd
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the banner message of the day:

```
B5(rw)->show banner motd  
      This system belongs to XYZ Corporation.  
Use of this system is strictly limited to authorized personnel.
```



## set banner motd

Use this command to set the banner message of the day displayed at session login.



**Note:** Banner message text must be enclosed in beginning and ending double quotation marks. The message itself cannot contain any additional double quotation marks.

### Syntax

```
set banner motd message
```

### Parameters

<i>message</i>	Specifies a message of the day. This is a text string that needs to be in double quotes if any spaces are used. Use a \n for a new line and \t for a tab (eight spaces).
----------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the message of the day banner to read: "This system belongs to XYZ Corporation. Use of this system is strictly limited to authorized personnel."

```
B5(rw)->set banner motd "\tThis system belongs to XYZ Corporation.\nUse of this system is strictly limited to authorized personnel."
```

## clear banner motd

Use this command to clear the banner message of the day displayed at session login to a blank string.

### Syntax

```
clear banner motd
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to clear the message of the day banner to a blank string:

```
B5(rw)->clear banner motd
```

## show version

Use this command to display hardware and firmware information. Refer to [“Downloading a Firmware Image”](#) on page 3-31 for instructions on how to download a firmware image.

### Syntax

```
show version
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display version information. Please note that you may see different information displayed, depending on the type of hardware.

```
B5(su)->show version
Copyright (c) 2007 by Enterasys Networks, Inc.

Model          Serial #          Versions
-----
B5G124-48P     001188021035    Hw:BCM5665 REV 17
                Bp:01.00.29
                Fw:6.42.xx.xxxx
                BuFw:03.01.13
                PoE:500_3
```

[Table 3-5](#) provides an explanation of the command output.

**Table 3-5 show version Output Details**

Output Field	What It Displays...
Model	Switch's model number.
Serial #	Serial number of the switch.
Versions	<ul style="list-style-type: none"> <li>Hw: Hardware version number.</li> <li>Bp: BootPROM version.</li> <li>Fw: Current firmware version number.</li> <li>BuFw: Backup firmware version number.</li> <li>PoE: Power over Ethernet driver version. (Displays only for PoE switches.)</li> </ul>

## set system name

Use this command to configure a name for the system.

### Syntax

```
set system name [string]
```

### Parameters

---

<i>string</i>	(Optional) Specifies a text string that identifies the system. <b>Note:</b> A name string containing a space in the text must be enclosed in quotes as shown in the example below.
---------------	---

---

### Defaults

If *string* is not specified, the system name will be cleared.

### Mode

Switch command, read-write.

### Example

This example shows how to set the system name to Information Systems:

```
B5(su)->set system name "Information Systems"
```

## set system location

Use this command to identify the location of the system.

### Syntax

```
set system location [string]
```

### Parameters

---

<i>string</i>	(Optional) Specifies a text string that indicates where the system is located. <b>Note:</b> A location string containing a space in the text must be enclosed in quotes as shown in the example below.
---------------	---

---

### Defaults

If *string* is not specified, the location name will be cleared.

### Mode

Switch command, read-write.

### Example

This example shows how to set the system location string:

```
B5(su)->set system location "Bldg N32-04 Closet 9"
```

## set system contact

Use this command to identify a contact person for the system.

### Syntax

```
set system contact [string]
```

### Parameters

---

<i>string</i>	(Optional) Specifies a text string that contains the name of the person to contact for system administration.
---------------	---

**Note:** A contact string containing a space in the text must be enclosed in quotes as shown in the example below.

---

### Defaults

If *string* is not specified, the contact name will be cleared.

### Mode

Switch command, read-write.

### Example

This example shows how to set the system contact string:

```
B5(su)->set system contact "Joe Smith"
```

## set width

Use this command to set the number of columns for the terminal connected to the switch's console port.

### Syntax

```
set width screenwidth [default]
```

### Parameters

---

<i>screenwidth</i>	Sets the number of terminal columns. Valid values are 50 to 150.
<i>default</i>	(Optional) Makes this setting persistent for all future sessions (written to NV-RAM).

---

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The number of rows of CLI output displayed is set using the **set length** command as described in "[set length](#)" on page 3-29.

## Example

This example shows how to set the terminal columns to 50:

```
B5(su)->set width 50
```

## set length

Use this command to set the number of lines the CLI will display. This command is persistent (written to NV-RAM).

### Syntax

```
set length screenlength
```

### Parameters

<i>screenlength</i>	Sets the number of lines in the CLI display. Valid values are 0, which disables the scrolling screen feature described in <a href="#">“Displaying Scrolling Screens”</a> on page 1-9, and from 5 to 512.
---------------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the terminal length to 50:

```
B5(su)->set length 50
```

## show logout

Use this command to display the time (in seconds) an idle console or Telnet CLI session will remain connected before timing out.

### Syntax

```
show logout
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

## Example

This example shows how to display the CLI logout setting:

```
B5(su)->show logout
Logout currently set to: 10 minutes.
```

## set logout

Use this command to set the time (in minutes) an idle console or Telnet CLI session will remain connected before timing out.

### Syntax

```
set logout timeout
```

### Parameters

---

<i>timeout</i>	Sets the number of minutes the system will remain idle before timing out.
----------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the system timeout to 10 minutes:

```
B5(su)->set logout 10
```

## show console

Use this command to display console settings.

### Syntax

```
show console [baud] [bits] [flowcontrol] [parity] [stopbits]
```

### Parameters

---

<b>baud</b>	(Optional) Displays the input/output baud rate.
<b>bits</b>	(Optional) Displays the number of bits per character.
<b>flowcontrol</b>	(Optional) Displays the type of flow control.
<b>parity</b>	(Optional) Displays the type of parity.
<b>stopbits</b>	(Optional) Displays the number of stop bits.

---

### Defaults

If no parameters are specified, all settings will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display all console settings:

```
B5(su)->show console
Baud      Flow      Bits  StopBits  Parity
-----  -
9600     Disable   8      1          none
```

# set console baud

Use this command to set the console port baud rate.

## Syntax

```
set console baud rate
```

## Parameters

<i>rate</i>	Sets the console baud rate. Valid values are: 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200.
-------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to set the console port baud rate to 19200:

```
B5(su)->set console baud 19200
```

# Downloading a Firmware Image

You can upgrade the operational firmware in the Enterasys B5 switch without physically opening the switch or being in the same location. There are two ways to download firmware to the switch:

- Via TFTP download. This procedure uses a TFTP server connected to the network and downloads the firmware using the TFTP protocol. For details on how to perform a TFTP download using the **copy** command, refer to “[copy](#)” on page 3-44. For information on setting TFTP timeout and retry parameters, refer to “[set tftp timeout](#)” on page 3-46 and “[set tftp retry](#)” on page 3-47.
- Via the serial (console) port. This procedure is an out-of-band operation that copies the firmware through the serial port to the switch. It should be used in cases when you cannot connect the switch to perform the in-band **copy** download procedure via TFTP. Serial console download has been successfully tested with the following applications:
  - HyperTerminal Copyright 1999
  - Tera Term Pro Version 2.3

Any other terminal applications may work but are not explicitly supported.

The B5 switch allows you to download and store dual images. The backup image can be downloaded and selected as the startup image by using the commands described in this section.

## Downloading from a TFTP Server

To perform a TFTP download, proceed as follows:

1. If you have not already done so, set the switch's IP address using the **set ip address** command as detailed in "set ip address" on page 3-10.
2. Download a new image file using the **copy** command as detailed in "copy" on page 3-44.

## Downloading via the Serial Port

To download switch firmware via the serial (console) port, proceed as follows:

1. With the console port connected, power up the switch. A message similar to the following displays:

```
Version 01.00.29 05-09-2005

Computing MD5 Checksum of operational code...
Select an option. If no selection in 2 seconds then
operational code will start.

1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2

Password: *****
```

2. Before the boot up completes, type **2** to select "Start Boot Menu". Use "administrator" for the Password.



**Note:** The "Boot Menu" password "administrator" can be changed using boot menu option 11.

```
Boot Menu Version 01.00.29 05-09-2005

Options available
1 - Start operational code
2 - Change baud rate
3 - Retrieve event log using XMODEM (64KB).
4 - Load new operational code using XMODEM
5 - Display operational code vital product data
6 - Run Flash Diagnostics
7 - Update Boot Code
8 - Delete operational code
9 - Reset the system
10 - Restore Configuration to factory defaults (delete config files)
11 - Set new Boot Code password
[Boot Menu] 2
```

3. Type **2**. The following baud rate selection screen displays:



- 1 - 1200
- 2 - 2400
- 3 - 4800
- 4 - 9600
- 5 - 19200
- 6 - 38400
- 7 - 57600
- 8 - 115200
- 0 - no change

4. Type **8** to set the switch baud rate to 115200. The following message displays:  
Setting baud rate to 115200, you must change your terminal baud rate.
5. Set the terminal baud rate to **115200** and press ENTER.
6. From the boot menu options screen, type **4** to load new operational code using XMODEM. When the XMODEM transfer is complete, the following message and header information will display:

```
[Boot Menu] 4
Ready to receive the file with XMODEM/CRC....
Ready to RECEIVE File xcode.bin in binary mode
Send several Control-X characters to cCKCKCKCKCKCKCK

XMODEM transfer complete, checking CRC....
Verified operational code CRC.

The following Enterasys Header is in the image:

MD5 Checksum.....fe967970996c4c8c43a10cd1cd7be99a
Boot File Identifier.....0x0517
Header Version.....0x0100
Image Type.....0x82
Image Offset.....0x004d
Image length.....0x006053b3
Ident Strings Length.....0x0028
Ident Strings.....
<platform specific>
Image Version Length.....0x7
Image Version Bytes.....0x30 0x2e 0x35 0x2e 0x30 0x2e 0x34 (0.5.0.4)
```

7. From the boot menu options screen, type **2** to display the baud rate selection screen again.
8. Type **4** set the switch baud rate to **9600**. The following message displays:  
Setting baud rate to 9600, you must change your terminal baud rate.
9. Set the terminal baud rate to **9600** and press ENTER.
10. From the boot menu options screen, type **1** to start the new operational code. A message similar to the following displays:

```
Operational Code Date: Tue Jun 29 08:34:05 2004
Uncompressing.....
```

## Reverting to a Previous Image

In the event that you need to downgrade to a previous version of code, you can do so by completing the following steps as described in this chapter.



**Caution:** Before reverting to a previous image, always back up your configuration by saving it to a file (**show config outfile** on page 3-43). You can then copy the file to a remote location (**copy** on page 3-44).



**Note:** You will not be able to perform these steps remotely unless you have remote console support.

1. Save your running configuration with the **save config** command.
2. Make a copy of the current configuration with the **show config outfile configs/filename** command. Use the **dir** command to confirm that the file was created.
3. If desired, copy the file to a remote TFTP server with the **copy** command:  
`copy configs/filename tftp://server_ipaddr/filename`
4. Load your previous version of code on the device, as described in “[Downloading a Firmware Image](#)” (page 3-31).
5. Set this older version of code to be the boot code with the **set boot system** command (page 3-35). When the system asks if you want to reset the device, specify no (**n**).
6. Reload the saved configuration onto the device with the **configure** command, described on page 3-44.
7. Reboot the system using the **reset** command (page 3-50).



**Caution:** If you do not follow the steps above, you may lose remote connectivity to the switch.

## Reviewing and Selecting a Boot Firmware Image

### Purpose

To display and set the image file the switch loads at startup. The B5 switch allows you to download and store a backup image, which can be selected as the startup image by using the commands described in this section.

### Commands

For information about...	Refer to page...
show boot system	<a href="#">3-34</a>
set boot system	<a href="#">3-35</a>

### show boot system

Use this command to display the firmware image the switch loads at startup.

#### Syntax

```
show boot system
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to display the switch's boot firmware image:

```
B5(su)->show boot system
Current system image to boot: bootfile
```

# set boot system

Use this command to set the firmware image the switch loads at startup.

## Syntax

```
set boot system filename
```

## Parameters

<i>filename</i>	Specifies the name of the firmware image file.
-----------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command allows you to set the firmware image to be loaded at startup. You can choose to reset the system to use the new firmware image immediately, or you can choose to only specify the new image to be loaded the next time the switch is rebooted.

You can use the **dir** command to display the "Active" image and the "Boot" image, which will be the image loaded at the next system reboot.



**Note:** If you are changing the firmware image to a version *earlier* than the current version, refer to ["Reverting to a Previous Image"](#) on page 3-33 for the correct steps to follow.

## Example

This example shows how to set the boot firmware image file to be used at the next reboot of the system, by answering "n" to the prompt. The **dir** command is then executed to display the Active and Boot images.

```
B5(su)->set boot system b5_06.42.03.0007
This command can optionally reset the system to boot the new image.
```

```

Do you want to reset now (y/n) [n]?n

B5(su)->dir
Images:
=====
Filename:      b5-series_06.42.00.0026 (Active)
Version:      06.42.00.0026
Size:         9405440 (bytes)
Date:         Fri Jul 18 12:48:35 2008
Checksum:     f1626ccf10d8f48cd6c3e79ab602342a
Compatibility: <platform specific>

Filename:      b5-series_06.42.03.0007 (Boot)
Version:      06.42.03.0007
Size:         8290304 (bytes)
Date:         Fri May 9 11:35:27 2008
Checksum:     9f820d79239f10890442f8ff1f2bc914
Compatibility: <platform specific>

```

## Starting and Configuring Telnet

### Purpose

To enable or disable Telnet, and to start a Telnet session to a remote host. The Enterasys B5 switch allows a total of four inbound and / or outbound Telnet session to run simultaneously.

### Commands

For information about...	Refer to page...
show telnet	<a href="#">3-36</a>
set telnet	<a href="#">3-37</a>
telnet	<a href="#">3-37</a>

### show telnet

Use this command to display the status of Telnet on the switch.

#### Syntax

```
show telnet
```

#### Parameters

None.

#### Defaults

None.

#### Mode

Switch command, read-only.

## Example

This example shows how to display Telnet status:

```
B5(su)->show telnet
Telnet inbound is currently: ENABLED
Telnet outbound is currently: ENABLED
```

## set telnet

Use this command to enable or disable Telnet on the switch.

### Syntax

```
set telnet {enable | disable} [inbound | outbound | all]
```

### Parameters

<b>enable   disable</b>	Enables or disables Telnet services.
<b>inbound   outbound   all</b>	(Optional) Specifies inbound service (the ability to Telnet to this switch), outbound service (the ability to Telnet to other devices), or all (both inbound and outbound).

### Defaults

If not specified, both inbound and outbound Telnet service will be enabled.

### Mode

Switch command, read-write.

### Example

This example shows how to disable inbound and outbound Telnet services:

```
B5(su)->set telnet disable all
Disconnect all telnet sessions and disable now (y/n)? [n]: y
All telnet sessions have been terminated, telnet is now disabled.
```

## telnet

Use this command to start a Telnet connection to a remote host. The Enterasys B5 switch allows a total of four inbound and / or outbound Telnet session to run simultaneously.

### Syntax

```
telnet host [port]
```

### Parameters

<i>host</i>	Specifies the name or IP address of the remote host.
<i>port</i>	(Optional) Specifies the server port number.

### Defaults

If not specified, the default *port* number 23 will be used.

## Mode

Switch command, read-write.

## Example

This example shows how to start a Telnet session to a host at 10.21.42.13:

```
B5(su)->telnet 10.21.42.13
```

# Managing Switch Configuration and Files

## Configuration Persistence Mode

The default state of configuration persistence mode is “auto,” which means that when CLI configuration commands are entered, or when a configuration file stored on the switch is executed, the configuration is saved to NVRAM automatically at the following intervals:

- On a standalone unit, the configuration is checked every two minutes and saved if there has been a change.
- On a stack, the configuration is saved across the stack every 30 minutes if there has been a change.

If you want to save a running configuration to NVRAM more often than the automatic intervals, execute the **save config** command and wait for the system prompt to return. After the prompt returns, the configuration will be persistent.

You can change the persistence mode from “auto” to “manual” with the **set snmp persistmode** command. If the persistence mode is set to “manual,” configuration commands will not be automatically written to NVRAM. Although the configuration commands will actively modify the running configuration, they will not persist across a reset unless the **save config** command has been executed.



**Note:** When your device is configured for manual SNMP persistence mode, and you attempt to change the boot system image, the device will not prompt you to save changes or warn you that changes will be lost.

## Purpose

To set and view the persistence mode for CLI configuration commands, manually save the running configuration, view, manage, and execute configuration files and image files, and set and view TFTP parameters.

## Commands

For information about...	Refer to page...
show snmp persistmode	<a href="#">3-39</a>
set snmp persistmode	<a href="#">3-40</a>
save config	<a href="#">3-40</a>
dir	<a href="#">3-41</a>
show file	<a href="#">3-42</a>

For information about...	Refer to page...
show config	<a href="#">3-43</a>
configure	<a href="#">3-44</a>
copy	<a href="#">3-44</a>
delete	<a href="#">3-45</a>
show tftp settings	<a href="#">3-45</a>
set tftp timeout	<a href="#">3-46</a>
clear tftp timeout	<a href="#">3-47</a>
set tftp retry	<a href="#">3-47</a>
clear tftp retry	<a href="#">3-48</a>

## show snmp persistmode

Use this command to display the configuration persistence mode setting.

### Syntax

```
show snmp persistmode
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Usage

By default, the mode is set to “auto save,” which automatically saves configuration changes at specific intervals. If the mode is set to “manual,” configuration commands are never automatically saved. In order to make configuration changes persistent when the mode is manual, the **save config** command must be issued as described in “[Configuration Persistence Mode](#)” on page 3-38.

### Example

This example shows how to display the configuration persistence mode setting. In this case, persistence mode is set to “manual”, which means configuration changes are not being automatically saved.

```
B5(su)->show snmp persistmode
persistmode is manual
```

## set snmp persistmode

Use this command to set the configuration persistence mode, which determines whether user-defined configuration changes are saved automatically, or require issuing the **save config** command. See “[Configuration Persistence Mode](#)” on page 3-38 for more information.

### Syntax

```
set snmp persistmode {auto | manual}
```

### Parameters

<b>auto</b>	Sets the configuration persistence mode to automatic. This is the default state.
<b>manual</b>	Sets the configuration persistence mode to manual. In order to make configuration changes persistent, the <b>save config</b> command must be issued as described in “ <a href="#">save config</a> ” on page 3-40. This mode is useful for reverting back to old configurations.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the configuration persistence mode to manual:

```
B5(su)->set snmp persistmode manual
```

## save config

Use this command to save the running configuration. If applicable, this command will save the configuration to all switch members in a stack.

### Syntax

```
save config
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to save the running configuration:

```
B5(su)->save config
```



## dir

Use this command to list configuration and image files stored in the file system.

### Syntax

```
dir [filename]
```

### Parameters

---

<i>filename</i>	(Optional) Specifies the file name or directory to list.
-----------------	--

---

### Defaults

If **filename** is not specified, all files in the system will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to list all the configuration and image files in the system. The display indicates which image file is the Active file and which image file is the Boot file that will be used the next time the system reboots.

```
B5(su)->dir
Images:
=====
Filename:      b5-series_06.42.00.0029 (Active)
Version:       06.42.00.0029
Size:          9411584 (bytes)
Date:          Fri Aug  1 06:55:23 2008
Checksum:      6126a7aadf05150afb6eca51982302
Compatibility: <platform specific>

Filename:      b5-series_06.42.00.0030 (Boot)
Version:       06.42.00.0030
Size:          9411584 (bytes)
Date:          Fri Aug  8 08:44:04 2008
Checksum:      627938b785fa7fdb8eed74672af1edcc
Compatibility: <platform specific>

Files:                Size
=====
configs:
base_may              22629
base_apr              22629
base_july             20581
base_june             20581
logs:
current.log          2065
```

## show file

Use this command to display the contents of a file.

### Syntax

```
show file filename
```

### Parameters

---

<i>filename</i>	Specifies the name of the file to display.
-----------------	--

---

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display a text file named “myconfig” in the configs/ directory. Note that only a portion of the file is shown in this example.

```
B5(rw)->show file configs/myconfig
...
17 : #snmp
18 :
19 : set snmp access ro security-model v1 exact read All notify All nonvolatile
20 :
21 : set snmp access ro security-model v2c exact read All notify All nonvolatile
22 :
23 : set snmp access public security-model v1 exact read All write All notify All
nonvolatile
24 :
25 : set snmp access public security-model v2c exact read All write All notify All
nonvolatile
26 :
27 : set snmp access public security-model usm exact read All write All notify All
nonvolatile
28 :
29 : set snmp community :xxxxxxxxxxx:
30 :
31 : set snmp group ro user ro security-model v1
32 :
33 : set snmp group public user public security-model v1
34 :
35 : set snmp group ro user ro security-model v2c
36 :
37 : set snmp group public user public security-model v2c
38 :
39 : set snmp group public user public security-model usm
40 :
41 : set snmp user public authentication md5 :xxxxxxxxx: encryption des privacy
:xxxxxxxxx:
42 :
43 : set snmp view viewname All subtree 1
44 :
45 : !
```

## show config

Use this command to display the system configuration or write the configuration to a file.

### Syntax

```
show config [all | facility] [outfile {configs/filename}]
```

### Parameters

<b>all</b>	(Optional) Displays default and non-default configuration settings.
<i>facility</i>	(Optional) Specifies the exact name of one facility for which to show configuration. For example, enter "router" to show only router configuration.
<b>outfile</b>	(Optional) Specifies that the current configuration will be written to a text file in the configs/ directory.
<b>configs/filename</b>	Specifies a filename in the configs/ directory to display.

### Defaults

By default, **show config** will display all non-default configuration information for all facilities.

### Mode

Switch command, read-only.

### Usage

The separate facilities that can be displayed by this command are identified in the display of the current configuration by a # preceding the facility name. For example, "#port" indicates the facility name "port."

### Examples

This example shows how to write the current configuration to a file named save\_config2:

```
B5(rw)->show config all outfile configs/save_config2
```

This example shows how to display configuration for the facility "port".

```
B5(rw)->show config port
```

This command shows non-default configurations only.

Use 'show config all' to show both default and non-default configurations.

```
begin
!
***** NON-DEFAULT CONFIGURATION *****
!
!

#port
set port jumbo disable ge.1.1

!
end
```

## configure

Use this command to execute a previously downloaded configuration file stored on the switch.

### Syntax

```
configure filename [append]
```

### Parameters

<i>filename</i>	Specifies the path and file name of the configuration file to execute.
<b>append</b>	(Optional) Appends the configuration file contents to the current configuration. This is equivalent to typing the contents of the config file directly into the CLI and can be used, for example, to make incremental adjustments to the current configuration.

### Defaults

If **append** is not specified, the current running configuration will be replaced with the contents of the configuration file, which will require an automated reset of the chassis.

### Mode

Switch command, read-write.

### Example

This example shows how to execute the "Jan1\_2004.cfg" configuration file:

```
B5(su)->configure configs/Jan1_2004.cfg
```

## copy

Use this command to upload or download an image or a CLI configuration file.

### Syntax

```
copy source {destination | system:image}
```

### Parameters

<i>source</i>	Specifies location and name of the source file to copy. Options are a local file path in the configs or logs directory, or the URL of a TFTP, Secure FTP (SFTP), or Secure Copy (SCP) server.
<i>destination</i>	Specifies location and name of the destination where the file will be copied. Options are a local file path in the configs directory, or the URL of a TFTP, SFTP, or SCP server.
<b>system:image</b>	The required destination of an image file. <b>Note:</b> Only TFTP can be used to download an image file.

### Defaults

None.

## Mode

Switch command, read-write.

## Usage

SFTP and SCP can only be used to transfer configuration files or the logs/current.log file. You cannot use SFTP or SCP to download images (**system:image**).

## Examples

This example shows how to download an image via TFTP:

```
B5(su)->copy tftp://10.1.192.34/version01000 system:image
```

This example shows how to download a configuration file to the configs directory:

```
B5(su)->copy tftp://10.1.192.1/Jan1_2004.cfg configs/Jan1_2004.cfg
```

This example shows how to upload a configuration file from the configs directory using SFTP.

```
B5(su)->copy configs/Jan1_2009.cfg sftp://user:passwd@10.1.192.1/Jan1_2009.cfg
```

## delete

Use this command to remove an image or a CLI configuration file from the switch.

## Syntax

```
delete filename
```

## Parameters

<i>filename</i>	Specifies the local path name to the file. Valid directories are /images and /configs.
-----------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

Use the [dir](#) command ([page 3-41](#)) to display current image and configuration file names.

## Example

This example shows how to delete the “Jan1\_2004.cfg” configuration file:

```
B5(su)->delete configs/Jan1_2004.cfg
```

## show tftp settings

Use this command to display TFTP settings used by the switch during data transfers using TFTP.

## Syntax

```
show tftp settings
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Usage

The TFTP timeout value can be set with the **set tftp timeout** command. The TFTP retry value can be set with the **set tftp retry** command.

## Example

This example shows the output of this command.

```
B5(ro)->show tftp settings
TFTP packet timeout (seconds): 2
TFTP max retry: 5
```

# set tftp timeout

Use this command to configure how long TFTP will wait for a reply of either an acknowledgement packet or a data packet during a data transfer.

## Syntax

```
set tftp timeout seconds
```

## Parameters

---

<i>seconds</i>	Specifies the number of seconds to wait for a reply. The valid range is from 1 to 30 seconds. Default value is 2 seconds.
----------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example sets the timeout period to 4 seconds.

```
B5(rw)->set tftp timeout 4
```

## clear tftp timeout

Use this command to reset the TFTP timeout value to the default value of 2 seconds.

### Syntax

```
clear tftp timeout
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the timeout value to the default of 2 seconds.

```
B5(rw)-> clear tftp timeout
```

## set tftp retry

Use this command to configure how many times TFTP will resend a packet, either an acknowledgement packet or a data packet.

### Syntax

```
set tftp retry retry
```

### Parameters

---

<i>retry</i>	Specifies the number of times a packet will be resent. The valid range is from 1 to 1000. Default value is 5 retries.
--------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example sets the retry count to 3.

```
B5(rw)->set tftp retry 3
```

## clear tftp retry

Use this command to reset the TFTP retry value to the default value of 5 retries.

### Syntax

```
clear tftp retry
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the retry value to the default of 5 retries.

```
B5(rw)-> clear tftp retry
```

## Clearing and Closing the CLI

### Purpose

To clear the CLI screen or to close your CLI session.

### Commands

For information about...	Refer to page...
cls	<a href="#">3-48</a>
exit	<a href="#">3-49</a>

## cls (clear screen)

Use this command to clear the screen for the current CLI session.

### Syntax

```
cls
```

### Parameters

None.

### Defaults

None.



## Mode

Switch command, read-only.

## Example

This example shows how to clear the CLI screen:

```
B5(su)->cls
```

# exit

Use either of these commands to leave a CLI session.

## Syntax

```
exit
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Usage

By default, switch timeout occurs after 15 minutes of user inactivity, automatically closing your CLI session. Use the [set logout](#) command ([page 3-30](#)) to change this default.

## Example

This example shows how to exit a CLI session:

```
B5(su)->exit
```

# Resetting the Switch

## Purpose

To reset one or more switches, and to clear the user-defined configuration parameters.

## Commands

For information about...	Refer to page...
reset	<a href="#">3-50</a>
clear config	<a href="#">3-50</a>

## reset

Use this command to reset the switch without losing any user-defined configuration settings.

### Syntax

```
reset [unit]
```

### Parameters

---

<i>unit</i>	(Optional) Specifies a unit to be reset.
-------------	--

---

### Defaults

If no *unit* ID is specified, the entire system will be reset.

### Mode

Switch command, read-write.

### Usage

A Enterasys B5 switch can also be reset with the RESET button located on its front panel. For information on how to do this, refer to the Enterasys B5 Installation Guide shipped with your switch.

### Examples

This example shows how to reset the system:

```
B5(su)->reset
Are you sure you want to reload the stack? (y/n) y

Saving Configuration to stacking members
Reloading all switches.
```

This example shows how to reset unit 1:

```
B5(su)->reset 1
Are you sure you want to reload the switch? (y/n) y

Reloading switch 1.
This switch is manager of the stack.
STACK: detach 3 units
```

## clear config

Use this command to clear the user-defined configuration parameters.

### Syntax

```
clear config [all]
```

### Parameters

---

<b>all</b>	(Optional) Clears user-defined configuration parameters (and stack unit numbers and priorities, if applicable).
------------	---

---

## Defaults

If **all** is not specified, stacking configuration parameters will not be cleared.

## Mode

Switch command, read-write.

## Usage

When using the **clear config** command to clear configuration parameters in a stack, it is important to remember the following:

- Use **clear config** to clear configuration parameters without clearing stack unit IDs. This command WILL NOT clear stack parameters and avoids the process of re-numbering the stack.
- Use **clear config all** when it is necessary to clear all configuration parameters, including stack unit IDs (if applicable) and switch priority values.
- Use the **clear ip address** command to clear the IP address.

Configuration parameters and stacking information can also be cleared on the master unit only by selecting option 10 (restore configuration to factory defaults) from the boot menu on switch startup. This selection will leave stacking priorities on all other units, if applicable.

## Example

This example shows how to clear configuration parameters (including stacking parameters, if applicable):

```
B5(su)->clear config all
```

# Using and Configuring WebView

## Purpose

By default, WebView (The Enterasys Networks embedded web server for switch configuration and management tasks) is enabled on TCP port number 80 on the Enterasys B5 switch. You can verify WebView status, and enable or disable WebView using the commands described in this section. WebView can also be securely used over SSL port 443, if SSL is enabled on the switch. By default, SSL is disabled.

To use WebView, type the IP address of the switch in your browser. To use WebView over SSL, type in https:// then the IP address of the switch. For example, https://172.16.2.10.

## Commands

For information about...	Refer to page...
show webview	<a href="#">3-52</a>
set webview	<a href="#">3-52</a>
show ssl	<a href="#">3-53</a>
set ssl	<a href="#">3-53</a>

## show webview

Use this command to display WebView status.

### Syntax

```
show webview
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display WebView status:

```
B5(rw)->show webview  
WebView is Enabled.
```

## set webview

Use this command to enable or disable WebView on the switch.

### Syntax

```
set webview {enable [ssl-only] | disable}
```

### Parameters

<b>enable   disable</b>	Enable or disable WebView on the switch.
<b>ssl-only</b>	(Optional) Enables WebView with SSL only.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

When you enable WebView without using the **ssl-only** option, HTTP can be used to access WebView. If you enable with the **ssl-only** option, only HTTPS can be used to access WebView. Use the [set ssl](#) command to enable SSL (and HTTPS) on the switch.

Refer to “[set ssl](#)” on page 3-53 for information about enabling and disabling SSL on the switch.

It is good practice for security reasons to disable HTTP access on the switch when finished configuring with WebView, and then to only enable WebView on the switch when changes need to be made.

## Example

This example shows how to disable WebView on the switch:ssl

```
B5(rw)->set webview disable
```

## show ssl

Use this command to display SSL status.

### Syntax

```
show ssl
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display SSL status:

```
B5(rw)->show ssl
SSL status: Enabled
```

## set ssl

Use this command to enable or disable the use of WebView over SSL port 443. By default, SSL is disabled on the switch. This command can also be used to reinitialize the hostkey that is used for encryption.

### Syntax

```
set ssl {enabled | disabled | reinitialize | hostkey reinitialize}
```

### Parameters

<b>enabled   disabled</b>	Enables or disables the ability to use WebView over SSL.
<b>reinitialize</b>	Stops and then restarts the SSL process.
<b>hostkey reinitialize</b>	Stops SSL, regenerates new keys, and then restarts SSL.

### Defaults

By default, SSL is disabled on the switch.

### Mode

Switch command, read-write.

## Example

This example shows how to enable SSL:

```
B5(rw)->set ssl enabled
```

# Gathering Technical Support Information

## Purpose

To gather common technical support information.

## Command

For information about...	Refer to page...
<a href="#">show support</a>	3-54

## show support

Use this command to display switch information for troubleshooting.

### Syntax

```
show support
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Usage

This command initiates a number of **show** commands to easily gather basic information from an installed device. To use this command, set your console to capture the output to a file first, before executing the command, since the output is extensive.

Output from the following commands is gathered by this command:

- show version
- show logging buffer
- show port status
- show system utilization process
- show system utilization storage
- show config

**Example**

There is no display example because the output of this command is quite lengthy.





## Configuring System Power and PoE

### Important Notice

The commands in this section apply only to PoE-equipped devices. Consult the Installation Guide for your product to determine if it is PoE-equipped.

The commands in this chapter allow you to review and set system power and PoE (Power over Ethernet) parameters, including the power available to the system, the usage threshold for each module, whether or not SNMP trap messages will be sent when power status changes, and per-port PoE settings.

For more extensive configuration information, refer to the “Configuring Power over Ethernet Management” feature guide on the Enterasys Networks web site: <https://extranet.enterasys.com/downloads/>

## Power Management

### Management of PoE Power to PDs

For each PoE-capable module, you can configure how its PoE controller makes power available to attached powered devices (PDs). On a per module basis, you can configure:

- **Real-time** mode, in which the PoE controller calculates the power needed by a PD based on the actual power consumption of the attached devices.
- **Class** mode, in which the PoE controller manages power based on the IEEE 802.3af/.3at definition of the class limits advertised by the attached devices, with the exception that for class 0 and class 4 devices, actual power consumption will always be used. In this mode, the maximum amount of power required by a device in the advertised class is reserved for the port, regardless of the actual amount of power being used by the device.

Power management to PDs is configured with the command “[set inlinepower management](#)” (page 4-7). PoE classes are defined as:

**Table 4-1 PoE Powered Device Classes**

Class	Power Output at Port	Power Range Used by Device
0	15.4 watts	0.44 to 12.95 watts
1	4.0 watts	0.44 to 3.84 watts
2	7.0 watts	3.84 to 6.49 watts
3	15.4 watts	6.49 to 12.95 watts

**Table 4-1 PoE Powered Device Classes**

Class	Power Output at Port	Power Range Used by Device
4	34 watts (802.3at)	12.95 to 25.5 watts (802.3at)
	Reserved (802.3af)	Treat as class 0 (802.3af)

## Commands

For information about...	Refer to page...
show inlinepower	<a href="#">4-2</a>
set inlinepower threshold	<a href="#">4-3</a>
set inlinepower trap	<a href="#">4-4</a>
set inlinepower detectionmode	<a href="#">4-4</a>
show port inlinepower	<a href="#">4-5</a>
set port inlinepower	<a href="#">4-6</a>
set inlinepower management	<a href="#">4-7</a>

## show inlinepower

Use this command to display system power properties.

### Syntax

```
show inlinepower
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display system power properties:

```
B5(su)->show inlinepower
Detection Mode          : auto
```

Unit	Status	Power(W)	Consumption(W)	Usage(%)	Threshold(%)	Trap	Mgmt Mode
1	auto	375	0.00	0.00	80	enable	realtime

[Table 4-2](#) provides an explanation of the command output.

**Table 4-2 show inlinepower Output Details**

Output	What It Displays...
Detection Mode	Displays the PD detection mode used by the switch. The detection mode can be configured with the command <code>set inlinepower detectionmode</code> (page 4-4).
Unit	Number of PoE-capable module.
Status	Whether the PoE administrative state is off (disabled) or auto (on). This state is not configurable.
Power (W)	Unit's available power wattage.
Consumption (W)	Unit's power wattage consumed.
Usage (%)	Unit's percentage of total system PoE power usage.
Threshold (%)	Unit's allotted percentage of total PoE power available in the system. The threshold can be configured with the command <code>set inlinepower threshold</code> (page 4-3).
Trap	Whether PoE trap messaging is enabled or disabled on this unit. Trap messaging can be configured with the command <code>set inlinepower trap</code> (page 4-4).
Mgmt Mode	Specifies the power management mode of the module, either <b>realtime</b> or <b>class</b> . Power management mode is configured with the command <code>set inlinepower management</code> (page 4-7).

## set inlinepower threshold

Use this command to set the power usage threshold on a specified unit or module.

### Syntax

```
set inlinepower threshold usage-threshold module-number
```

### Parameters

<i>usage-threshold</i>	Specifies a power threshold as a percentage of available system power. Valid values are <b>11</b> to <b>100</b> .
<i>module-number</i>	Specifies the module or unit on which to set the power threshold.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The threshold is expressed as a percentage of the available PoE power. When this threshold is reached, a trap will be sent if traps are enabled with the `set inlinepower trap` command.

### Example

This example shows how to set the power threshold to 90 on module/unit 1:

```
B5(su)->set inlinepower threshold 90 1
```

## set inlinepower trap

Use this command to enable or disable the sending of an SNMP trap message for a unit or module whenever the status of its ports changes, or whenever the unit's power usage threshold is crossed.

### Syntax

```
set inlinepower trap {disable | enable} module-number
```

### Parameters

<b>disable   enable</b>	Disables or enables inline power trap messaging.
<i>module-number</i>	Specifies the module or unit on which to disable or enable trap messaging.

### Defaults

Sending of traps is disabled by default.

### Mode

Switch command, read-write.

### Usage

The module's or unit's power usage threshold must be set using the **set inlinepower threshold** command as described on page 4-3.

### Example

This example shows how to enable inline power trap messaging on module 1:

```
B5(su)->set inlinepower trap enable 1
```

## set inlinepower detectionmode

Use this command to specify the method the switch will use to detect PDs (powered devices) connected to its ports.

### Syntax

```
set inlinepower detectionmode {auto | ieee}
```

### Parameters

<b>auto</b>	Specifies that the switch will use the standard 802.3af detection method first. If that fails, then the switch will use the legacy (pre 802.3af standard) capacitance method of detection.
<b>ieee</b>	Specifies that the switch will only use the standard 802.3af detection method.

### Defaults

Default detection mode is **auto**.

### Mode

Switch command, read-write.

## Usage

This command is used to specify how the switch should detect PDs connected to its ports. The PoE hardware in the switches can use the IEEE standard 802.3af (resistor-based) method or a proprietary method using capacitor detection.

If **auto** is configured, the switch will first use the IEEE resistor-based detection method, and if that fails, the switch will use the capacitor-based detection method. If **ieee** is configured, only the IEEE resistor-based detection method will be used.

## Example

This example sets the switch's PD detection mode to IEEE standard 802.3af only.

```
B5(su)->set inlinepower detectionmode ieee
```

## show port inlinepower

Use this command to display information about ports on the switch supporting PoE.

### Syntax

```
show port inlinepower [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays information for specific PoE port(s).
--------------------	---

### Defaults

If no port string is specified, information for all PoE ports will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display PoE information for port `ge.2.1`. In this case, the port's administrative state, PoE priority and class have not been changed from default values:

```
B5(su)->show port inlinepower ge.2.1
```

Port	Type	Admin	Oper	Priority	Class	Power(W)	Capability	Power Select
ge.2.1		auto	Searching	Low	0		802.3at	802.3at

**Table 4-3 show port inlinepower Output Details**

Output Field	What it Displays
Port	The port being displayed in this row.
Type	A text string describing the type of device connected to the port, set with the <a href="#">set port inlinepower</a> command.
Admin	The port's PoE administrative state, off (disabled) or auto (on). Can be set with the <a href="#">set port inlinepower</a> command.

**Table 4-3 show port inlinepower Output Details (Continued)**

Output Field	What it Displays
Oper	The operational mode of the port. Values displayed can be: <ul style="list-style-type: none"> <li>Searching — no device is connected to the port.</li> <li>Delivering Power — power being delivered to connected device.</li> <li>Over Budget — connected device requires more power than the switch can allocate to that port.</li> <li>Overload — connected device consumed more power than it was allowed.</li> <li>Other Fault — another PoE error has been detected, such as a short on the PoE load, error with PoE signaling, general error detection.</li> </ul>
Priority	The port's priority for PoE allocation. Values can be critical (highest), high or low. Can be set with the <a href="#">set port inlinepower</a> command.
Class	The PoE class of the connected powered device.
Power (W)	The amount of power being delivered to the port.
Capability	Whether the port is able to support <b>802.3af</b> devices only or <b>802.3at</b> (and also 802.3af) devices. Can be set with the <a href="#">set port inlinepower</a> command.
Power Select	If a port is capable of supporting 802.3at and 802.3af devices, this field displays the power level the port is supplying — either 802.3af or 802.3at.

## set port inlinepower

Use this command to configure PoE parameters on one or more ports.

### Syntax

```
set port inlinepower port-string {[admin {off | auto}] [capability {802.3af | 802.3at}] [priority {critical | high | low}] [type type]}
```

### Parameters

<i>port-string</i>	Specifies the port(s) on which to configure PoE.
<b>admin off   auto</b>	(Optional) Sets the PoE administrative state to off (disabled) or auto (on). When you set the admin state to <b>off</b> , PoE power is disabled on that port.
<b>capability 802.3af   802.3at</b>	(Optional) Sets the sport to support either 802.3af power level or 802.3at and also 802.3af power levels.
<b>priority critical   high   low</b>	(Optional) Sets the port(s) priority for the PoE allocation algorithm to critical (highest), high or low.
<b>type <i>type</i></b>	(Optional) Specifies a string describing the type of device connected to a port. The string can be a maximum of 20 characters.

### Defaults

At least one of the optional parameters must be entered.

### Mode

Switch command, read-write.

## Usage

If the capability of a port is set to **802.3at**, the port will automatically detect the power level required by the attached powered device and deliver the required level.

If you want to disable PoE on an RJ45 port that is shared with a combo fiber port, use the command **set inlinepower *port-string* admin off**.

## Example

This example shows how to enable PoE on port `ge.3.1` with critical priority:

```
B5(su)->set port inlinepower ge.3.1 admin auto priority critical
```

# set inlinepower management

Use this command to configure how power is made available to attached powered devices, on a per module basis. Power can be made available based on the class of the device or based on the actual power being consumed when the device powers up.

## Syntax

```
set inlinepower management {class | realtime} [module-number]
```

## Parameters

<b>class</b>	Specifies that power needs should be calculated based on the class of the PoE device.
<b>realtime</b>	Specifies that power needs should be calculated based on the actual power being consumed by the PoE device when it powers up.
<i>module-number</i>	(Optional) Specifies that this command should apply only to the slot identified.

## Defaults

Realtime.

If a module number is not specified, all modules are configured.

## Mode

Switch command, read-write.

## Usage

For each PoE-capable module, you can configure how its PoE controller makes power available to attached powered devices (PDs).

In **realtime** mode, the PoE controller calculates the power needed by a PD based on the actual power consumption of the attached devices.

In **class** mode, the PoE controller manages power based on the IEEE 802.3af/.3at definition of the class limits advertised by the attached devices. Note that for class 0 and class 4 devices, actual power consumption will always be used. In class mode, the maximum amount of power required by a device in the advertised class is reserved for the port, regardless of the actual amount of power being used by the device.

Refer to “[Management of PoE Power to PDs](#)” on page 4-1 for more information. Use the **show inlinepower** command to display the current management mode for each module slot.

## Example

The following example sets the power management mode to realtime on slot 1, then displays the current configuration with the **show inlinepower** command.

```
B5(su)->set inlinepower management realtime 1
```

```
B5(su)->show inlinepower
```

```
Detection Mode      : auto
```

Unit	Status	Power(W)	Consumption(W)	Usage(%)	Threshold(%)	Trap	Mgmt Mode
----	-----	-----	-----	-----	-----	----	-----
1	auto	480	0.00	0.00	80	disable	realtime



## Transmit Queue Monitoring Configuration

This chapter describes the commands used to monitor and manage transmit queues.

For information about...	Refer to page...
<a href="#">Transmit Queue Monitoring Overview</a>	5-1
<a href="#">Commands</a>	5-1

### Transmit Queue Monitoring Overview

The commands described in this chapter can be used to monitor transmit queues and, if a queue is found to be stalled, to take corrective action.

Stalled transmit queues may be caused by a duplex mismatch, hardware error, or by excessive pause frames. Excessive pause frames are not expected under normal conditions but may be the result of a soft or hard failure on an attached device, or even a deliberate denial of service attack.

Transmit queue monitoring periodically samples each port's transmit queue depths (total packets queued) and transmit counters to identify stalled ports and free the resources tied up on the associated transmit queues. This feature allows you to configure a minimum number of transmits for a sample period and to set levels for the number of consecutive failures that will trigger different levels of corrective actions.

Corrective actions that can be configured include logging, discarding received pause frames, and disabling the port. The ability to pause the switch is treated as a privilege — if an attached device violates that privilege, its pause frames can be ignored. When a switch port is in the discarding pause state, the port will be allowed to transmit (including Wake-on-LAN magic packets). The port retains its ability to transmit its own pause frames, and the attached device is still allowed the normal switching of packets. Because disabling a port and discarding pause frames is a punitive action, a port restore interval "downtime" is provided. At the end of the downtime interval, all disabled ports will have complete functionality restored. In addition, any change in a port's link state clears that port's failure count and restores the port to normal operation.

### Commands

For information about...	Refer to page...
<a href="#">set txqmonitor</a>	5-2
<a href="#">set txqmonitor downtime</a>	5-2
<a href="#">set txqmonitor minrate</a>	5-3
<a href="#">set txqmonitor threshold</a>	5-3

For information about...	Refer to page...
<a href="#">clear txqmonitor</a>	5-4
<a href="#">show txqmonitor</a>	5-5
<a href="#">show txqmonitor flowcontrol</a>	5-6
<a href="#">show txqmonitor port</a>	5-6

## set txqmonitor

Use this command to enable or disable transmit queue monitoring on the switch. Transmit queue monitoring is enabled by default.

### Syntax

```
set txqmonitor {enable | disable}
```

### Parameters

<b>enable   disable</b>	Enables or disables transmit queue monitoring on the switch. Monitoring is enabled by default.
-------------------------	--

### Defaults

Monitoring is enabled by default.

### Mode

Switch command, read-write.

### Example

This example disables transmit queue monitoring on the switch.

```
B5(su)-> set txqmonitor disable
```

## set txqmonitor downtime

Use this command to configure the time interval, in seconds, that ports disabled by the transmit queue monitoring feature remain disabled.

### Syntax

```
set txqmonitor downtime seconds
```

### Parameters

<i>seconds</i>	Specifies the downtime in seconds. A value of 0 will set the downtime to forever, meaning that disabled ports will remain disabled until cleared manually or until their next link state transition.  The default value is 0.
----------------	---

## Defaults

The default value is 0, meaning that disabled ports will remain disabled until cleared manually or until their next link state transition.

## Mode

Switch command, read-write.

## Usage

When the downtime is configured as 0, disabled ports can be manually enabled using the **clear txqmonitor down** command (page 5-4).

## Example

This example sets the downtime to 3600 seconds.

```
B5(su)-> set txqmonitor downtime 3600
```

# set txqmonitor minrate

Use this command to set the minimum rate (in packets per second) of transmitted packets in a sampling interval.

## Syntax

```
set txqmonitor minrate rate
```

## Parameters

<i>rate</i>	The number of packets per second that must be transmitted per sampling interval, if packets exist on the port's transmit queues. The default value is 1 packet per second.
-------------	---

## Defaults

One packet per second.

## Mode

Switch command, read-write.

## Example

This example sets the minimum rate of packets per second per sampling interval to 6.

```
B5(su)-> set txqmonitor minrate 6
```

# set txqmonitor threshold

Use this command to set the transmit queue monitoring threshold levels for triggering actions applied to a stalled port.

## Syntax

```
set txqmonitor threshold { [logging | ignorepause | disableinterface] value }
```

## Parameters

<b>logging</b>	Specifies the logging trigger level.
<b>ignorepause</b>	Specifies the discard received pause frames trigger level.
<b>disableinterface</b>	Specifies the port disable trigger level.
<i>value</i>	The number of successive failed sample intervals that will trigger an action. A value of 0 disables the associated action.

## Defaults

**logging:** 2 sequential failures

**ignorepause:** 5 sequential failures

**disableinterface:** 10 sequential failures

## Mode

Switch command, read-write.

## Example

This example sets the disable interface threshold to 6 sequential failed sample intervals.

```
B5(su)-> set txqmonitor threshold disableinterface 6
```

# clear txqmonitor

Use this command to restore all transmit queue monitoring options to their default values.

## Syntax

```
clear txqmonitor { all | globalstate | ignorepause [port-string] |  
down [port-string] | threshold | downtime | minrate }
```

## Parameters

<b>all</b>	Clear all transmit queue monitoring options to their default values.
<b>globalstate</b>	Clear the global state to the default of enabled.
<b>ignorepause</b> [ <i>port-string</i> ]	Restore ports in the discarding pause frame state to the default of not discarding pause frames.  Optionally, restore only specified port or ports.
<b>down</b> [ <i>port-string</i> ]	Re-enable ports disabled by transmit queue monitoring.  Optionally, enable only specified port or ports.
<b>threshold</b>	Clear all trigger thresholds to default values. See <a href="#">set txqmonitor threshold</a> for default values.
<b>downtime</b>	Clear the downtime value to the default of 0, meaning that disabled ports will remain disabled until cleared manually or until their next link state transition.
<b>minrate</b>	Clear the number of packets per second that must be transmitted per sampling interval to the default value of 1 packet per second.

## Defaults

If *port-string* is not specified with the **ignorepause** or **down** parameters, all ports will be cleared.

## Mode

Switch command, read-write.

## Example

This example re-enables port ge.1.1 that was disabled by transmit queue monitoring.

```
B5(su)-> clear txqmonitor down ge.1.1
```

# show txqmonitor

Use this command to display information about transmit queue monitoring.

## Syntax

```
show txqmonitor [ downports | downtime | globalstate | ignorepause | minrate |
operstatus | threshold ]
```

## Parameters

<b>downports</b>	(Optional) Lists the ports disabled by transmit queue monitoring.
<b>downtime</b>	(Optional) Displays the currently configured downtime interval in seconds.
<b>globalstate</b>	(Optional) Displays the global state of transmit queue monitoring, either enabled or disabled.
<b>ignorepause</b>	(Optional) Displays the ports currently discarding received pause frames.
<b>minrate</b>	(Optional) Displays the currently configured minimum acceptable transmit rate per sampling period.
<b>operstatus</b>	(Optional) Displays the operational status of all ports relative to transmit queue monitoring. Ports are either operational or disabled.
<b>threshold</b>	(Optional) Display the currently configured trigger values for transmit queue monitoring corrective actions.

## Defaults

If no parameter is specified, all transmit queue monitoring information is displayed.

## Mode

Switch mode, read-only.

## Examples

This example displays the global state of transmit queue monitoring.

```
B5(su)-> show txqmonitor globalstate
txqmonitor enabled
```

This example displays the currently configured trigger values.

```
B5(su)->show txqmonitor threshold
```

```

logging                2
ignorepause           5
disableinterface     10

```

## show txqmonitor flowcontrol

Use this command to display the flow control information for one or more ports.

### Syntax

```
show txqmonitor flowcontrol [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Specifies the port or ports for which to display flow control information.
--------------------	---

---

### Defaults

If no *port-string* is specified, flow control information for all ports is displayed.

### Mode

Switch mode, read-only.

### Usage

This command displays counters for transmitted and received pause frames per port.

### Example

This example shows the the pause frame counts for ports 1 through 3.

```

B5(su)->show txqmonitor flowcontrol ge.1.1-3
port          TX Pause Count    RX Pause Count
-----
ge.1.1        0                  0
ge.1.2        0                  0
ge.1.3        0                  146

```

## show txqmonitor port

Use this command to display transmit queue monitoring information for one or more ports.

### Syntax

```
show txqmonitor port [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Specifies the ports for which to display information.
--------------------	--

---

### Defaults

If *port-string* is not specified, information for all ports is displayed.

## Mode

Switch mode, read-only.

## Usage

This command displays transmit queue monitoring information about ports, including:

- Status — whether the port is operating normally, or ignoring received pause frames, or disabled due to transmit queue monitoring corrective action
- Transmit queue sampling counts — the number of consecutive samples showing stalled transmit queues, and the total number of samples showing stalled queues.

## Examples

This example displays transmit queue monitoring information for ports 1 through 3. The output shows that port ge.1.2 is currently ignoring received pause frames and port ge.1.3 is disabled due to 10 consecutive monitoring samples showing a stalled transmit queue.

```
B5(su)->show txqmonitor port ge.1.1-3
```

port	status	consecutive samples stalled	total samples stalled
ge.1.1	normal	0	0
ge.1.2	ignorepause	0	5
ge.1.3	down	10	10





---

## Discovery Protocol Configuration

This chapter describes how to configure discovery protocols. For more extensive configuration information, refer to the “Configuring Neighbor Discovery” feature guide on the Enterasys Networks web site: <https://extranet.enterasys.com/downloads/>

For information about...	Refer to page...
<a href="#">Configuring CDP</a>	<a href="#">6-1</a>
<a href="#">Configuring Cisco Discovery Protocol</a>	<a href="#">6-7</a>
<a href="#">Configuring Link Layer Discovery Protocol and LLDP-MED</a>	<a href="#">6-13</a>

### Configuring CDP

#### Purpose

To review and configure the Enterasys CDP discovery protocol. This protocol is used to discover network topology. When enabled, this protocol allows Enterasys devices to send periodic PDUs about themselves to neighboring devices.

#### Commands

The commands used to review and configure the CDP discovery protocol are listed below.

For information about...	Refer to page...
<code>show cdp</code>	<a href="#">6-2</a>
<code>set cdp state</code>	<a href="#">6-3</a>
<code>set cdp auth</code>	<a href="#">6-4</a>
<code>set cdp interval</code>	<a href="#">6-4</a>
<code>set cdp hold-time</code>	<a href="#">6-5</a>
<code>clear cdp</code>	<a href="#">6-5</a>
<code>show neighbors</code>	<a href="#">6-6</a>

## show cdp

Use this command to display the status of the CDP discovery protocol and message interval on one or more ports.

### Syntax

```
show cdp [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays CDP status for a specific port. For a detailed description of possible port-string values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

### Defaults

If *port-string* is not specified, all CDP information will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display CDP information for ports ge.1.1 through ge.1.9:

```
B5(su)->show cdp ge.1.1-9
CDP Global Status      :auto-enable
CDP Version Supported  :30 hex
CDP Hold Time         :180
CDP Authentication Code :00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 hex
CDP Transmit Frequency :60

Port      Status
-----
ge.1.1    auto-enable
ge.1.2    auto-enable
ge.1.3    auto-enable
ge.1.4    auto-enable
ge.1.5    auto-enable
ge.1.6    auto-enable
ge.1.7    auto-enable
ge.1.8    auto-enable
ge.1.9    auto-enable
```

[Table 6-1](#) provides an explanation of the command output.

**Table 6-1 show cdp Output Details**

Output Field	What It Displays...
CDP Global Status	Whether CDP is globally auto-enabled, enabled or disabled. The default state of auto-enabled can be reset with the set cdp state command. For details, refer to <a href="#">“set cdp state”</a> on page 6-3.
CDP Versions Supported	CDP version number(s) supported by the switch.
CDP Hold Time	Minimum time interval (in seconds) at which CDP configuration messages can be set. The default of 180 seconds can be reset with the set cdp hold-time command. For details, refer to <a href="#">“set cdp hold-time”</a> on page 6-5.

**Table 6-1 show cdp Output Details (Continued)**

Output Field	What It Displays...
CDP Authentication Code	Authentication code for CDP discovery protocol. The default of 00-00-00-00-00-00-00-00 can be reset using the <code>set cdp auth</code> command. For details, refer to <a href="#">“set cdp auth”</a> on page 6-4.
CDP Transmit Frequency	Frequency (in seconds) at which CDP messages can be transmitted. The default of 60 seconds can be reset with the <code>set cdp interval</code> command. For details, refer to <a href="#">“set cdp interval”</a> on page 6-4.
Port	Port designation. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
Status	Whether CDP is enabled, disabled or auto-enabled on the port.

## set cdp state

Use this command to enable or disable the CDP discovery protocol on one or more ports.

### Syntax

```
set cdp state {auto | disable | enable} [port-string]
```

### Parameters

<b>auto   disable   enable</b>	Auto-enables, disables or enables the CDP protocol on the specified port(s). In auto-enable mode, which is the default mode for all ports, a port automatically becomes CDP-enabled upon receiving its first CDP message.
<i>port-string</i>	(Optional) Enables or disables CDP on specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

### Defaults

If *port-string* is not specified, the CDP state will be globally set.

### Mode

Switch command, read-write.

### Examples

This example shows how to globally enable CDP:

```
B5(su)->set cdp state enable
```

This example shows how to enable the CDP for port ge.1.2:

```
B5(su)->set cdp state enable ge.1.2
```

This example shows how to disable the CDP for port ge.1.2:

```
B5(su)->set cdp state disable ge.1.2
```

## set cdp auth

Use this command to set a global CDP authentication code.

### Syntax

```
set cdp auth auth-code
```

### Parameters

---

<i>auth-code</i>	Specifies an authentication code for the CDP protocol. This can be up to 16 hexadecimal values separated by commas.
------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The authentication code value determines a switch's CDP domain. If two or more switches have the same CDP authentication code, they will be entered into each other's CDP neighbor tables. If they have different authentication codes, they are in different domains and will not be entered into each other's CDP neighbor tables.

A switch with the default authentication code (16 null characters) will recognize all switches, no matter what their authentication code, and enter them into its CDP neighbor table.

### Example

This example shows how to set the CDP authentication code to 1,2,3,4,5,6,7,8:

```
B5(su)->set cdp auth 1,2,3,4,5,6,7,8:
```

## set cdp interval

Use this command to set the message interval frequency (in seconds) of the CDP discovery protocol.

### Syntax

```
set cdp interval frequency
```

### Parameters

---

<i>frequency</i>	Specifies the transmit frequency of CDP messages in seconds. Valid values are from 5 to 900 seconds.
------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to set the CDP interval frequency to 15 seconds:

```
B5(su)->set cdp interval 15
```

## set cdp hold-time

Use this command to set the hold time value for CDP discovery protocol configuration messages.

### Syntax

```
set cdp hold-time hold-time
```

### Parameters

<i>hold-time</i>	Specifies the hold time value for CDP messages in seconds. Valid values are from 15 to 600.
------------------	---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set CDP hold time to 60 seconds:

```
B5(su)->set cdp hold-time 60
```

## clear cdp

Use this command to reset CDP discovery protocol settings to defaults.

### Syntax

```
clear cdp {[state] [port-state port-string] [interval] [hold-time] [auth-code]}
```

### Parameters

<b>state</b>	(Optional) Resets the global CDP state to auto-enabled.
<b>port-state</b> <i>port-string</i>	(Optional) Resets the port state on specific port(s) to auto-enabled.
<b>interval</b>	(Optional) Resets the message frequency interval to 60 seconds.
<b>hold-time</b>	(Optional) Resets the hold time value to 180 seconds.
<b>auth-code</b>	(Optional) Resets the authentication code to 16 bytes of 00 (00-00-00-00-00-00-00-00-00-00).

### Defaults

At least one optional parameter must be entered.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the CDP state to auto-enabled:

```
B5(su)->clear cdp state
```

# show neighbors

This command displays Neighbor Discovery information for either the CDP or Cisco DP protocols.

## Syntax

```
show neighbors [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Specifies the port or ports for which to display Neighbor Discovery information.
--------------------	---

---

## Defaults

If no port is specified, all Neighbor Discovery information is displayed.

## Mode

Switch command, read-only.

## Usage

This command displays information discovered by both the CDP and the Cisco DP protocols.

## Example

This example displays Neighbor Discovery information for all ports.

```
B5(su)->show neighbors
```

Port	Device ID	Port ID	Type	Network Address
ge.1.1	00036b8b1587	12.227.1.176	ciscodp	12.227.1.176
ge.1.6	0001f496126f	140.2.3.1	ciscodp	140.2.3.1
ge.1.6	00-01-f4-00-72-fe	140.2.4.102	cdp	140.2.4.102
ge.1.6	00-01-f4-00-70-8a	140.2.4.104	cdp	140.2.4.104
ge.1.6	00-01-f4-c5-f7-20	140.2.4.101	cdp	140.2.4.101
ge.1.6	00-01-f4-89-4f-ae	140.2.4.105	cdp	140.2.4.105
ge.1.6	00-01-f4-5f-1f-c0	140.2.1.11	cdp	140.2.1.11
ge.1.19	0001f400732e	165.32.100.10	ciscodp	165.32.100.10

# Configuring Cisco Discovery Protocol

## Purpose

To review and configure the Cisco discovery protocol. Discovery protocols are used to discover network topology. When enabled, they allow Cisco devices to send periodic PDUs about themselves to neighboring devices. Specifically, this feature enables recognizing PDUs from Cisco phones. A table of information about detected phones is kept by the switch and can be queried by the network administrator.

## Commands

The commands used to review and configure the Cisco discovery protocol are listed below. Refer also to “[show neighbors](#)” on page 6-6.

For information about...	Refer to page...
show ciscodp	<a href="#">6-7</a>
show ciscodp port info	<a href="#">6-8</a>
set ciscodp status	<a href="#">6-9</a>
set ciscodp timer	<a href="#">6-9</a>
set ciscodp holdtime	<a href="#">6-10</a>
set ciscodp port	<a href="#">6-10</a>
clear ciscodp	<a href="#">6-12</a>

## show ciscodp

Use this command to display global Cisco discovery protocol information.

### Syntax

```
show ciscodp
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display global Cisco DP information.

```
B5(su)->show ciscodp
CiscoDP :Enabled
Timer :5
Holdtime (TTL): 180
```

Device ID : 001188554A60  
 Last Change : WED NOV 08 13:19:56 2006

[Table 6-2](#) provides an explanation of the command output.

**Table 6-2 show ciscodp Output Details**

Output Field	What It Displays...
CiscoDP	Whether Cisco DP is globally enabled or disabled. Auto indicates that Cisco DP will be globally enabled only if Cisco DP PDUs are received.  Default setting of auto-enabled can be reset with the <b>set ciscodp status</b> command.
Timer	The number of seconds between Cisco discovery protocol PDU transmissions. The default of 60 seconds can be reset with the <b>set ciscodp timer</b> command.
Holdtime	Number of seconds neighboring devices will hold PDU transmissions from the sending device. Default value of 180 can be changed with the <b>set ciscodp holdtime</b> command.
Device ID	The MAC address of the switch.
Last Change	The time that the last Cisco DP neighbor was discovered.

## show ciscodp port info

Use this command to display summary information about the Cisco discovery protocol on one or more ports.

### Syntax

```
show ciscodp port info [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays Cisco DP information for a specific port. For a detailed description of possible port-string values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

### Defaults

If *port-string* is not specified, Cisco DP information for all ports will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display Cisco DP information for Gigabit Ethernet port 1 in slot 1.

```
B5(su)->show ciscodp port info ge.1.1
```

```
port      state      vvid      trusted    cos
-----
ge.1.1    enable    none      yes        0
```

[Table 6-3](#) provides an explanation of the command output.



**Table 6-3 show ciscodp port info Output Details**

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible <i>port-string</i> values, refer to “Port String Syntax Used in the CLI” on page 7-1.
State	Whether Cisco DP is enabled, disabled or auto-enabled on the port. Default state of enabled can be changed using the <b>set ciscodp port</b> command.
vvid	Whether a voice VLAN ID has been set on this port. Default of none can be changed using the <b>set ciscodp port</b> command.
trusted	The trust mode of the port. Default of trusted can be changed using the <b>set ciscodp port</b> command.
cos	The Class of Service priority value for untrusted traffic. The default of 0 can be changed using the <b>set ciscodp port</b> command.

## set ciscodp status

Use this command to enable or disable the Cisco discovery protocol globally on the switch.

### Syntax

```
set ciscodp state {auto | disable / enable}
```

### Parameters

<b>auto</b>	Globally enable only if Cisco DP PDUs are received.
<b>disable</b>	Globally disable Cisco discovery protocol.
<b>enable</b>	Globally enable Cisco discovery protocol.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to globally enable CiscoDP:

```
B5(su)->set ciscodp state enable
```

## set ciscodp timer

Use this command to set the number of seconds between Cisco discovery protocol PDU transmissions.

### Syntax

```
set ciscodp timer seconds
```

## Parameters

---

<i>seconds</i>	Specifies the number of seconds between Cisco DP PDU transmissions. Valid values are from 5 to 254 seconds.
----------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to set the Cisco DP timer to 120 seconds.

```
B5(su)->set ciscodp timer 120
```

# set ciscodp holdtime

Use this command to set the time to live (TTL) for Cisco discovery protocol PDUs. This is the amount of time, in seconds, neighboring devices will hold PDU transmissions from the sending device.

## Syntax

```
set ciscodp holdtime hold-time
```

## Parameters

---

<i>hold-time</i>	Specifies the time to live for Cisco DP PDUs. Valid values are from 10 to 255 seconds.
------------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to set Cisco DP hold time to 180 seconds:

```
B5(su)->set ciscodp hold-time 180
```

# set ciscodp port

Use this command to set the status, voice VLAN, extended trust mode, and CoS priority for untrusted traffic for the Cisco Discovery Protocol on one or more ports.

## Syntax

```
set ciscodp port {[status {disable | enable}] [vvid {vlan-id | none | dot1p | untagged}] [trusted {yes | no}] [cos value]} port-string
```

## Parameters

<b>status</b>	Sets the CiscoDP port operational status.
<b>disable</b>	Does not transmit or process CiscoDP PDUs.
<b>enable</b>	Transmits and processes CiscoDP PDUs.
<b>vvid</b>	Sets the port voice VLAN for CiscoDP PDU transmission.
<i>vlan-id</i>	Specifies the VLAN ID, range 1-4093.
<b>none</b>	No voice VLAN will be used in CiscoDP PDUs. This is the default.
<b>dot1p</b>	Instructs attached phone to send 802.1p tagged frames.
<b>untagged</b>	Instructs attached phone to send untagged frames.
<b>trusted</b>	Sets the extended trust mode on the port.
<b>yes</b>	Instructs attached phone to allow the device connected to it to transmit traffic containing any CoS or Layer 2 802.1p marking. This is the default value.
<b>no</b>	Instructs attached phone to overwrite the 802.1p tag of traffic transmitted by the device connected to it to 0, by default, or to the value configured with the <b>cos</b> parameter.
<b>cos value</b>	Instructs attached phone to overwrite the 802.1p tag of traffic transmitted by the device connected to it with the specified <i>value</i> , when the trust mode of the port is set to untrusted. <i>Value</i> can range from 0 to 7, with 0 indicating the lowest priority.
<i>port-string</i>	Specifies the port(s) on which status will be set.

## Defaults

- Status: enabled
- Voice VLAN: none
- Trust mode: trusted
- CoS value: 0

## Mode

Switch mode, read-write.

## Usage

The following points describe how the Cisco DP extended trust settings work on the switch.

- A Cisco DP port trust status of trusted or untrusted is only meaningful when a Cisco IP phone is connected to a switch port and a PC or other device is connected to the back of the Cisco IP phone.
- A Cisco DP port state of trusted or untrusted only affects tagged traffic transmitted by the device connected to the Cisco IP phone. Untagged traffic transmitted by the device connected to the Cisco IP phone is unaffected by this setting.
- If the switch port is configured to a Cisco DP trust state of **trusted** (with the **trusted yes** parameter of this command), this setting is communicated to the Cisco IP phone instructing it to allow the device connected to it to transmit traffic containing any CoS or Layer 2 802.1p marking.

- If the switch port is configured to a Cisco DP trust state of **untrusted (trusted no)**, this setting is communicated to the Cisco IP phone instructing it to overwrite the 802.1p tag of traffic transmitted by the device connected to it to 0, by default, or to the value specified by the **cos** parameter of this command.
- There is a one-to-one correlation between the value set with the **cos** parameter and the 802.1p value assigned to ingress traffic by the Cisco IP phone. A value of 0 equates to an 802.1p priority of 0. Therefore, a value of 7 is given the highest priority.



**Note:** The Cisco Discovery Protocol must be globally enabled using the **set cisco dp status** command before operational status can be set on individual ports.

## Examples

This example shows how to set the Cisco DP port voice VLAN ID to 3 on port ge.1.6 and enable the port operational state.

```
B5(rw)->set cisco dp port status enable vvid 3 ge.1.6
```

This example shows how to set the Cisco DP extended trust mode to untrusted on port ge.1.5 and set the CoS priority to 1.

```
B5(rw)->set cisco dp port trusted no cos 1 ge.1.5
```

## clear cisco dp

Use this command to clear the Cisco discovery protocol back to the default values.

### Syntax

```
clear cisco dp [status | timer | holdtime | {port {status | vvid | trust | cos}] [port-string]
```

### Parameters

<b>status</b>	Clears global CiscoDP enable status to default of auto.
<b>timer</b>	Clears the time between CiscoDP PDU transmissions to default of 60 seconds.
<b>holdtime</b>	Clears the time-to-live for CiscoDP PDU data to default of 180 seconds.
<b>port</b>	Clears the CiscoDP port configuration.
<b>status</b>	Clears the individual port operational status to the default of enabled.
<b>vvid</b>	Clears the individual port voice VLAN for CiscoDP PDU transmission to 0.
<b>trust</b>	Clears the trust mode configuration of the port to trusted.
<b>cos</b>	Clears the CoS priority for untrusted traffic of the port to 0.
<i>port-string</i>	(Optional) Specifies the port(s) on which status will be set.

### Defaults

If no parameters are entered, all Cisco DP parameters are reset to the defaults globally and for all ports.

### Mode

Switch mode, read-write.

## Examples

This example shows how to clear all the Cisco DP parameters back to the default settings.

```
B5(rw)->clear ciscodp
```

This example shows how to clear the Cisco DP status on port ge.1.5.

```
B5(rw)->clear ciscodp port status ge.1.5
```

# Configuring Link Layer Discovery Protocol and LLDP-MED

## Overview

The Link Layer Discovery Protocol (LLDP) provides an industry standard, vendor-neutral way to allow network devices to advertise their identities and capabilities on a local area network, and to discover that information about their neighbors.

LLDP-MED is an enhancement to LLDP that provides the following benefits:

- Auto-discovery of LAN policies, such as VLAN id, 802.1p priority, and DiffServ codepoint settings, leading to “plug-and-play” networking
- Device location and topology discovery, allowing creation of location databases and, in the case of VoIP, provision of E911 services
- Extended and automated power management of Power over Ethernet endpoints
- Inventory management, allowing network administrators to track their network devices and to determine their characteristics, such as manufacturer, software and hardware versions, and serial or asset numbers

The information sent by an LLDP-enabled device is extracted and tabulated by its peers. The communication can be done when information changes or on a periodic basis. The information tabulated is aged to ensure that it is kept up to date. Ports can be configured to send this information, receive this information, or both send and receive.

Either LLDP or LLDP-MED, but not both, can be used on an interface between two devices. A switch port uses LLDP-MED when it detects that an LLDP-MED-capable device is connected to it.

LLDP information is contained within a Link Layer Discovery Protocol Data Unit (LLDPDU) sent in a single 802.3 Ethernet frame. The information fields in LLDPDU are a sequence of short, variable-length, information elements known as TLVs — type, length, and value fields where:

- Type identifies what kind of information is being sent
- Length indicates the length of the information string in octets
- Value is the actual information that needs to be sent

The LLDP standard specifies that certain TLVs are mandatory in transmitted LLDPDUs, while others are optional. You can configure on a port-specific basis which optional LLDP and LLDP-MED TLVs should be sent in LLDPDUs.

## Configuration Tasks

The commands included in this implementation allow you to perform the following configuration tasks:

Step	Task	Command(s)
1.	Configure global system LLDP parameters	<code>set lldp tx-interval</code> <code>set lldp hold-multiplier</code> <code>set lldp trap-interval</code> <code>set lldp med-fast-repeat</code> <code>clear lldp</code>
2.	Enable/disable specific ports to: <ul style="list-style-type: none"> <li>Transmit and process received LLDPDUs</li> <li>Send LLDP traps</li> <li>Send LLDP-MED traps</li> </ul>	<code>set/clear lldp port status</code> <code>set/clear lldp port trap</code> <code>set/clear lldp port med-trap</code>
3.	Configure an ECS ELIN value for specific ports	<code>set/clear lldp port location-info</code>
4.	Configure Network Policy TLVs for specific ports	<code>set/clear lldp port network-policy</code>
5.	Configure which optional TLVs should be sent by specific ports. For example, if you configured an ECS ELIN and/or Network Policy TLVs, you must enable those optional TLVs to be transmitted on the specific ports.	<code>set/clear lldp tx-tlv</code>

## Commands

The commands used to review and configure the CDP discovery protocol are listed below.

For information about...	Refer to page...
<code>show lldp</code>	<a href="#">6-15</a>
<code>show lldp port status</code>	<a href="#">6-15</a>
<code>show lldp port trap</code>	<a href="#">6-16</a>
<code>show lldp port tx-tlv</code>	<a href="#">6-17</a>
<code>show lldp port location-info</code>	<a href="#">6-17</a>
<code>show lldp port local-info</code>	<a href="#">6-18</a>
<code>show lldp port remote-info</code>	<a href="#">6-21</a>
<code>show lldp port network-policy</code>	<a href="#">6-22</a>
<code>set lldp tx-interval</code>	<a href="#">6-23</a>
<code>set lldp hold-multiplier</code>	<a href="#">6-24</a>
<code>set lldp trap-interval</code>	<a href="#">6-24</a>
<code>set lldp med-fast-repeat</code>	<a href="#">6-25</a>
<code>set lldp port status</code>	<a href="#">6-25</a>
<code>set lldp port trap</code>	<a href="#">6-26</a>
<code>set lldp port med-trap</code>	<a href="#">6-26</a>
<code>set lldp port location-info</code>	<a href="#">6-27</a>
<code>set lldp port tx-tlv</code>	<a href="#">6-28</a>
<code>set lldp port network-policy</code>	<a href="#">6-29</a>

For information about...	Refer to page...
clear lldp	<a href="#">6-31</a>
clear lldp port status	<a href="#">6-31</a>
clear lldp port trap	<a href="#">6-32</a>
clear lldp port med-trap	<a href="#">6-32</a>
clear lldp port location-info	<a href="#">6-33</a>
clear lldp port network-policy	<a href="#">6-33</a>
clear lldp port tx-tlv	<a href="#">6-34</a>

## show lldp

Use this command to display LLDP configuration information.

### Syntax

```
show lldp
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display LLDP configuration information.

```
B5(ro)->show lldp
Message Tx Interval      : 30
Message Tx Hold Multiplier : 4
Notification Tx Interval : 5
MED Fast Start Count    : 3

Tx-Enabled Ports        : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
Rx-Enabled Ports        : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;

Trap-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
MED Trap-Enabled Ports  : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
```

## show lldp port status

Use this command to display the LLDP status of one or more ports. The command lists the ports that are enabled to send and receive LLDP PDUs. Ports are enabled or disabled with the [set lldp port status](#) command.

### Syntax

```
show lldp port status [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Displays LLDP status for one or a range of ports.
--------------------	--

---

## Defaults

If *port-string* is not specified, LLDP status information will be displayed for all ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display LLDP port status information for all ports.

```
B5(ro)->show lldp port status
```

```
Tx-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12
```

```
Rx-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12
```

# show lldp port trap

Use this command to display the ports that are enabled to send an LLDP notification when a remote system change has been detected or an LLDP-MED notification when a change in the topology has been sensed. Ports are enabled to send LLDP notifications with the [set lldp port trap](#) command and to send LLDP-MED notifications with the [set lldp port med-trap](#) command.

## Syntax

```
show lldp port trap [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Displays the port or range of ports that have been enabled to send LLDP and/or LLDP-MED notifications.
--------------------	---

---

## Defaults

If *port-string* is not specified, LLDP port trap information will be displayed for all ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display LLDP port trap information for all ports.

```
B5(ro)->show lldp port trap
```

```
Trap-Enabled Ports    :
```

```
MED Trap-Enabled Ports:
```



## show lldp port tx-tlv

Use this command to display information about which optional TLVs have been configured to be transmitted on ports. Ports are configured to send optional TLVs with the [set lldp port tx-tlv](#) command.

### Syntax

```
show lldp port tx-tlv [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays information about TLV configuration for one or a range of ports.
--------------------	--

### Defaults

If *port-string* is not specified, TLV configuration information will be displayed for all ports.

### Mode

Switch command, read-only.

### Example

This example shows how to display transmit TLV information for three ports.

```
B5(ro)->show lldp port tx-tlv ge.1.1-3
```

```
* Means TLV is supported and enabled on this port
```

```
o Means TLV is supported on this port
```

```
Means TLV is not supported on this port
```

```
Column Pro Id uses letter notation for enable: s-stp, l-lacp, g-gvrp
```

Ports	Port Desc	Sys Name	Sys Desc	Sys Cap	Mgmt Addr	Vlan Id	Pro Id	MAC PHY	PoE	Link Aggr	Max Frame	MED Cap	MED Pol	MED Loc	MED PoE
ge.1.1	*	*	*	*	*	*	slg	*	*	*	*	*		*	
ge.1.2	*	*	*	*	*	*	slg	*	*	*	*				
ge.1.3	*	*	*	*	*	*	slg	*	*	*	*	*		*	

## show lldp port location-info

Use this command to display configured location information for one or more ports. Ports are configured with a location value using the [set lldp port location-info](#) command.

### Syntax

```
show lldp port location-info [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays port location information for one or a range of ports.
--------------------	--

## Defaults

If *port-string* is not specified, port location configuration information will be displayed for all ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display port location information for three ports.

```
B5(ro)->show lldp port location-info ge.1.1-3
```

Ports	Type	Location
ge.1.1	ELIN	1234567890
ge.1.2	ELIN	1234567890
ge.1.3	ELIN	1234567890

# show lldp port local-info

Use this command to display the local system information stored for one or more ports. You can use this information to detect misconfigurations or incompatibilities between the local port and the attached endpoint device (remote port).

## Syntax

```
show lldp port local-info [port-string]
```

## Parameters

<i>port-string</i>	(Optional) Displays local system information for one or a range of ports.
--------------------	---

## Defaults

If *port-string* is not specified, local system information will be displayed for all ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display the local system information stored for port ge.4.1. [Table 6-4](#) describes the output fields of this command.

```
B5(rw)->show lldp port local-info ge.4.1
```

```
Local Port   : ge.4.1           Local Port Id: ge.4.1
-----
Port Desc    : ... 1000BASE-TX RJ45 Gigabit Ethernet Frontpanel Port
Mgmt Addr    : 10.21.64.100
Chassis ID   : 00-E0-63-93-74-A5
Sys Name     : LLDP PoE test Chassis
Sys Desc     : Enterasys Networks, Inc.
Sys Cap Supported/Enabled : bridge,router/bridge
```

```

Auto-Neg Supported/Enabled      : yes/yes
Auto-Neg Advertised            : 10BASE-T, 10BASE-TFD,
                                100BASE-TX, 100BASE-TXFD,
                                1000BASE-TFD,
                                Bpause
Operational Speed/Duplex/Type  : 100 full tx
Max Frame Size (bytes)         : 1522

Vlan Id                        : 1
LAG Supported/Enabled/Id       : no/no/0
Protocol Id : Spanning Tree v-3 (IEEE802.1s)
                        LACP v-1
                        GVRP

Network Policy
(app/tag/vlanId/cos/dscp)      : voice/tagged/10/3/5
                                voice signaling/tagged/10/3/5
                                guest voice/tagged/10/3/5
                                guest voice signaling/tagged/10/3/5
                                softphone voice/tagged/10/3/5
                                video conferencing/tagged/10/3/5
                                streaming video/tagged/10/3/5
                                video signaling/tagged/10/3/5

ECS ELIN                       : 1234567890123456789012345

PoE Device                     : PSE device
PoE Power Source               : primary
PoE MDI Supported/Enabled     : yes/yes
PoE Pair Controllable/Used    : false/spare
PoE Power Class                : 2
PoE Power Limit (mW)          : 15400
PoE Power Priority             : high

```

[Table 6-4](#) describes the information displayed by the **show lldp port local-info** command.

**Table 6-4 show lldp port local-info Output Details**

Output Field	What it Displays...
Local Port	Identifies the port for which local system information is displayed.
Local Port Id	Mandatory basic LLDP TLV that identifies the port transmitting the LLDPDU. Value is ifName object defined in RFC 2863.
Port Desc	Optional basic LLDP TLV. Value is ifDescr object defined in RFC 2863.
Mgmt Addr	Optional basic LLDP TLV. IPv4 address of host interface.
Chassis ID	Mandatory basic LLDP TLV that identifies the chassis transmitting the LLDPDU. Value is MAC address of chassis.
Sys Name	Optional basic LLDP TLV. Value is the administratively assigned name for the system.
Sys Desc	Optional basic LLDP TLV. Value is sysDescr object defined in RFC 3418.
Sys Cap Supported/Enabled	Optional basic LLDP TLV. System capabilities, value can be bridge and/or router.
Auto-Neg Supported/Enabled	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Auto-negotiation supported and enabled settings should be the same on the two systems attached to the same link.
Auto-Neg Advertised	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Lists the configured advertised values on the port.

**Table 6-4 show lldp port local-info Output Details (Continued)**

Output Field	What it Displays...
Operational Speed/Duplex/Type	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Lists the operational MAU type, duplex, and speed of the port. If the received TLV indicates that auto-negotiation is supported but not enabled, these values will be used by the port.
Max Frame Size (bytes)	IEEE 802.3 Extensions Maximum Frame Size TLV. Value indicates maximum frame size capability of the device's MAC and PHY. In normal mode, max frame size is 1522 bytes. In jumbo mode, max frame size is 10239 bytes.
Vlan Id	IEEE 802.1 Extensions Port VLAN ID TLV. Value is port VLAN ID (pvid).
LAG Supported/Enabled/Id	IEEE 802.3 Extensions Link Aggregation TLV. Values indicate whether the link associated with this port can be aggregated, whether it is currently aggregated, and if aggregated, the aggregated port identifier.
Protocol Id	IEEE 802.1 Extensions Protocol Identity TLV. Values can include Spanning tree, LACP, and GARP protocols and versions. Only those protocols enabled on the port are displayed.
Network Policy (app/tag/vlanId/cos/dscp)	LLDP-MED Extensions Network Policy TLV. For all applications enabled on the port to be transmitted in a TLV, displays the application name, VLAN type (tagged or untagged), VLAN Id, and both the Layer 2 and Layer 3 priorities associated with the application.
ECS ELIN	LLDP-MED Extensions Location Identification TLV. Emergency Call Services (ECS) Emergency Location Identification Number (ELIN) is currently the only type supported. Value is the ELIN configured on this port.
PoE Device	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Value is the Power Type of the device. On a switch port, the value is Power Sourcing Entity (PSE).
PoE Power Source	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Value can be primary or backup, indicating whether the PSE is using its primary or backup power source.
PoE MDI Supported/Enabled	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether sending the Power via MDI TLV is supported/enabled. Value can be yes or no.
PoE Pair Controllable/Used	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether pair selection can be controlled on the given port (refer to RFC 3621). Value for Controllable can be true or false. Value of Used can be signal (signal pairs only are in use) or spare (spare pairs only are in use).
PoE Power Class	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power class supplied by the port. Value can range from 0 to 4.
PoE Power Limit (mW)	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the total power the port is capable of sourcing over a maximum length cable, based on its current configuration, in milli-Watts.
PoE Power Priority	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power priority configured on the port. Value can be critical, high, or low.

## show lldp port remote-info

Use this command to display the remote system information stored for a remote device connected to a local port. You can use this information to detect misconfigurations or incompatibilities between the local port and the attached endpoint device (remote port).

### Syntax

```
show lldp port remote-info [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays remote system information for one or a range of ports.
--------------------	--

### Defaults

If *port-string* is not specified, remote system information will be displayed for all ports.

### Mode

Switch command, read-only.

### Example

This example shows how to display the remote system information stored for port ge.3.1. The remote system information was received from an IP phone, which is an LLDP-MED-enabled device. [Table 6-5](#) describes the output fields that are unique to the remote system information displayed for a MED-enabled device.

```
B5(ro)->show lldp port remote-info ge.3.1
Local Port   : ge.3.1      Remote Port Id : 00-09-6e-0e-14-3d
-----
Mgmt Addr    : 0.0.0.0
Chassis ID   : 0.0.0.0
Device Type  : Communication Device Endpoint (class III)
Sys Name     : AVE0E143D
Sys Cap Supported/Enabled : bridge,telephone/bridge

Auto-Neg Supported/Enabled : yes/yes
Auto-Neg Advertised        : 10BASE-T, 10BASE-TFD
                           : 100BASE-TX, 100BASE-TXFD
                           : pause, Spause

Operational Speed/Duplex/Type : 100/full/TX

Network Policy
(app/tag/vlanId/cos/dscp)    : voice/untagged/0/6/46

Hardware Revision           : 4610D01A
Firmware Revision          : b10d01b2_7.bin
Software Revision          : a10d01b2_7.bin
Serial Number               : 05GM42004348
Manufacturer                : Avaya
Model Number                : 4610
```

Note that the information fields displayed by the **show lldp port remote-info** command will vary, depending on the type of remote device that is connected to the port.

Table 6-5 describes the output fields that are unique to the remote system information database. Refer to Table 6-4 on page 19 for descriptions of the information fields that are common to both the local and the remote system information databases.

**Table 6-5 show lldp port remote-info Output Display**

Output Field	What it Displays...
Remote Port Id	Displays whatever port Id information received in the LLDPDU from the remote device. In this case, the port Id is MAC address of remote device.
Device Type	Mandatory LLDP-MED Capabilities TLV. Displayed only when the port is connected to an LLDP-MED-capable endpoint device.
Hardware Revision	LLDP-MED Extensions Inventory Management TLV component.
Firmware Revision	LLDP-MED Extensions Inventory Management TLV component.
Software Revision	LLDP-MED Extensions Inventory Management TLV component.
Serial Number	LLDP-MED Extensions Inventory Management TLV component.
Manufacturer	LLDP-MED Extensions Inventory Management TLV component.
Model Number	LLDP-MED Extensions Inventory Management TLV component.
Asset ID	LLDP-MED Extensions Inventory Management TLV component. In the above example, no asset ID was received from the remote device so the field is not displayed.

## show lldp port network-policy

Use this command to display LLDP port network policy configuration information. Network policy information is configured using the [set lldp port network-policy](#) command.

### Syntax

```
show lldp port network-policy {all | voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} [port-string]
```

### Parameters

<b>all</b>	Displays information about all network policy applications.
<b>voice</b>	Displays information about only the voice application type.
<b>voice-signaling</b>	Displays information about only the voice signaling application type.
<b>guest-voice</b>	Displays information about only the guest voice application type.
<b>guest-voice-signaling</b>	Displays information about only the guest voice signaling application type.
<b>softphone-voice</b>	Displays information about only the softphone voice application type.
<b>video-conferencing</b>	Displays information about only the video conferencing application type.
<b>streaming-video</b>	Displays information about only the streaming video application type.
<b>video-signaling</b>	Displays information about only the video signaling application type.

---

<i>port-string</i>	(Optional) Displays information about LLDP network policy for one or a range of ports.
--------------------	--

---

## Defaults

If *port-string* is not specified, only non-default values will be displayed for all ports that have non-default values configured.

If a *port-string* is specified, then all values, default and non-default, are displayed for the specified ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display all LLDP network policy information for ge.1.1.

```
B5(ro)->show lldp port network-policy all ge.1.1
```

Ports	Application	State	Tag	Vlan-Id	Cos	Dscp
-----	-----	-----	-----	-----	---	---
ge.1.1	voice	enabled	untagged	1	0	0
	voice signaling	enabled	untagged	1	0	0
	guest voice	enabled	untagged	1	0	0
	guest voice signaling	enabled	untagged	1	0	0
	softphone voice	enabled	untagged	1	0	0
	video conferencing	enabled	untagged	1	0	0
	streaming video	enabled	untagged	1	0	0
	video signaling	enabled	untagged	1	0	0

## set lldp tx-interval

Use this command to set the time, in seconds, between successive LLDP frame transmissions initiated by changes in the LLDP local system information.

## Syntax

```
set lldp tx-interval frequency
```

## Parameters

---

<i>frequency</i>	Specifies the number of seconds between transmissions of LLDP frames. Value can range from 5 to 32,768 seconds. The default is 30 seconds.
------------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example sets the transmit interval to 20 seconds.

```
B5(rw)->set lldp tx-interval 20
```

## set lldp hold-multiplier

Use this command to set the time-to-live value used in LLDP frames sent by this device. The time-to-live for LLDPDU data is calculated by multiplying the transmit interval by the hold multiplier value.

### Syntax

```
set lldp hold-multiplier multiplier-val
```

### Parameters

---

<i>multiplier-val</i>	Specifies the multiplier to apply to the transmit interval to determine the time-to-live value. Value can range from 2 to 10. Default value is 4.
-----------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example sets the transmit interval to 20 seconds and the hold multiplier to 5, which will configure a time-to-live of 100 to be used in the TTL field in the LLDPDU header.

```
B5(rw)->set lldp tx-interval 20
B5(rw)->set lldp hold-multiplier 5
```

## set lldp trap-interval

Use this command to set the minimum interval between LLDP notifications sent by this device. LLDP notifications are sent when a remote system change has been detected.

### Syntax

```
set lldp trap-interval frequency
```

### Parameters

---

<i>frequency</i>	Specifies the minimum time between LLDP trap transmissions, in seconds. The value can range from 5 to 3600 seconds. The default value is 5 seconds.
------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.



## Example

This example sets the minimum interval between LLDP traps to 10 seconds.

```
B5(rw)->set lldp trap-interval 10
```

## set lldp med-fast-repeat

Network connectivity devices transmit only LLDP TLVs in LLDPDUs until they detect that an LLDP-MED endpoint device has connected to a port. At that point, the network connectivity device starts sending LLDP-MED TLVs at a fast start rate on that port. Use this command to set the number of successive LLDPDUs (with LLDP-MED TLVs) to be sent for one complete fast start interval.

### Syntax

```
set lldp med-fast-repeat count
```

### Parameters

<i>count</i>	Specifies the number of fast start LLDPDUs to be sent when an LLDP-MED endpoint device is detected. Value can range from 1 to 10. Default is 3.
--------------	---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example sets the number of fast start LLDPDUs to be sent to 4.

```
B5(rw)->set lldp med-fast-repeat 4
```

## set lldp port status

Use this command to enable or disable transmitting and processing received LLDPDUs on a port or range of ports.

### Syntax

```
set lldp port status {tx-enable | rx-enable | both | disable} port-string
```

### Parameters

<b>tx-enable</b>	Enables transmitting LLDPDUs on the specified ports.
<b>rx-enable</b>	Enables receiving and processing LLDPDUs from remote systems on the specified ports.
<b>both</b>	Enables both transmitting and processing received LLDPDUs on the specified ports.
<b>disable</b>	Disables both transmitting and processing received LLDPDUs on the specified ports.

---

<i>port-string</i>	Specifies the port or range of ports to be affected.
--------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example enables both transmitting LLDPDUs and receiving and processing LLDPDUs from remote systems on ports ge.1.1 through ge.1.6.

```
B5(rw)->set lldp port status both ge.1.1-6
```

## set lldp port trap

Use this command to enable or disable sending LLDP notifications (traps) when a remote system change is detected.

### Syntax

```
set lldp port trap {enable | disable} port-string
```

### Parameters

---

<b>enable</b>	Enable transmitting LLDP traps on the specified ports.
<b>disable</b>	Disable transmitting LLDP traps on the specified ports.
<i>port-string</i>	Specifies the port or range of ports to be affected.

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example enables transmitting LLDP traps on ports ge.1.1 through ge.1.6.

```
B5(rw)->set lldp port trap enable ge.1.1-6
```

## set lldp port med-trap

Use this command to enable or disable sending an LLDP-MED notification when a change in the topology has been sensed on the port (that is, a remote endpoint device has been attached or removed from the port).

### Syntax

```
set lldp port med-trap {enable | disable} port-string
```

## Parameters

<b>enable</b>	Enables transmitting LLDP-MED traps on the specified ports.
<b>disable</b>	Disables transmitting LLDP-MED traps on the specified ports.
<i>port-string</i>	Specifies the port or range of ports to be affected.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example enables transmitting LLDP-MED traps on ports ge.1.1 through ge.1.6.

```
B5(rw)->set lldp port med-trap enable ge.1.1-6
```

# set lldp port location-info

Use this command to configure LLDP-MED location information on a port or range of ports. Currently, only Emergency Call Services (ECS) Emergency Location Identification Number (ELIN) is supported.

## Syntax

```
set lldp port location-info elin elin-string port-string
```

## Parameters

<b>elin</b>	Specifies that the ECS ELIN data format is to be used.
<i>elin-string</i>	Specifies the location identifier. Value can be from 10 to 25 numerical characters.
<i>port-string</i>	Specifies the port or range of ports to be affected.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

After you configure a location information value, you must also configure the port to send the Location Information TLV with the [set lldp port tx-tlv](#) command. This example configures the ELIN identifier 5551234567 on ports ge.1.1 through ge.1.6 and then configures the ports to send the Location Information TLV.

```
B5(rw)->set lldp port location-info 5551234567 ge.1.1-6
B5(rw)->set lldp port tx-tlv med-loc ge.1.1-6
```

## set lldp port tx-tlv

Use this command to select the optional LLDP and LLDP-MED TLVs to be transmitted in LLDPDUs by the specified port or ports. Use the [show lldp port local-info](#) command to display the values of these TLVs for the port.

### Syntax

```
set lldp port tx-tlv {[all] | [port-desc] [sys-name] [sys-desc] [sys-cap] [mgmt-addr] [vlan-id] [stp] [lACP] [gvrp] [mac-phy] [poe] [link-aggr] [max-frame] [med-cap] [med-pol] [med-loc] [med-poe]} port-string
```

### Parameters

<b>all</b>	Adds all optional TLVs to transmitted LLDPDUs.
<b>port-desc</b>	Port Description optional basic LLDP TLV. Value sent is ifDescr object defined in RFC 2863.
<b>sys-name</b>	System Name optional basic LLDP TLV. Value sent is the administratively assigned name for the system.
<b>sys-desc</b>	System Description optional basic LLDP TLV. Value sent is sysDescr object defined in RFC 3418.
<b>sys-cap</b>	System Capabilities optional basic LLDP TLV. For a network connectivity device, value sent can be bridge and/or router.
<b>mgmt-addr</b>	Management Address optional basic LLDP TLV. Value sent is IPv4 address of host interface.
<b>vlan-id</b>	Port VLAN ID IEEE 802.1 Extensions TLV. Value sent is port VLAN ID (PVID).
<b>stp</b>	Spanning Tree information defined by Protocol Identity IEEE 802.1 Extensions TLV. If STP is enabled on the port, value sent includes version of protocol being used.
<b>lACP</b>	LACP information defined by Protocol Identity IEEE 802.1 Extensions TLV. If LACP is enabled on the port, value sent includes version of protocol being used.
<b>gvrp</b>	GVRP information defined by Protocol Identity IEEE 802.1 Extensions TLV. If LACP is enabled on the port, value sent includes version of protocol being used.
<b>mac-phy</b>	MAC-PHY Configuration/Status IEEE 802.3 Extensions TLV. Value sent includes the operational MAU type, duplex, and speed of the port.
<b>poe</b>	Power via MDI IEEE 802.3 Extensions TLV. Values sent include whether pair selection can be controlled on port, and the power class supplied by the port. Only valid for PoE-enabled ports.
<b>link-aggr</b>	Link Aggregation IEEE 802.3 Extensions TLV. Values sent indicate whether the link associated with this port can be aggregated, whether it is currently aggregated, and if aggregated, the aggregated port identifier.
<b>max-frame</b>	Maximum Frame Size IEEE 802.3 Extensions TLV. Value sent indicates maximum frame size of the port's MAC and PHY.

<b>med-cap</b>	LLDP-MED Capabilities TLV. Value sent indicates the capabilities (whether the device supports location information, network policy, extended power via MDI) and Device Type (network connectivity device) of the sending device.
<b>med-pol</b>	LLDP-MED Network Policy TLV. Values sent include application name, VLAN type (tagged or untagged), VLAN ID, and both Layer 2 and Layer 3 priorities associated with application, for all applications enabled on the port. See the <a href="#">set lldp port network-policy</a> command for more information.
<b>med-loc</b>	LLDP-MED Location Identification TLV. Value sent is the ECS ELIN value configured on the port. See the <a href="#">set lldp port location-info</a> command for more information.
<b>med-poe</b>	LLDP-MED Extended Power via MDI TLV. Values sent include the Power Limit (total power the port is capable of sourcing over a maximum length cable) and the power priority configured on the port. Only valid for PoE-enabled ports.
<i>port-string</i>	Specifies the port or range of ports to be affected.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example configures the management address, MED capability, MED network policy, and MED location identification TLVs to be sent in LLDPDUs by port `ge.1.1`.

```
B5(rw)->set lldp port tx-tlv mgmt-addr med-cap med-pol med-loc ge.1.1
```

# set lldp port network-policy

Use this command to configure LLDP network policies for a set of applications on a port or range of ports. The policies configured with this command are sent in LLDPDUs as LLDP-MED Network Policy TLVs. Multiple Network Policy TLVs can be sent in a single LLDPDU.

## Syntax

```
set lldp port network-policy {all | voice | voice-signaling | guest-voice |
guest-voice-signaling | softphone-voice | video-conferencing | streaming-video |
video-signaling} [state {enable | disable}] [tag {tagged | untagged}]
[vid {vlan-id | dot1p}] [cos cos-value] [dscp dscp-value] port-string
```

## Parameters

<b>all</b>	Configures all applications.
<b>voice</b>	Configures the voice application.
<b>voice-signaling</b>	Configures the voice signaling application.  This application will not be advertised if the <b>voice</b> application is configured with the same parameters.

<b>guest-voice</b>	Configures the guest voice application.
<b>guest-voice-signaling</b>	Configures the guest voice signaling application. This application will not be advertised if the <b>guest-voice</b> application is configured with the same parameters.
<b>softphone-voice</b>	Configures the softphone voice application.
<b>video-conferencing</b>	Configures the video conferencing application.
<b>streaming-video</b>	Configures the streaming video application.
<b>video-signaling</b>	Configures the video signaling application. This application will not be advertised if the <b>video-conferencing</b> application is configured with the same parameters.
<b>state enable   disable</b>	(Optional) Enables or disables advertising the application information being configured.
<b>tag tagged   untagged</b>	(Optional) Indicates whether the application being configured is using a tagged or untagged VLAN. If untagged, both the VLAN ID and the CoS priority fields are ignored and only the DSCP value has relevance.
<b>vid <i>vlan-id</i>   dot1p</b>	(Optional) VLAN identifier for the port. The value of <i>vlan-id</i> can range from 1 to 4093.  Use <b>dot1p</b> if the device is using priority tagged frames, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used.
<b>cos <i>cos-value</i></b>	(Optional) Specifies the Layer 2 priority to be used for the application being configured. The value can range from 0 to 7. A value of 0 represents use of the default priority as defined in IEEE 802.1D.
<b>dscp <i>dscp-value</i></b>	(Optional) Specifies the DSCP value to be used to provide Diffserv node behavior for the application being configured. The value can range from 0 to 63. A value of 0 represents use of the default DSCP value as defined in RFC 2475.
<b><i>port-string</i></b>	Specifies the port or range of ports to be affected.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This feature allows administrators to quickly provision LLDP end-points via the switch. LLDP clients will use these LLDP network policy parameters for traffic originating from the end-point.

As described in the ANSI/TIA Standards document 1057, the Network Policy TLV is “intended for use with applications that have specific real-time network policy requirements, such as interactive voice and/or video services” and should be implemented only on direct links between network connectivity devices and endpoint devices. Refer to the ANSI/TIA Standards document 1057 for descriptions of the application types.

After you configure Network Policy TLVs, you must also configure the port to send the Network Policy TLV with the `set lldp port tx-tlv` command.

### Example

This example configures the voice application TLV on port ge.2.1 and then configures the port to send the Network Policy TLV.

```
B5(rw)->set lldp port network-policy voice state enable tag tagged vlan dot1p
ge.2.1
B5(rw)->set lldp port tx-tlv med-pol ge.2.1
```

## clear lldp

Use this command to return LLDP parameters to their default values.

### Syntax

```
clear lldp {all | tx-interval | hold-multiplier | trap-interval | med-fast-repeat}
```

### Parameters

<b>all</b>	Returns <b>all</b> LLDP configuration parameters to their default values, including port LLDP configuration parameters.
<b>tx-interval</b>	Returns the number of seconds between transmissions of LLDP frames to the default of 30 seconds.
<b>hold-multiplier</b>	Returns the multiplier to apply to the transmit interval to determine the time-to-live value to the default value of 4.
<b>trap-interval</b>	Returns the minimum time between LLSP trap transmissions to the default value of 5 seconds.
<b>med-fast-repeat</b>	Returns the number of fast start LLDPDUs to be sent when an LLDP-MED endpoint device is detected to the default of 3.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example returns the transmit interval to the default value of 30 seconds.

```
B5(rw)->clear lldp tx-interval
```

## clear lldp port status

Use this command to return the port status to the default value of both (both transmitting and processing received LLDPDUs are enabled).

### Syntax

```
clear lldp port status port-string
```

## Parameters

---

<i>port-string</i>	Specifies the port or range of ports to be affected.
--------------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example returns port `ge.1.1` to the default state of enabled for both transmitting and processing received LLDPDUs.

```
B5(rw)->clear lldp port status ge.1.1
```

# clear lldp port trap

Use this command to return the port LLDP trap setting to the default value of disabled.

## Syntax

```
clear lldp port trap port-string
```

## Parameters

---

<i>port-string</i>	Specifies the port or range of ports to be affected.
--------------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example returns port `ge.1.1` to the default LLDP trap state of disabled.

```
B5(rw)->clear lldp port trap ge.1.1
```

# clear lldp port med-trap

Use this command to return the port LLDP-MED trap setting to the default value of disabled.

## Syntax

```
clear lldp port med-trap port-string
```

## Parameters

---

<i>port-string</i>	Specifies the port or range of ports to be affected.
--------------------	--

---



## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example returns port `ge.1.1` to the default LLDP-MED trap state of disabled.

```
B5(rw)->clear lldp port med-trap ge.1.1
```

# clear lldp port location-info

Use this command to return the port ECS ELIN location setting to the default value of null.

## Syntax

```
clear lldp port location-info elin port-string
```

## Parameters

<b>elin</b>	Specifies that the ECS ELIN location information value should be cleared.
<i>port-string</i>	Specifies the port or range of ports to be affected.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example returns the location information ELIN value on port `ge.1.1` to the default value of null.

```
B5(rw)->clear lldp port location-info elin ge.1.1
```

# clear lldp port network-policy

Use this command to return LLDP network policy for a set of applications on a port or range of ports to default values.

## Syntax

```
clear lldp port network-policy {all | voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} {[state] [tag] [vid] [cos] [dscp]} port-string
```

## Parameters

<b>all</b>	Applies command to all applications.
------------	--------------------------------------

<b>voice</b>	Applies command to the voice application.
<b>voice-signaling</b>	Applies command to the voice signaling application.
<b>guest-voice</b>	Applies command to the guest voice application.
<b>guest-voice-signaling</b>	Applies command to the guest voice signaling application.
<b>softphone-voice</b>	Applies command to the softphone voice application.
<b>video-conferencing</b>	Applies command to the video conferencing application.
<b>streaming-video</b>	Applies command to the streaming video application.
<b>video-signaling</b>	Applies command to the video signaling application.
<b>state</b>	(Optional) Clears the state of advertising the application information being configured to disabled.
<b>tag</b>	(Optional) Clears the tag value of the application being configured to untagged.
<b>vid</b>	(Optional) Clears the VLAN identifier for the port to the default value of 1.
<b>cos</b>	(Optional) Clears the Layer 2 priority to be used for the application being configured to the default value of 0. (A value of 0 represents use of the default priority as defined in IEEE 802.1D.)
<b>dscp</b>	(Optional) Clears the DSCP value to be used to provide Diffserv node behavior for the application being configured to the default value of 0. (A value of 0 represents use of the default DSCP value as defined in RFC 2475.)
<i>port-string</i>	Specifies the port or range of ports to be affected.

## Defaults

At least one application (or **all**) and one policy parameter must be specified.

## Mode

Switch command, read-write.

## Example

This example returns all network policy values for all applications on port ge.1.1 to their default values.

```
B5(rw)->clear lldp port network-policy all state tag vid cos dscp ge.1.1
```

## clear lldp port tx-tlv

Use this command to clear the optional LLDP and LLDP-MED TLVs to be transmitted in LLDPDUs by the specified port or ports to the default value of disabled.

## Syntax

```
clear lldp port tx-tlv {[all] | [port-desc] [sys-name] [sys-desc] [sys-cap] [mgmt-addr] [vlan-id] [stp] [lACP] [gvrp] [mac-phy] [poe] [link-aggr] [max-frame] [med-cap] [med-pol] [med-loc] [med-poe]} port-string
```

## Parameters

<b>all</b>	Disables all optional TLVs from being transmitted in LLDPDUs.
<b>port-desc</b>	Disables the Port Description optional basic LLDP TLV from being transmitted in LLDPDUs.
<b>sys-name</b>	Disables the System Name optional basic LLDP TLV from being transmitted in LLDPDUs.
<b>sys-desc</b>	Disables the System Description optional basic LLDP TLV from being transmitted in LLDPDUs.
<b>sys-cap</b>	Disables the System Capabilities optional basic LLDP TLV from being transmitted in LLDPDUs.
<b>mgmt-addr</b>	Disables the Management Address optional basic LLDP TLV from being transmitted in LLDPDUs.
<b>vlan-id</b>	Disables the Port VLAN ID IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
<b>stp</b>	Disables the Spanning Tree information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
<b>lacp</b>	Disables the LACP information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
<b>gvrp</b>	Disables the GVRP information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
<b>mac-phy</b>	Disables the MAC-PHY Configuration/Status IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
<b>poe</b>	Disables the Power via MDI IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs. Only valid for PoE-enabled ports.
<b>link-aggr</b>	Disables the Link Aggregation IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
<b>max-frame</b>	Disables the Maximum Frame Size IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
<b>med-cap</b>	Disables the LLDP-MED Capabilities TLV from being transmitted in LLDPDUs.
<b>med-pol</b>	Disables the LLDP-MED Network Policy TLV from being transmitted in LLDPDUs.
<b>med-loc</b>	Disables the LLDP-MED Location Identification TLV from being transmitted in LLDPDUs.
<b>med-poe</b>	Disables the LLDP-MED Extended Power via MDI TLV from being transmitted in LLDPDUs. Only valid for PoE-enabled ports.
<i>port-string</i>	Specifies the port or range of ports to be affected.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example disables the management address, MED capability, MED network policy, and MED location identification TLVs from being sent in LLDPDUs by port `ge.1.1`.

```
B5(rw)->clear lldp port tx-tlv mgmt-addr med-cap med-pol med-loc ge.1.1
```

## Port Configuration

This chapter describes the Port Configuration set of commands and how to use them.

For information about...	Refer to page...
<a href="#">Port Configuration Summary</a>	<a href="#">7-1</a>
<a href="#">Reviewing Port Status</a>	<a href="#">7-2</a>
<a href="#">Disabling / Enabling and Naming Ports</a>	<a href="#">7-7</a>
<a href="#">Setting Speed and Duplex Mode</a>	<a href="#">7-11</a>
<a href="#">Enabling / Disabling Jumbo Frame Support</a>	<a href="#">7-14</a>
<a href="#">Setting Auto-Negotiation and Advertised Ability</a>	<a href="#">7-16</a>
<a href="#">Setting Flow Control</a>	<a href="#">7-22</a>
<a href="#">Setting Port Link Traps and Link Flap Detection</a>	<a href="#">7-24</a>
<a href="#">Configuring Broadcast Suppression</a>	<a href="#">7-35</a>
<a href="#">Port Mirroring</a>	<a href="#">7-38</a>
<a href="#">Link Aggregation Control Protocol (LACP)</a>	<a href="#">7-44</a>
<a href="#">Configuring Protected Ports</a>	<a href="#">7-58</a>

## Port Configuration Summary

### Port String Syntax Used in the CLI

Commands requiring a *port-string* parameter use the following syntax to designate port type, slot location, and port number:

**port type.unit\_or\_slot number.port number**

Where **port type** can be:

**fe** for 100-Mbps Ethernet

**ge** for 1-Gbps Ethernet

**tg** for 10-Gbps Ethernet

**host** for the host port

**vlan** for vlan interfaces

**lag** for IEEE802.3 link aggregation ports

Where **unit\_or\_slotnumber** can be:

**1 - 8** for switch units in a stack

Where **port number** depends on the device. The highest valid port number is dependent on the number of ports in the device and the port type.

### Port Slot/Unit Parameters Used in the CLI

The “unit” parameter is often used interchangeably with “module” in the standalone switch CLI to indicate a module slot location.

### Examples



**Note:** You can use a wildcard (\*) to indicate all of an item. For example, fe.3.\* would represent all 100Mbps Ethernet (fe) ports in slot 3, and ge.3 \* would represent all 1-Gigabit Ethernet (ge) ports in slot 3.

This example shows the *port-string* syntax for specifying the 1-Gigabit Ethernet port 14 in unit 3.

```
ge . 3 . 14
```

This example shows the *port-string* syntax for specifying all 1-Gigabit Ethernet ports in unit 3 in the system.

```
ge . 3 . *
```

This example shows the *port-string* syntax for specifying all ports (of any interface type) in the system.

```
* . * . *
```

## Reviewing Port Status

### Purpose

To display operating status, duplex mode, speed, port type, and statistical information about traffic received and transmitted through one or all switch ports on the device.

### Commands

For information about...	Refer to page...
show port	<a href="#">7-3</a>
show port status	<a href="#">7-3</a>
show port counters	<a href="#">7-4</a>
clear port counters	<a href="#">7-6</a>
show port cablestatus	<a href="#">7-6</a>

## show port

Use this command to display whether or not one or more ports are enabled for switching.

### Syntax

```
show port [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays operational status for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

### Defaults

If *port-string* is not specified, operational status information for all ports will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display operational status information for ge.3.14:

```
B5(su)->show port ge.3.14
Port ge.3.14 enabled
```

## show port status

Use this command to display operating and admin status, speed, duplex mode and port type for one or more ports on the device.

### Syntax

```
show port status [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays status for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

### Defaults

If *port-string* is not specified, status information for all ports will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display status information for ge.1.1 and ge.1.2:

```
B5(su)->show port status ge.1.1-2
```

Port	Alias (truncated)	Oper Status	Admin Status	Speed (bps)	Duplex	Type
ge.1.47		Down	Up	N/A	N/A	RJ45
ge.1.48		Up	Up	1.0G	full	RJ45

Table 7-1 provides an explanation of the command output.

**Table 7-1 show port status Output Details**

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
Alias (truncated)	Alias configured for the port. For details on using the <b>set port alias</b> command, refer to <a href="#">“set port alias”</a> on page 7-9.
Oper Status	Operating status (up or down).
Admin Status	Whether the specified port is enabled (up) or disabled (down). For details on using the <b>set port disable</b> command to change the default port status of enabled, refer to <a href="#">“set port disable”</a> on page 7-8. For details on using the <b>set port enable</b> command to re-enable ports, refer to <a href="#">“set port enable”</a> on page 7-8.
Speed	Operational speed in Mbps or Kbps of the specified port. For details on using the <b>set port speed</b> command to change defaults, refer to <a href="#">“set port speed”</a> on page 7-12.
Duplex	Duplex mode (half or full) of the specified port. For details on using the <b>set port duplex</b> command to change defaults, refer to <a href="#">“Setting Auto-Negotiation and Advertised Ability”</a> on page 7-16.
Type	Physical port and interface type.

## show port counters

Use this command to display port counter statistics detailing traffic through the device and through all MIB2 network devices.

### Syntax

```
show port counters [port-string] [switch | mib2]
```

### Parameters

<i>port-string</i>	(Optional) Displays counter statistics for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>switch</b>   <b>mib2</b>	(Optional) Displays switch or MIB2 statistics. Switch statistics detail performance of the Enterasys B5 device. MIB2 interface statistics detail performance of all network devices.

### Defaults

If *port-string* is not specified, counter statistics will be displayed for all ports.

If **mib2** or **switch** are not specified, all counter statistics will be displayed for the specified port(s).

### Mode

Switch command, read-only.



## Examples

This example shows how to display all counter statistics, including MIB2 network traffic and traffic through the device for ge.3.1:

```
B5(su)->show port counters ge.3.1
```

```
Port: ge.3.1   MIB2 Interface: 1
```

```
No counter discontinuity time
```

```
-----
```

```
MIB2 Interface Counters
```

```
-----
```

```
In Octets                               0
In Unicast Pkts                         0
In Multicast Pkts                       0
In Broadcast Pkts                       0
In Discards                             0
In Errors                               0
Out Octets                               0
Out Unicasts Pkts                       0
Out Multicast Pkts                      0
Out Broadcast Pkts                      0
Out Errors                               0
```

```
802.1Q Switch Counters
```

```
-----
```

```
Frames Received                         0
Frames Transmitted                       0
```

This example shows how to display all ge.3.1 port counter statistics related to traffic through the device.

```
B5(su)->show port counters ge.3.1 switch
```

```
Port: ge.3.1           Bridge Port: 2
```

```
802.1Q Switch Counters
```

```
-----
```

```
Frames Received                         0
Frames Transmitted                       0
```

[Table 7-2](#) provides an explanation of the command output.

**Table 7-2 show port counters Output Details**

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">"Port String Syntax Used in the CLI"</a> on page 7-1.
MIB2 Interface	MIB2 interface designation.
Bridge Port	IEEE 802.1D bridge port designation.
MIB2 Interface Counters	MIB2 network traffic counts
802.1Q Switch Counters	Counts of frames received, transmitted, and filtered.

## clear port counters

Use this command to clear port counter statistics for a port or range of ports.

### Syntax

```
clear port counters [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Specifies the port or range of ports to clear port counter statistics.
--------------------	---

---

### Defaults

If no *port-string* is specified, port counters are cleared for all ports.

### Mode

Switch command, read-write

### Example

This example clears the port counters for ge.3.1.

```
B5(rw)->clear port counters ge.3.1
```

## show port cablestatus

Use this command to troubleshoot and locate faults in copper cable connections on a per port basis. This command is only available on switch platforms that provide 1 Gigabit Ethernet RJ45 ports.

### Syntax

```
show port cablestatus [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Specifies the port or ports to show status for.
--------------------	--

---

### Defaults

If no port is specified, information about all ports will be displayed.

### Mode

Switch command, read-only.

### Usage

For 1 Gigabit Ethernet RJ45 ports only, this command will display the status of the port's cable connection (described in [Table 7-3](#) below), and the approximate length of the cable attached to the port. If your switch platform does not support 1 GE RJ45 ports, this command will not be available.

If no cable is attached to the port, the status will be "Open" and no length will be shown. If the port is not a 1GE RJ45 port, the command will return a status of "Not Supported."

Since running the cable diagnostics may momentarily interrupt packet flow, a warning message is displayed and you are prompted to continue.

## Example

This example shows the cable status for port ge.1.1.

```
B5(su)->show port cablestatus ge.1.1
Warning: port(s) will be offline momentarily.
Do you want to continue (y/n) [n]?y
```

```
Port      Status      Length
-----
ge.1.1    Normal      3(m)-5(m)
```

[Table 7-3](#) provides an explanation of the command output.

**Table 7-3 show port cablestatus Output Details**

Output Field	What it displays...
Port	Lists the port designation.
Status	Indicates the status of the port. The value is one of the following: <b>Normal</b> = normal <b>Open</b> = no cable attached to port <b>Short</b> = detection of an inter-pair short <b>Fail</b> = unknown error or crosstalk <b>Detach</b> = indicates ports on stack units that are no longer present, but were previously connected <b>Not Supported</b> = ports other than 1GE RJ45 ports
Length	Indicates the approximate length of the cable attached to the port.

## Disabling / Enabling and Naming Ports

### Purpose

To disable and re-enable one or more ports, and to assign an alias to a port. By default, all ports are enabled at device startup. You may want to disable ports for security or to troubleshoot network issues. Ports may also be assigned an alias for convenience.

### Commands

For information about...	Refer to page...
set port disable	<a href="#">7-8</a>
set port enable	<a href="#">7-8</a>
show port alias	<a href="#">7-9</a>
set port alias	<a href="#">7-9</a>

## set port disable

Use this command to administratively disable one or more ports. When this command is executed, in addition to disabling the physical Ethernet link, the port will no longer learn entries in the forwarding database.

### Syntax

```
set port disable port-string
```

### Parameters

---

<i>port-string</i>	Specifies the port(s) to disable. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to disable ge.1.1:

```
B5(su)->set port disable ge.1.1
```

## set port enable

Use this command to administratively enable one or more ports.

### Syntax

```
set port enable port-string
```

### Parameters

---

<i>port-string</i>	Specifies the port(s) to enable. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to enable ge.1.3:

```
B5(su)->set port enable ge.1.3
```

## show port alias

Use this command to display the alias name for one or more ports.

### Syntax

```
show port alias [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays alias name(s) for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

---

### Defaults

If *port-string* is not specified, aliases for all ports will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display alias information for ports 1-3 on slot 3:

```
B5(rw)->show port alias ge.3.1-3
Port ge.3.1 user
Port ge.3.2 user
Port ge.3.3 Admin
```

## set port alias

Use this command to assign an alias name to a port.

### Syntax

```
set port alias port-string [name]
```

### Parameters

---

<i>port-string</i>	Specifies the port to which an alias will be assigned. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<i>name</i>	(Optional) Assigns an alias name to the port. If the alias name contains spaces, the text string must be surrounded by double quotes. Maximum length is 60 characters.

---

### Defaults

If *name* is not specified, the alias assigned to the port will be cleared.

### Mode

Switch command, read-write.

## Examples

This example shows how to assign the alias "Admin" to `ge.3.3`:

```
B5(rw)->set port alias ge.3.3 Admin
```

This example shows how to clear the alias for `ge.3.3`:

```
B5(rw)->set port alias ge.3.3
```

# Setting Speed and Duplex Mode

## Purpose

To review and set the operational speed in Mbps and the default duplex mode: **Half**, for half duplex, or **Full**, for full duplex for one or more ports.



**Note:** These settings only take effect on ports that have auto-negotiation disabled.

## Commands

For information about...	Refer to page...
show port speed	<a href="#">7-11</a>
set port speed	<a href="#">7-12</a>
show port duplex	<a href="#">7-12</a>
set port duplex	<a href="#">7-16</a>

## show port speed

Use this command to display the default speed setting on one or more ports.

### Syntax

```
show port speed [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays default speed setting(s) for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

### Defaults

If *port-string* is not specified, default speed settings for all ports will display.

### Mode

Switch command, read-only.

### Example

This example shows how to display the default speed setting for 1-Gigabit Ethernet port 14 in slot 3:

```
B5(su)->show port speed ge.3.14
default speed is 10 on port ge.3.14.
```

## set port speed

Use this command to set the default speed of one or more ports. This setting only takes effect on ports that have auto-negotiation disabled.

### Syntax

```
set port speed port-string {10 | 100 | 1000}
```

### Parameters

---

<i>port-string</i>	Specifies the port(s) for which to a speed value will be set. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
10   100   1000	Specifies the port speed. Valid values are: 10 Mbps, 100 Mbps, or 1000 Mbps.

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set ge.3.3 to a port speed of 10 Mbps:

```
B5(su)->set port speed ge.3.3 10
```

## show port duplex

Use this command to display the default duplex setting (half or full) for one or more ports.

### Syntax

```
show port duplex [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays default duplex setting(s) for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

---

### Defaults

If *port-string* is not specified, default duplex settings for all ports will be displayed.

### Mode

Switch command, read-only.



## Example

This example shows how to display the default duplex setting for Ethernet port 14 in slot 3:

```
B5(su)->show port duplex ge.3.14
default duplex mode is full on port ge.3.14.
```

## set port duplex

Use this command to set the default duplex type for one or more ports. This command will only take effect on ports that have auto-negotiation disabled.

### Syntax

```
set port duplex port-string {full | half}
```

### Parameters

<i>port-string</i>	Specifies the port(s) for which duplex type will be set. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>full   half</b>	Sets the port(s) to full-duplex or half-duplex operation.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set ge.1.17 to full duplex:

```
B5(su)->set port duplex ge.1.17 full
```

# Enabling / Disabling Jumbo Frame Support

## Purpose

To review, enable, and disable jumbo frame support on one or more ports. This allows Gigabit Ethernet ports to transmit frames up to 10 KB in size. LAG ports can also be configured for jumbo frame support.

## Commands

For information about...	Refer to page...
show port jumbo	<a href="#">7-14</a>
set port jumbo	<a href="#">7-15</a>
clear port jumbo	<a href="#">7-15</a>

## show port jumbo

Use this command to display the status of jumbo frame support and maximum transmission units (MTU) on one or more ports.

### Syntax

```
show port jumbo [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays the status of jumbo frame support for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

### Defaults

If *port-string* is not specified, jumbo frame support status for all ports will display.

### Mode

Switch command, read-only.

### Example

This example shows how to display the status of jumbo frame support for ge.1.1:

```
B5(su)->show port jumbo ge.1.1
```

```
Port Number   Jumbo Status   Max Frame Size
-----
ge.1.1        Enable         9216
```

## set port jumbo

Use this command to enable or disable jumbo frame support on one or more ports.

### Syntax

```
set port jumbo {enable | disable} [port-string]
```

### Parameters

<b>enable   disable</b>	Enables or disables jumbo frame support.
<i>port-string</i>	(Optional) Specifies the port(s) on which to disable or enable jumbo frame support. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

### Defaults

If *port-string* is not specified, jumbo frame support will be enabled or disabled on all ports.

### Mode

Switch command, read-write.

### Example

This example shows how to enable jumbo frame support for Gigabit Ethernet port 14 in unit/slot 3:

```
B5(su)->set port jumbo enable ge.3.14
```

## clear port jumbo

Use this command to reset jumbo frame support status to enabled on one or more ports.

### Syntax

```
clear port jumbo [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Specifies the port(s) on which to reset jumbo frame support status to enabled. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
--------------------	--

### Defaults

If *port-string* is not specified, jumbo frame support status will be reset on all ports.

### Mode

Switch command, read-write.

### Example

This example shows how to reset jumbo frame support status for Gigabit Ethernet port 14 in slot 3:

```
B5(su)->clear port jumbo ge.3.14
```

# Setting Auto-Negotiation and Advertised Ability

## Purpose

To review, disable or enable auto-negotiation, and to configure port advertisement for speed and duplex.

During auto-negotiation, the port “tells” the device at the other end of the segment what its capabilities and mode of operation are. If auto-negotiation is disabled, the port reverts to the values specified by default speed, default duplex, and the port flow control commands.

In normal operation, with all capabilities enabled, advertised ability enables a port to “advertise” that it has the ability to operate in any mode. The user may choose to configure a port so that only a portion of its capabilities are advertised and the others are disabled.



**Note:** Advertised ability can be activated only on ports that have auto-negotiation enabled.

## Commands

For information about...	Refer to page...
show port negotiation	<a href="#">7-16</a>
set port negotiation	<a href="#">7-17</a>
show port advertise	<a href="#">7-17</a>
set port advertise	<a href="#">7-18</a>
clear port advertise	<a href="#">7-19</a>
show port mdix	<a href="#">7-20</a>
set port mdix	<a href="#">7-20</a>

## show port negotiation

Use this command to display the status of auto-negotiation for one or more ports.

### Syntax

```
show port negotiation [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays auto-negotiation status for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
--------------------	--

### Defaults

If *port-string* is not specified, auto-negotiation status for all ports will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display auto-negotiation status for 1-Gigabit Ethernet port 14 in slot 3:

```
B5(su)->show port negotiation ge.3.14
auto-negotiation is enabled on port ge.3.14.
```

# set port negotiation

Use this command to enable or disable auto-negotiation on one or more ports.

## Syntax

```
set port negotiation port-string {enable | disable}
```

## Parameters

<i>port-string</i>	Specifies the port(s) for which to enable or disable auto-negotiation. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>enable   disable</b>	Enables or disables auto-negotiation.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to disable auto-negotiation on 1-Gigabit Ethernet port 3 in slot 14:

```
B5(su)->set port negotiation ge.3.14 disable
```

# show port advertise

Use this command to display port capability and advertisement as far as speed and duplex for auto-negotiation.

## Syntax

```
show port advertise [port-string]
```

## Parameters

<i>port-string</i>	(Optional) Displays advertised ability for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

## Defaults

If *port-string* is not specified, advertisement for all ports will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display advertisement status for Gigabit ports 13 and 14:

```
B5(su)->show port advertise ge.1.13-14
ge.1.13      capability      advertised      remote
-----
10BASE-T      yes              yes             yes
10BASE-TFD    yes              yes             yes
100BASE-TX     yes              yes             yes
100BASE-TXFD  yes              yes             yes
1000BASE-T     no               no              no
1000BASE-TFD  yes              yes             yes
pause         yes              yes             no

ge.1.14      capability      advertised      remote
-----
10BASE-T      yes              yes             yes
10BASE-TFD    yes              yes             yes
100BASE-TX     yes              yes             yes
100BASE-TXFD  yes              yes             yes
1000BASE-T     no               no              no
1000BASE-TFD  yes              yes             yes
pause         yes              yes             no
```

## set port advertise

Use this command to configure what a port will advertise for speed/duplex capabilities in auto-negotiation.

### Syntax

```
set port advertise {port-string}{10t | 10tfd | 100tx | 100txfd | 1000t | 1000tfd
| pause}
```

### Parameters

<i>port-string</i>	Select the ports for which to configure advertisements. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>10t</b>	Advertise 10BASE-T half duplex mode.
<b>10tfd</b>	Advertise 10BASE-T full duplex mode.
<b>100tx</b>	Advertise 100BASE-TX half duplex mode.
<b>100txfd</b>	Advertise 100BASE-TX full duplex mode.
<b>1000t</b>	Advertise 1000BASE-T half duplex mode.
<b>1000tfd</b>	Advertise 1000BASE-T full duplex mode.
<b>pause</b>	Advertise PAUSE for full-duplex links.

### Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to configure port 1 to advertise 1000BASE-T full duplex:

```
B5(su)->set port advertise ge.1.1 1000tfd
```

## clear port advertise

Use this command to configure a port to not advertise a specific speed/duplex capability when auto-negotiating with another port.

## Syntax

```
clear port advertise {port-string}{10t | 10tfd | 100tx | 100txfd | 1000t | 1000tfd  
| pause}
```

## Parameters

<i>port-string</i>	Clear advertisements for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>10t</b>	Do not advertise 10BASE-T half duplex mode.
<b>10tfd</b>	Do not advertise 10BASE-T full duplex mode.
<b>100tx</b>	Do not advertise 100BASE-TX half duplex mode.
<b>100txfd</b>	Do not advertise 100BASE-TX full duplex mode.
<b>1000t</b>	Do not advertise 1000BASE-T half duplex mode.
<b>1000tfd</b>	Do not advertise 1000BASE-T full duplex mode.
<b>pause</b>	Do not advertise PAUSE for full-duplex links.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to configure port 1 to not advertise 10 MB capability for auto-negotiation:

```
B5(su)->clear port advertise ge.1.1 10t 10tfd
```

## show port mdix

Use this command to display the status of cable connection type configuration mode for one or more ports. Switch ports can automatically detect and configure the required cable type, either straight through (MDI) or cross-over (MDIX), or the ports can be configured to only allow one type of cable type, either MDI or MDIX.

### Syntax

```
show port mdix {all|auto|forced-auto|mdi|mdix} [port-string]
```

### Parameters

<b>all</b>	Display information about all ports.
<b>auto</b>	Display information about the ports configured to automatically determine the required MDI/MDIX mode.
<b>forced-auto</b>	Display information about the ports forced automatically to determine the required MDI/MDIX mode.
<b>mdi</b>	Display information about the ports configured with MDI only mode.
<b>mdix</b>	Display information about the ports configured with MDIX only mode.
<i>port-string</i>	(Optional) Display the selected MDI/MDIX mode only for the port or ports specified.

### Defaults

If *port-string* is not specified, information is displayed for all ports.

### Mode

Switch command, read-only.

### Example

This example displays information about ports configured for MDIX only mode.

```
B5(su)->show port mdix mdix
```

```

Port Number   MDIX Mode
-----
ge.1.27       MDIX
ge.1.28       MDIX

```

## set port mdix

Use this command to configure cable connection type configuration mode for one or more ports.

### Syntax

```
set port mdix {auto|forced-auto|mdi|mdix} [port-string]
```

### Parameters

<b>auto</b>	Configure ports to automatically determine the required MDI/MDIX mode. This is the default condition.
<b>forced-auto</b>	Force ports to automatically determine the required MDI/MDIX mode.



---

<b>mdi</b>	Configure ports to use MDI mode only.
<b>mdix</b>	Configure ports to use MDIX mode only.
<i>port-string</i>	(Optional) Specify the port or ports to configure.

---

## Defaults

If *port-string* is not entered, all ports on the switch are configured.

## Mode

Switch command, read-write.

## Usage

By default, Enterasys Networks switch devices are configured to automatically detect the cable type connection, straight through (MDI) or cross-over (MDIX), required by the cable connected to the port. You can configure ports to only use MDI or MDIX connections with this command.

This command only configures Ethernet ports, and cannot be used to configure combo ports on the switch. Fiber ports always have a status of MDIX.

## Example

This example configures ports ge.1.1 and ge.1.2 to use MDIX mode.

```
B5(su)->set port mdix mdix ge.1.1-2
```

# Setting Flow Control

## Purpose

To review, enable or disable port flow control. Flow control is used to manage the transmission between two devices as specified by IEEE 802.3x to prevent receiving ports from being overwhelmed by frames from transmitting devices.

## Commands

For information about...	Refer to page...
show flowcontrol	<a href="#">7-22</a>
set flowcontrol	<a href="#">7-22</a>

## show flowcontrol

Use this command to display the flow control state.

### Syntax

```
show flowcontrol
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the port flow control state:

```
B5(su)->show flowcontrol  
Flow control status: enabled
```

## set flowcontrol

Use this command to enable or disable flow control.

### Syntax

```
set flowcontrol {enable | disable}
```

### Parameters

---

<b>enable   disable</b>	Enables or disables flow control settings.
-------------------------	--

---

**Defaults**

None.

**Mode**

Switch command, read-write.

**Example**

This example shows how to enable flow control:

```
B5(su)->set flowcontrol enable
```

# Setting Port Link Traps and Link Flap Detection

## Purpose

To disable or re-enable link traps, display link trap status, and to configure the link flapping detection function. By default, all ports are enabled to send SNMP trap messages indicating changes to their link status (up or down).

The link flap function detects when a link is going up and down rapidly (also called “link flapping”) on a physical port, and takes the required actions (disable port, and eventually send notification trap) to stop such a condition. If left unresolved, the “link flapping” condition can be detrimental to network stability because it can trigger Spanning Tree and routing table recalculation.

## Commands

For information about...	Refer to page...
show port trap	<a href="#">7-24</a>
set port trap	<a href="#">7-25</a>
show linkflap	<a href="#">7-25</a>
set linkflap globalstate	<a href="#">7-28</a>
set linkflap portstate	<a href="#">7-28</a>
set linkflap interval	<a href="#">7-29</a>
set linkflap action	<a href="#">7-29</a>
clear linkflap action	<a href="#">7-30</a>
set linkflap threshold	<a href="#">7-30</a>
set linkflap downtime	<a href="#">7-31</a>
clear linkflap down	<a href="#">7-31</a>
clear linkflap	<a href="#">7-32</a>
show newaddrtrap	<a href="#">7-33</a>
set newaddrtrap	<a href="#">7-33</a>

## show port trap

Use this command to display whether the port is enabled for generating an SNMP trap message if its link state changes.

### Syntax

```
show port trap [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays link trap status for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

## Defaults

If *port-string* is not specified, the trap status for all ports will be displayed.

## Mode

Switch command, read-write.

## Example

This example shows how to display link trap status for ge.3.1 through 4:

```
B5(su)->show port trap ge.3.1-4
Link traps enabled on port ge.3.1.
Link traps enabled on port ge.3.2.
Link traps enabled on port ge.3.3.
Link traps enabled on port ge.3.4.
```

# set port trap

Use this command to enable or disable ports for sending SNMP trap messages when their link status changes.

## Syntax

```
set port trap port-string {enable | disable}
```

## Parameters

<i>port-string</i>	Specifies the port(s) for which to enable or disable port traps. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>enable   disable</b>	Enables or disables sending trap messages when link status changes.

## Defaults

Sending traps when link status changes is enabled by default.

## Mode

Switch command, read-write.

## Example

The following example disables sending trap on ge.3.1.

```
B5(su)->set port trap ge.3.1 disable
```

# show linkflap

Use this command to display link flap detection state and configuration information.

## Syntax

```
show linkflap {globalstate | portstate | parameters | metrics | portsupported |
actsupported | maximum | downports | action | operstatus | threshold | interval}
| downtime | currentcount | totalcount | timelapsed | violations [port-string]
```

## Parameters

<b>globalstate</b>	Displays the global enable state of link flap detection.
<b>portstate</b>	Displays the port enable state of link flap detection.
<b>parameters</b>	Displays the current value of settable link flap detection parameters.
<b>metrics</b>	Displays linkflap detection metrics.
<b>portsupported</b>	Displays ports which can support the link flap detection function.
<b>actsupported</b>	Displays link flap detection actions supported by system hardware.
<b>maximum</b>	Displays the maximum allowed linkdowns per 10 seconds supported by system hardware.
<b>downports</b>	Displays ports disabled by link flap detection due to a violation.
<b>action</b>	Displays linkflap actions taken on violating port(s).
<b>operstatus</b>	Displays whether linkflap has deactivated port(s).
<b>threshold</b>	Displays the number of allowed link down transitions before action is taken.
<b>interval</b>	Displays the time period for counting link down transitions.
<b>downtime</b>	Displays how long violating port(s) are deactivated.
<b>currentcount</b>	Displays how many linkdown transitions are in the current interval.
<b>totalcount</b>	Displays how many linkdown transitions have occurred since the last reset.
<b>timelapsed</b>	Displays the time period since the last link down event or reset.
<b>violations</b>	Displays the number of link flap violations since the last reset.
<i>port-string</i>	(Optional) Displays information for specific port(s).

## Defaults

- If not specified, information about all link flap detection settings will be displayed.
- If *port-string* is not specified, information for all ports will be displayed.

## Mode

Switch mode, read-only.

## Usage

The linkflap default conditions are shown in the following table.

Linkflap Parameter	Default Condition
Linkflap global state	Disabled
Linkflap port state	Disabled
Linkflap action	None
Linkflap interval	5
Linkflap maximum allowed link downs per 10 seconds	20
Linkflap threshold (number of allowed link down transitions before action is taken)	10

## Examples

This example shows how to display the global status of the link trap detection function:

```
B5(rw)->show linkflap globalstate
Linkflap feature globally disabled
```

This example shows how to display ports disabled by link flap detection due to a violation:

```
B5(rw)->show linkflap downports
Ports currently held DOWN for Linkflap violations:
None.
```

This example shows how to display the link flap parameters table:

```
B5(rw)->show linkflap parameters
Linkflap Port Settable Parameter Table (X means error occurred)
Port      LF Status  Actions  Threshold  Interval  Downtime
-----  -
ge.1.1    disabled  .....  10         5         300
ge.1.2    enabled   D..S..T  3          5         300
ge.1.3    disabled  ...S..T  10         5         300
```

[Table 7-4](#) provides an explanation of the **show linkflap parameters** command output.

**Table 7-4 show linkflap parameters Output Details**

Output Field	What it displays...
Port	Port designation.
LF Status	Link flap enabled state.
Actions	Actions to be taken if the port violates allowed link flap behavior. D = disabled, S = Syslog entry will be generated, T= SNMP trap will be generated.
Threshold	Number of link down transitions necessary to trigger the link flap action.
Interval	Time interval (in seconds) for accumulating link down transitions.
Downtime	Interval (in seconds) port(s) will be held down after a link flap violation.

This example shows how to display the link flap metrics table:

```
B5(rw)->show linkflap metrics
Port      LinkStatus  CurrentCount  TotalCount  TimeElapsed  Violations
-----  -
ge.1.1    operational  0             0           241437       0
ge.1.2    disabled    4             15          147          5
ge.1.3    operational  3             3           241402       0
```

[Table 7-5](#) provides an explanation of the **show linkflap metrics** command output.

**Table 7-5 show linkflap metrics Output Details**

Output Field	What it displays...
Port	Port designation.
LinkStatus	Link status according to the link flap function.
CurrentCount	Link down count accruing toward the link flap threshold.
TotalCount	Number of link downs since system start,

**Table 7-5 show linkflap metrics Output Details (Continued)**

Output Field	What it displays...
TimeElapsed	Time (in seconds) since the last link down event.
Violations	Number of link flap violations on listed ports since system start.

## set linkflap globalstate

Use this command to globally enable or disable the link flap detection function.

### Syntax

```
set linkflap globalstate {disable | enable}
```

### Parameters

<b>disable   enable</b>	Globally disables or enables the link flap detection function.
-------------------------	--

### Defaults

By default, the function is disabled globally and on all ports.

### Mode

Switch mode, read-write.

### Usage

By default, the function is disabled globally and on all ports. If disabled globally after per-port settings have been configured using the linkflap commands, per-port settings will be retained.

### Example

This example shows how to globally enable the link trap detection function.

```
B5(rw)->set linkflap globalstate enable
```

## set linkflap portstate

Use this command to enable or disable link flap monitoring on one or more ports.

### Syntax

```
set linkflap portstate {disable | enable} [port-string]
```

### Parameters

<b>disable   enable</b>	Disables or enables the link flap detection function.
<i>port-string</i>	(Optional) Specifies the port or ports on which to disable or enable monitoring.

### Defaults

If *port-string* is not specified, all ports are enabled or disabled.



## Mode

Switch command, read-write.

## Example

This example shows how to enable the link trap monitoring on all ports.

```
B5(rw)->set linkflap portstate enable
```

# set linkflap interval

Use this command to set the time interval (in seconds) for accumulating link down transitions.

## Syntax

```
set linkflap interval port-string interval-value
```

## Parameters

<i>port-string</i>	Specifies the port(s) on which to set the link flap interval.
<i>interval-value</i>	Specifies an interval in seconds. A value of 0 will set the interval to forever.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to set the link flap interval on port ge.1.4 to 1000 seconds.

```
B5(rw)->set linkflap interval ge.1.4 1000
```

# set linkflap action

Use this command to set reactions to a link flap violation.

## Syntax

```
set linkflap action port-string {disableInterface | gensyslogentry | gentrap | all}
```

## Parameters

<i>port-string</i>	Specifies the port(s) on which to set the link flap action.
<b>disableInterface</b>	Sets the reaction as disabling the interface.
<b>gensyslogentry</b>	Sets the reaction as generating a syslog entry.
<b>gentrap</b>	Sets the reaction as generating an SNMP trap.
<b>all</b>	Sets the reaction as all of the above.

## Defaults

None.

## Mode

Switch mode, read-write.

## Example

This example shows how to set the link flap violation action on port ge.1.4 to generating a Syslog entry.

```
B5(rw)->set linkflap action ge.1.4 gensyslogentry
```

# clear linkflap action

Use this command to clear reactions to a link flap violation.

## Syntax

```
clear linkflap action port-string {disableInterface | gensyslogentry | gentrap | all}
```

## Parameters

<i>port-string</i>	Specifies the port(s) on which to clear the link flap action.
<b>disableInterface</b>	Clears the reaction as disabling the interface.
<b>gensyslogentry</b>	Clears the reaction as generating a syslog entry.
<b>gentrap</b>	Clears the reaction as generating an SNMP trap.
<b>all</b>	Clears the reaction as all of the above.

## Defaults

If *port-string* is not specified, actions will be cleared on all ports.

## Mode

Switch mode, read-write.

## Example

This example shows how to clear the link flap violation action on port ge.1.4 to generating a Syslog entry.

```
B5(rw)->clear linkflap action ge.1.4 gensyslogentry
```

# set linkflap threshold

Use this command to set the link flap action trigger count.

## Syntax

```
set linkflap threshold port-string threshold-value
```

## Parameters

<i>port-string</i>	Specifies the port(s) on which to set the link flap action trigger count.
<i>threshold-value</i>	Specifies the number of link down transitions necessary to trigger the link flap action. A minimum of 1 must be configured.

## Defaults

None.

## Mode

Switch mode, read-write.

## Example

This example shows how to set the link flap threshold on port ge.1.4 to 5.

```
B5(rw)->set linkflap threshold ge.1.4 5
```

# set linkflap downtime

Use this command to set the time interval (in seconds) one or more ports will be held down after a link flap violation.

## Syntax

```
set linkflap downtime port-string downtime-value
```

## Parameters

<i>port-string</i>	Specifies the port(s) on which to set the link flap downtime.
<i>downtime-value</i>	Specifies a downtime in seconds. A value of 0 will set the downtime to forever.

## Defaults

None.

## Mode

Switch mode, read-write.

## Example

This example shows how to set the link flap downtime on port ge.1.4 to 5000 seconds.

```
B5(rw)->set linkflap downtime ge.1.4 5000
```

# clear linkflap down

Use this command to toggle link flap disabled ports to operational.

## Syntax

```
clear linkflap down [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Specifies the ports to make operational.
--------------------	---

---

## Defaults

If *port-string* is not specified, all ports disabled by a link flap violation will be made operational.

## Mode

Switch mode, read-write.

## Example

This example shows how to make disabled port ge.1.4 operational.

```
B5(rw)->clear linkflap down ge.1.4
```

# clear linkflap

Use this command to clear all link flap options and / or statistics on one or more ports.

## Syntax

```
clear linkflap {all | stats [port-string] | parameter port-string {threshold | interval | downtime | all}}
```

## Parameters

---

<b>all   stats</b>	Clears all options and statistics, or clears only statistics.
<b>parameter</b>	Clears link flap parameters.
<b>threshold   interval   downtime   all</b>	Clears link flap threshold, interval, downtime or all parameters.
<i>port-string</i>	(Optional unless parameter is specified) Specifies the port(s) on which to clear settings.

---

## Defaults

If *port-string* is not specified, settings and/or statistics will be cleared on all ports.

## Mode

Switch mode, read-write.

## Example

This example shows how to clear all link flap options on port ge.1.4.

```
B5(rw)->clear linkflap all ge.1.4
```

## show newaddrtrap

Use this command to display the global and port-specific status of the new MAC addresses trap function.

### Syntax

```
show newaddrtrap [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays the status of the new MAC addresses trap function on specific ports.
--------------------	--

---

### Defaults

If *port-string* is not specified, the status of the new MAC addresses trap function will be displayed for all ports.

### Mode

Switch command, read-only.

### Usage

By default, this function is disabled globally and per port.

### Example

This example displays the New Address Trap state for ports 1 through 5 in unit/slot 1.

```
B5(ro)->show newaddrtrap ge.1.1-5
New Address Traps Globally disabled
```

```
Port      Enable State
-----
ge.1.1    disabled
ge.1.2    disabled
ge.1.3    disabled
ge.1.4    disabled
ge.1.5    disabled
```

## set newaddrtrap

Use this command to enable or disable trap messaging, globally or on one or more ports, when new source MAC addresses are detected.

### Syntax

```
set newaddrtrap [port-string] {enable | disable}
```

## Parameters

<i>port-string</i>	(Optional) Enable or disable the new MAC addresses trap function on specific ports.
<b>enable</b>   <b>disable</b>	Enable or disable the new MAC addresses trap function. If entered without the <i>port-string</i> parameter, enables or disables the function globally. When entered with the <i>port-string</i> parameter, enables or disables the function on specific ports.

## Defaults

If *port-string* is not specified, the trap function is set globally.

## Mode

Switch mode, read-write.

## Usage

This command enables and disables sending SNMP trap messages when a new source MAC address is detected by a port. If the port is a CDP port, however, traps for new source MAC addresses will not be sent.

The default mode is disabled globally and per port.

## Example

This example enables the trap function globally and then on ports 1 through 5 in unit/slot 1.

```
B5(rw)->set newaddrtrap enable
B5(rw)->set newaddrtrap ge.1.1-5 enable
```

# Configuring Broadcast Suppression

## Purpose

To review and set the broadcast suppression threshold for one or more ports. This feature limits the number of received broadcast frames the switch will accept per port. Broadcast suppression thresholds apply only to broadcast traffic—multicast traffic is not affected. By default, a broadcast suppression threshold of 14881 packets per second (pps) will be used, regardless of actual port speed. Broadcast suppression protects against broadcast storms and ARP sweeps.

## Commands

For information about...	Refer to page...
show port broadcast	<a href="#">7-35</a>
set port broadcast	<a href="#">7-36</a>
clear port broadcast	<a href="#">7-36</a>

## show port broadcast

Use this command to display port broadcast suppression thresholds.

### Syntax

```
show port broadcast [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Select the ports for which to show broadcast suppression thresholds. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

### Defaults

If *port-string* is not specified, broadcast status of all ports will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display the broadcast suppression thresholds for ports 1 through 4:

```
B5(su)->show port broadcast ge.1.1-4
Port          Total BC      Threshold
              Packets      (pkts/s)
-----
ge.1.1        0             50
ge.1.2        0             50
ge.1.3        0             40
ge.1.4        0            14881
```

## set port broadcast

Use this command to set the broadcast suppression threshold, in packets per second, on one or more ports. This sets a threshold on the broadcast traffic that is received and switched out to other ports.

### Syntax

```
set port broadcast port-string threshold-val
```

### Parameters

<i>port-string</i>	Select the ports for which to configure broadcast suppression thresholds. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<i>threshold-val</i>	Sets the packets per second threshold on broadcast traffic. Maximum value is <ul style="list-style-type: none"> <li>• 148810 for Fast Ethernet ports</li> <li>• 1488100 for 1-Gigabit ports.</li> <li>• 14881000 for 10-Gigabit ports</li> </ul>

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

Per port broadcast suppression is hardset to be globally enabled on the B5. If you would like to disable broadcast suppression, you can get the same result by setting the threshold limit for each port to the maximum number of packets which can be received per second as listed in the parameters section, above. The default broadcast suppression threshold for all ports is set to 14881.

### Example

This example configures ports 1 through 5 with a broadcast limit of 50 pps:

```
B5(su)->set port broadcast ge.1.1-5 50
```

## clear port broadcast

Use this command to clear the broadcast threshold limit to the default value of 14881 for the selected port.

### Syntax

```
clear port broadcast port-string threshold
```

### Parameters

<i>port-string</i>	Select the ports for which to clear broadcast suppression thresholds. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--



**Defaults**

None.

**Mode**

Switch command, read-write.

**Example**

This example clears the broadcast threshold limit to 14881 pps for ports 1 through 5:

```
B5(su)->clear port broadcast ge.1.1-5 threshold
```

## Port Mirroring



**Caution:** Port mirroring configuration should be performed only by personnel who are knowledgeable about the effects of port mirroring and its impact on network operation.

The Enterasys B5 device allows you to mirror (or redirect) the traffic being switched on a port for the purposes of network traffic analysis and connection assurance. When port mirroring is enabled, one port becomes a monitor port for another port within the device (the stack, if applicable).



**Note:** An Enterasys Networks Feature Guide document containing an in-depth discussion of port mirroring configuration is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads//>

## Mirroring Features

The Enterasys B5 device supports the following mirroring features:

- Mirroring can be configured in a many-to-one configuration so that one target (destination) port can monitor traffic on up to 8 source ports. Only one mirror destination port can be configured per stack, if applicable.
- Both transmit and receive traffic will be mirrored.
- A destination port will only act as a mirroring port when the session is operationally active.
- When a port mirror is created, the mirror destination port is removed from the egress list of VLAN 1 after a reboot.
- MAC addresses will be learned for packets tagged with the mirror VLAN ID. This will prevent the ability to snoop traffic across multiple hops.



**Caution:** Traffic mirrored to a VLAN may contain control traffic. This may be interpreted by the downstream neighbor as legal control frames. It is recommended that you disable any protocols (such as Spanning Tree) on inter-switch connections that might be affected .

## Remote Port Mirroring

Remote port mirroring is an extension to port mirroring which facilitates simultaneous mirroring of multiple source ports on multiple switches across a network to one or more remote destination ports.

Remote port mirroring involves configuration of the following port mirroring related parameters:

1. Configuration of normal port mirroring source ports and one destination port on all switches, as described above.
2. Configuration of a mirror VLAN, which is a unique VLAN on which mirrored packets traverse across the network. The mirror VLAN has to be configured on ALL switches across the network along which mirrored traffic traverses, from the switch where the source ports reside to the switch where the mirrored packets are sniffed and/or captured.

You must ensure that switches involved are properly configured to facilitate correct remote port mirroring operation. The following points in particular need to be observed:

- On the source switch, the correct destination port must be chosen to ensure that there is an egress path from that port to the desired remote destination(s).

- All ports on the path from the source port to the remote destination must be members of the mirror VLAN.
- On switches on the path from the source port to the remote destination, egress tagging has to be enabled on potential egress ports for the mirror VLAN.

With the introduction of remote port mirroring:

- Configured mirror destination ports will NOT lose their switching or routing properties as they do on A2, B2, or C2 products.
- On switches where the mirror VLAN has been configured, any traffic on that VLAN will be flooded on the VLAN. It will never be unicast, even if the source address of the traffic as been learned on the switch.

## Configuring SMON MIB Port Mirroring

### Overview

SMON port mirroring support allows you to redirect traffic on ports remotely using SMON MIBs. This is useful for troubleshooting or problem solving when network management through the console port, telnet, or SSH is not feasible.

### Procedures

Perform the following steps to configure and monitor port mirroring using SMON MIB objects.

To create and enable a port mirroring instance:

1. Open a MIB browser, such as Netsight MIB Tools
2. In the MIB directory tree, navigate to the **portCopyEntry** folder and expand it.
3. Select the **portCopyStatus** MIB.
4. Enter a desired source and target port in the **Instance** field using the format *source.target*.

For example, 3.2 would create a relationship where source port ge.1.3 would be mirrored to target port ge.1.2.



**Note:** In order to configure a port mirroring relationship, both source and destination interfaces must be enabled and operational (up).

5. Enter MIB option **4** (createAndGo) and perform an SNMP **Set** operation.
6. (Optional) Use the CLI to verify the port mirroring instance has been created and enabled as shown in the following example:

```
B5(su)->show port mirroring
Port Mirroring
=====
Source Port      = ge.1.3
Target Port      = ge.1.2
Frames Mirrored = Rx and Tx
Port Mirroring status enabled
```

To create a port mirroring instance without automatically enabling it:

1. Complete steps 1-4 above.
2. Enter MIB option **5** (createAndWait) and perform an SNMP **Set** operation.

- (Optional) Use the CLI to verify the port mirroring instance has been created set to disabled mode as shown in the following example:

```
B5(su)->show port mirroring
Port Mirroring
=====
Source Port      = ge.1.3
Target Port      = ge.1.2
Frames Mirrored  = Rx and Tx
Port Mirroring status disabled
```

- When you are ready to enable this instance, enter MIB option **1** (active) and perform an SNMP **Set** operation.
- (Optional) Use the CLI to verify the port mirroring instance has been enabled.

To delete a port mirroring instance:

- Select a previously created port mirroring instance in your MIB browser.
- Enter MIB option **6** (destroy) and perform an SNMP **Set** operation.
- (Optional) Use the CLI to verify the port mirroring instance has been deleted as shown in the following example:

```
B5(su)->show port mirroring
No Port Mirrors configured.
```

## Purpose

To review and configure port mirroring on the device.

## Commands

For information about...	Refer to page...
show port mirroring	<a href="#">7-40</a>
set port mirroring	<a href="#">7-41</a>
clear port mirroring	<a href="#">7-42</a>
set mirror vlan	<a href="#">7-42</a>
clear mirror vlan	<a href="#">7-43</a>

## show port mirroring

Use this command to display the source and target ports for mirroring, and whether mirroring is currently enabled or disabled for those ports.

### Syntax

```
show port mirroring
```

### Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to display port mirroring information. In this case, ge.1.4 is configured as a source port and ge.1.11 is a target and mirroring has been enabled between these ports:

```
B5(su)->show port mirroring

Port Mirroring
=====
Source Port = ge.1.4
Target Port = ge.1.11
Frames Mirrored = Rx and Tx
Port Mirroring status enabled.
```

## set port mirroring

Use this command to create a new mirroring relationship or to enable or disable an existing mirroring relationship between two ports.



**Notes:** When a port mirror is created, the mirror destination port is removed from VLAN 1's egress list after a reboot.

"MAC addresses will be learned for packets tagged with the mirror VLAN ID. This will prevent the ability to snoop traffic across multiple hops.

## Syntax

```
set port mirroring {create | disable | enable} source destination}
```

## Parameters

<b>create   disable   enable</b>	Creates, disables or enables mirroring settings on the specified ports. By default, port mirrors are enabled automatically when created.
<i>source</i>	Specifies the source port designation. This is the port on which the traffic will be monitored. Up to 8 source ports can be specified. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">"Port String Syntax Used in the CLI"</a> on page 7-1.
<i>destination</i>	Specifies the target port designation. This is the port that will duplicate or "mirror" all the traffic on the monitored port. Only one destination port can be configured per stack, if applicable.  For a detailed description of possible <i>port-string</i> values, refer to <a href="#">"Port String Syntax Used in the CLI"</a> on page 7-1.

## Defaults

Port mirrors are automatically enabled when created on this platform.

## Mode

Switch command, read-write.

## Usage

Note that LAG ports and their underlying physical ports, as described in “[Link Aggregation Control Protocol \(LACP\)](#)” on page 7-44, cannot be mirrored.

## Example

This example shows how to create and enable port mirroring with ge.1.4 as the source port, and ge.1.11 as the target port:

```
B5(su)->set port mirroring create ge.1.4 ge.1.11
```

# clear port mirroring

Use this command to clear a port mirroring relationship.

## Syntax

```
clear port mirroring source destination
```

## Parameters

---

<i>source</i>	Specifies the source ports (up to 8 ports) of the mirroring configuration to be cleared. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
<i>destination</i>	Specifies the target port of the mirroring configuration to be cleared.

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear a port mirroring relationship between source port ge.1.4 and target port ge.1.11:

```
B5(su)->clear port mirroring ge.1.4 ge.1.11
```

# set mirror vlan

Assigns a VLAN to be reserved for mirroring tr. If a mirrored VLAN is created, all mirrored traffic will egress VLAN tagged. All traffic on the mirror VLAN will be flooded.

## Syntax

```
set mirror vlan vlan-id
```

## Parameters

---

<i>vlan-id</i>	Specifies the VLAN to be used for remote port mirroring. The ID can range from 2 to 4093.
----------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

Refer to “[Remote Port Mirroring](#)” on page 7-38 for information about configuring mirror VLANs.

Use the **show port mirroring** command to display the VLANs configured for remote port mirroring.

## Example

The following example assigns a VLAN for mirroring traffic and then shows the configured port mirroring with the **show port mirror** command.

```
B5(su)->set mirror vlan 2

B5(su)->show port mirroring
Port Mirroring
=====
Source Port      = ge.1.1
Target Port      = ge.1.10
Frames Mirrored = Rx and Tx
Port Mirroring status enabled

Mirror Vlan      = 2
```

## clear mirror vlan

Use this command to clear the VLAN to be reserved for mirroring traffic.

### Syntax

```
clear mirror vlan vlan-id
```

### Parameters

---

<i>vlan-id</i>	Specifies the VLAN to be cleared. The ID can range from 2 to 4093.
----------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

The following example clears VLAN 2 from being used for remote port mirroring.

```
B5(su)->clear mirror vlan 2
```

# Link Aggregation Control Protocol (LACP)



**Caution:** Link aggregation configuration should only be performed by personnel who are knowledgeable about Spanning Tree and Link Aggregation, and fully understand the ramifications of modifications beyond device defaults. Otherwise, the proper operation of the network could be at risk.

Using multiple links simultaneously to increase bandwidth is a desirable switch feature, which can be accomplished if both sides agree on a set of ports that are being used as a Link Aggregation Group (LAG). Once a LAG is formed from selected ports, problems with looping can be avoided since the Spanning Tree can treat this LAG as a single port.

The Link Aggregation Control Protocol (LACP) logically groups interfaces together to create a greater bandwidth uplink, or link aggregation, according to the IEEE 802.3ad standard. This standard allows the switch to determine which ports are in LAGs and configure them dynamically. Since the protocol is based on the IEEE 802.3ad specification, any switch from any vendor that supports this standard can aggregate links automatically.

802.3ad LACP aggregations can also be run to end-users (that is, a server) or to a router.

For more information about configuring LACP, see the “Configuring Link Aggregation” Feature Guide on the Enterasys web site: <https://extranet.enterasys.com/downloads/>



**Note:** Earlier (proprietary) implementations of port aggregation referred to groups of aggregated ports as “trunks”.

## LACP Operation

For each aggregatable port in the device, LACP:

- Maintains configuration information (reflecting the inherent properties of the individual links as well as those established by management) to control aggregation.
- Exchanges configuration information with other devices to allocate the link to a Link Aggregation Group (LAG).



**Note:** A given link is allocated to, at most, one Link Aggregation Group (LAG) at a time. The allocation mechanism attempts to maximize aggregation, subject to management controls.

- Attaches the port to the aggregator used by the LAG, and detaches the port from the aggregator when it is no longer used by the LAG.
- Uses information from the partner device’s link aggregation control entity to decide whether to aggregate ports.

The operation of LACP involves the following activities:

- Checking that candidate links can actually be aggregated.
- Controlling the addition of a link to a LAG, and the creation of the group if necessary.
- Monitoring the status of aggregated links to ensure that the aggregation is still valid.
- Removing a link from a LAG if its membership is no longer valid, and removing the group if it no longer has any member links.

In order to allow LACP to determine whether a set of links connect to the same device, and to determine whether those links are compatible from the point of view of aggregation, it is necessary to be able to establish:



- A globally unique identifier for each device that participates in link aggregation.
- A means of identifying the set of capabilities associated with each port and with each aggregator, as understood by a given device.
- A means of identifying a LAG and its associated aggregator.



**Note:** The path cost of a LAG port will be displayed as zero when it is not an active link.

## LACP Terminology

Table 7-6 defines key terminology used in LACP configuration.

**Table 7-6 LACP Terms and Definitions**

Term	Definition
Aggregator	Virtual port that controls link aggregation for underlying physical ports. Each Enterasys B5 module provides 6 aggregator ports, which are designated in the CLI as <b>lag.0.1</b> through <b>lag.0.6</b> .
LAG	Link Aggregation Group. Once underlying physical ports (for example, <b>ge.x.x</b> ) are associated with an aggregator port, the resulting aggregation will be represented as one LAG with a <b>lag.x.x</b> port designation.  Enterasys B5 LAGs can have up to 8 associated physical ports.
LACPDU	Link Aggregation Control Protocol Data Unit. The protocol exchanges aggregation state/mode information by way of a port's actor and partner operational states. LACPDU's sent by the first party (the actor) convey to the second party (the actor's protocol partner) what the actor knows, both about its own state and that of its partner.
Actor and Partner	An actor is the local device sending LACPDU's. Its protocol partner is the device on the other end of the link aggregation. Each maintains current status of the other via LACPDU's containing information about their ports' LACP status and operational state.
Admin Key	Value assigned to aggregator ports and physical ports that are candidates for joining a LAG. The LACP implementation on Enterasys B5 devices will use this value to form an oper key and will determine which underlying physical ports are capable of aggregating by comparing oper keys. Aggregator ports allow only underlying ports with oper keys matching theirs to join their LAG. On Enterasys B5 devices, the default admin key value is 32768.
System Priority	Value used to build a LAG ID, which determines aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator.  <b>Note:</b> Only one LACP system priority can be set on a Enterasys B5 device, using either the <b>set lacp asyspri</b> command ( <a href="#">page 7-49</a> ), or the <b>set port lacp</b> command ( <a href="#">page 7-54</a> ).

## Enterasys B5 Usage Considerations

By default, the global LACP state is globally enabled, disabled per port.

After enabling LACP on the desired ports, the default values will result in the maximum number of aggregations possible. If the switch is placed in a configuration with its peers not running the

protocol, no dynamic link aggregations will be formed and the switch will function normally (that is, will block redundant paths). For information about building static aggregations, refer to **set lacp static** (page 7-50).

Each Enterasys B5 module provides six virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.6**. Each LAG can have up to eight associated physical ports. Once underlying physical ports (for example, **fe.x.x**, or **ge.x.x**) are associated with an aggregator port, the resulting aggregation will be represented as one LAG with a **lag.0.x** port designation. LACP determines which underlying physical ports are capable of aggregating by comparing operational keys. Aggregator ports allow only underlying ports with keys matching theirs to join their LAG.

LACP uses a system priority value to build a LAG ID, which determines aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator.

There are a few cases in which ports will not aggregate:

- An underlying physical port is attached to another port on this same switch (loopback).
- There is no available aggregator for two or more ports with the same LAG ID. This can happen if there are simply no available aggregators, or if none of the aggregators have a matching admin key and system priority.
- 802.1x authentication is enabled using the **set eapol** command (page 16-18) and ports that would otherwise aggregate are not 802.1X authorized.

The LACP implementation on the Enterasys B5 device will allow up to eight physical ports into a LAG. The device with the lowest LAG ID determines which underlying physical ports are allowed into a LAG based on the ports' LAG port priority. Ports with the lowest LAG port priority values are allowed into the LAG and all other speed groupings go into a standby state.

Multi-port LAGs will continue to operate as long as there is at least one active port in the LAG. Therefore, there is no need to create backup single port LAGs or to specifically assign the LAG and all its physical ports to the egress list of the LAG's VLAN.

Typically, two or more ports are required to form a LAG. However, you can enable the creation of single port LAGs as described in "**set lacp singleportlag**" on page 7-52. If a single port LAG goes down and the switch stays up, the switch will reconfigure the LAG to the same LAG number if the port comes back up.



**Note:** To aggregate, underlying physical ports must be running in full duplex mode and must be of the same operating speed.

## Commands

For information about...	Refer to page...
show lacp	7-47
set lacp	7-48
set lacp asyspri	7-49
set lacp aadminkey	7-49
clear lacp	7-50
set lacp static	7-50
clear lacp static	7-51

For information about...	Refer to page...
set lacp singleportlag	<a href="#">7-52</a>
clear lacp singleportlag	<a href="#">7-51</a>
show port lacp	<a href="#">7-53</a>
set port lacp	<a href="#">7-54</a>
clear port lacp	<a href="#">7-56</a>

## show lacp

Use this command to display information about one or more aggregator ports.

### Syntax

```
show lacp [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays LACP information for specific LAG port(s). Valid port designations are lag.0.1 - 6.
--------------------	---

### Defaults

If *port-string* is not specified, link aggregation information for all LAGs will be displayed.

### Mode

Switch command, read-only.

### Usage

Each Enterasys B5 module provides 6 virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.6**. Once underlying physical ports (that is, **ge.x.x**) are associated with an aggregator port, the resulting aggregation will be represented as one Link Aggregation Group (LAG) with a **lag.x.x** port designation.

### Example

This example shows how to display lacp information for lag.0.1. The following table describes the output fields.

```
B5(su)->show lacp lag.0.1
Global Link Aggregation state: enabled
Single Port LAGs:                disabled

Aggregator: lag.0.1
      Actor                               Partner
System Identifier: 00:01:F4:5F:1E:20      00:11:88:11:74:F9
  System Priority:           32768          32768
    Admin Key:               32768
      Oper Key:               32768          0
  Attached Ports:  ge.1.1
                   ge.1.3
```

[Table 7-7](#) provides an explanation of the command output.

**Table 7-7 show lacp Output Details**

Output Field	What It Displays...
Global Link Aggregation state	Shows if LACP is enabled or disabled on the switch.
Single Port LAGs	Displays if the single port LAG feature has been enabled on the switch. See “ <a href="#">set lacp singleportlag</a> ” on page 7-52 for more about single port LAG.
Aggregator	LAG port designation. Each Enterasys B5 module provides 6 virtual link aggregator ports, which are designated in the CLI as <b>lag.0.1</b> through <b>lag.0.6</b> . Once underlying physical ports (for example, <b>fe.x.x</b> ) are associated with an aggregator port, the resulting Link Aggregation Group (LAG) is represented with a <b>lag.x.x</b> port designation.
Actor	Local device participating in LACP negotiation.
Partner	Remote device participating in LACP negotiation.
System Identifier	MAC addresses for actor and partner.
System Priority	System priority value which determines aggregation precedence. Only one LACP system priority can be set on a Enterasys B5 device, using either the <b>set lacp asyspri</b> command ( <a href="#">page 7-49</a> ), or the <b>set port lacp</b> command ( <a href="#">page 7-54</a> ).
Admin Key	Port’s assigned key. Enterasys B5 devices provide a default admin key value of 32768 for all LAG ports (lag.0.1 though lag.0.6).
Oper Key	Port’s operational key, derived from the admin key. Only underlying physical ports with oper keys matching the aggregator’s will be allowed to aggregate.
Attached Ports	Underlying physical ports associated with this aggregator.

## set lacp

Use this command to disable or enable the Link Aggregation Control Protocol (LACP) on the device.

### Syntax

```
set lacp {disable | enable}
```

### Parameters

<b>disable   enable</b>	Disables or enables LACP.
-------------------------	---------------------------

### Defaults

By default, the global LACP state is enabled, disabled per port.

### Mode

Switch command, read-write.

### Example

This example shows how to disable LACP:

```
B5(su)->set lacp disable
```

## set lacp asyspri

Use this command to set the LACP system priority.

### Syntax

```
set lacp asyspri value
```

### Parameters

<b>asyspri</b>	Sets the system priority to be used in creating a LAG (Link Aggregation Group) ID. Valid values are <b>0</b> to <b>65535</b> .
<i>value</i>	Specifies a system priority value. Valid values are <b>0</b> to <b>65535</b> , with precedence given to lower values.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

LACP uses this value to determine aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator.

### Example

This example shows how to set the LACP system priority to 1000:

```
B5(su)->set lacp asyspri 1000
```

## set lacp aadminkey

Use this command to set the administratively assigned key for one or more aggregator ports.

### Syntax

```
set lacp aadminkey port-string value
```

### Parameters

<i>port-string</i>	Specifies the LAG port(s) on which to assign an admin key.
<i>value</i>	Specifies an admin key value to set. Valid values are <b>0</b> to <b>65535</b> . The default admin key value is 32768.

### Defaults

None.

### Mode

Switch command, read-write.

## Usage

LACP will use this value to form an oper key. Only underlying physical ports with oper keys matching those of their aggregators will be allowed to aggregate. The default admin key value for all LAG ports is 32768.

## Example

This example shows how to set the LACP admin key to 2000 for LAG port 6:

```
B5(su)->set lacp aadminkey lag.0.6 2000
```

## clear lacp

Use this command to clear LACP system priority or admin key settings.

### Syntax

```
clear lacp {[asyspri] [aadminkey port-string]}
```

### Parameters

---

<b>asyspri</b>	Clears system priority.
<b>aadminkey</b> <i>port-string</i>	Resets admin keys for one or more ports to the default value of 32768.

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the actor admin key for LAG port 6:

```
B5(su)->clear lacp aadminkey lag.0.6
```

## set lacp static

Use this command to disable or enable static link aggregation, or to assign one or more underlying physical ports to a Link Aggregation Group (LAG).

### Syntax

```
set lacp static {disable | enable} | lagportstring [key] port-string
```

### Parameters

---

<b>disable   enable</b>	Disables or enables static link aggregation.
<i>lagportstring</i>	Specifies the LAG aggregator port to which new ports will be assigned.

---

<i>key</i>	(Optional) Specifies the new member port and LAG port aggregator admin key value. Only ports with matching keys are allowed to aggregate. Valid values are 0 - 65535.  <b>Note:</b> This key value must be unique. If ports other than the desired underlying physical ports share the same admin key value, aggregation will fail or undesired aggregations will form.
<i>port-string</i>	Specifies the member port(s) to add to the LAG. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

## Defaults

If not specified, a *key* will be assigned according to the specified aggregator. For example a key of 4 would be assigned to lag.0.4.

## Mode

Switch command, read-write.

## Example

This example shows how to add port ge.1.6 to the LAG of aggregator port 6:

```
B5(su)->set lacp static lag.0.6 ge.1.6
```

# clear lacp static

Use this command to remove specific ports from a Link Aggregation Group.

## Syntax

```
clear lacp static lagportstring port-string
```

## Parameters

<i>lagportstring</i>	Specifies the LAG aggregator port from which ports will be removed.
<i>port-string</i>	Specifies the port(s) to remove from the LAG. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to remove ge.1.6 from the LAG of aggregator port 6:

```
B5(su)->clear lacp static lag.0.6 ge.1.6
```

## set lacp singleportlag

Use this command to enable or disable the formation of single port LAGs.

### Syntax

```
set lacp singleportlag {enable | disable}
```

### Parameters

---

<b>disable   enable</b>	Enables or disables the formation of single port LAGs.
-------------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

When single port LAGs are enabled, Link Aggregation Groups can be formed when only one port is receiving protocol transmissions from a partner. When this setting is disabled, two or more ports are required to form a LAG.

This setting has no effect on existing LAGs created with multiple member ports. It also does not prevent previously formed LAGs from coming up after they have gone down, as long as any previous LAG member ports come up connected to the same switch as before the LAG went down.

### Example

This example enables the formation of single port LAGs:

```
B5(su)->set lacp singleportlag enable
```

## clear lacp singleportlag

Use this command to reset the single port LAG function back to the default state of disabled.

### Syntax

```
clear lacp singleportlag
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.



## Example

This example shows how to reset the single port LAG function back to disabled:

```
B5(su)->clear lacp singleportlag
```

## show port lacp

Use this command to display link aggregation information for one or more underlying physical ports.

### Syntax

```
show port lacp port port-string {[status {detail | summary}] | [counters]}
```

### Parameters

<b>port</b> <i>port-string</i>	Displays LACP information for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
<b>status detail   summary</b>	Displays LACP status in detailed or summary information.
<b>counters</b>	Displays LACP counter information.

### Defaults

None.

### Mode

Switch command, read-only.

### Usage

State definitions, such as ActorAdminState and Partner AdminState, are indicated with letter abbreviations. If the **show port lacp** command displays one or more of the following letters, it means the state is true for the associated actor or partner ports:

- **E** = Expired
- **F** = Defaulted
- **D** = Distributing (tx enabled)
- **C** = Collecting (rx enabled)
- **S** = Synchronized (actor and partner agree)
- **G** = Aggregation allowed
- **S/l** = Short/Long LACP timeout
- **A/p** = Active/Passive LACP

For more information about these states, refer to **set port lacp** ([page 7-54](#)) and the IEEE 802.3 2002 specification.

### Examples

This example shows how to display detailed LACP status information for port ge.1.1

```
B5(su)-> show port lacp port ge.1.1 status detail
```

Global Link Aggregation state : Disabled

```

Port Instance:          ge.1.1 Port enable state:          Disabled
ActorPort:             1 PartnerAdminPort:              1
ActorSystemPriority:   32768 PartnerOperPort:            1
ActorPortPriority:     32768 PartnerAdminSystemPriority:  32768
ActorAdminKey:         32768 PartnerOperSystemPriority:   32768
ActorOperKey:         32768 PartnerAdminPortPriority:     32768
ActorAdminState:      -----GLA PartnerOperPortPriority:  32768
ActorOperState:       -F---GLA PartnerAdminKey:           1
ActorSystemID: 00:1F:45:47:81:FC PartnerOperKey:         1
SelectedAggID:        None PartnerAdminState:            -----GSA
AttachedAggID:        None PartnerOperState:             -----SA
MuxState:             Detached PartnerAdminSystemID:      00:00:00:00:00:00
DebugRxState:        Portdisable PartnerOperSystemID:    00:00:00:00:00:00

```

This example shows how to display summarized LACP status information for port ge.1.12:

```

B5(su)->show port lacp port ge.1.12 status summary
Port   Aggr      Actor System      Partner System
      Pri:   System ID:  Key:      Pri: System ID:  Key:
ge.1.12  none [(32768,00e0639db587,32768),(32768,000000000000, 1411)]

```

This example shows how to display LACP counters for port ge.1.12:

```

B5(su)->show port lacp port ge.1.12 counters
Port Instance:          ge.1.12
LACPDUsRx:              11067
LACPDUsTx:              0
IllegalRx:              0
UnknownRx:              0
MarkerPDUsRx:           0
MarkerPDUsTx:           0
MarkerResponsePDUsRx:  0
MarkerResponsePDUsTx:  374

```

## set port lacp

Use this command to set link aggregation parameters for one or more ports. These settings will determine the specified underlying physical ports' ability to join a LAG, and their administrative state once aggregated.

### Syntax

```

set port lacp port port-string {[aadminkey aadminkey] [aadminstate {lacpactive |
lacptimeout | lacpagg | lacpsync | lacpcollect | lacpdist | lacpdef | lacpexpire}]
[aportpri aportpri] [asyspri asyspri] [enable | [disable] [padminkey padminkey]
[padminport padminport] [padminportpri padminportpri] [padminstate {lacpactive |
lacptimeout | lacpagg | lacpsync | lacpcollect | lacpdist | lacpdef | lacpexpire}]
[padminsysid padminsysid] [padminsyspri padminsyspri]

```

## Parameters

<b>port</b> <i>port-string</i>	Specifies the physical port(s) on which to configure LACP. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>aadminkey</b> <i>aadminkey</i>	Sets the port’s actor admin key. LACP will use this value to form an oper key and will determine which underlying physical ports are capable of aggregating by comparing oper keys. Aggregator ports allow only underlying ports with oper keys matching theirs to join their LAG. Valid values are <b>1 - 65535</b> . The default key value is 32768.
<b>aadminstate</b> <b>lacpactive</b>   <b>lacptimeout</b>   <b>lacpagg</b>   <b>lacpsync</b>   <b>lacpcollect</b>   <b>lacpdist</b>   <b>lacpdef</b>   <b>lacpexpire</b>	Sets the port’s actor LACP administrative state to allow for:  <b>lacpactive</b> - Transmitting LACP PDUs.  <b>lacptimeout</b> - Transmitting LACP PDUs every 1 sec. vs 30 sec. (default).  <b>lacpagg</b> - Aggregation on this port.  <b>lacpsync</b> - Transition to synchronization state.  <b>lacpcollect</b> - Transition to collection state.  <b>lacpdist</b> - Transition to distribution state.  <b>lacpdef</b> - Transition to defaulted state.  <b>lacpexpire</b> - Transition to expired state.
<b>aportpri</b> <i>aportpri</i>	Sets the port’s actor port priority. Valid values are <b>0 - 65535</b> , with lower values designating higher priority.
<b>asyspri</b> <i>asyspri</i>	Sets the port’s actor system priority. The LACP implementation on the Enterasys B5 device uses this value to determine aggregation precedence when there are two devices competing for the same aggregator. Valid values are <b>0 - 65535</b> , with higher precedence given to lower values.  <b>Note:</b> Only one LACP system priority can be set on a Enterasys B5 device, using either this command, or the <b>set lacp asyspri</b> command ( <a href="#">“set lacp asyspri”</a> on page 7-49).
<b>enable</b>	(Optional) Enables LACPDU processing on this port.
<b>disable</b>	(Optional) Disables LACPDU processing on this port. By default, LACP is disabled on ports.
<b>padminkey</b> <i>padminkey</i>	Sets a default value to use as the port’s partner admin key. Only ports with matching admin keys are allowed to aggregate. Valid values are <b>1 - 65535</b> .
<b>padminport</b> <i>padminport</i>	Sets a default value to use as the port’s partner admin value. Valid values are <b>1 - 65535</b> .
<b>padminportpri</b> <i>padminportpri</i>	Sets a default value to use as the port’s partner port priority. Valid values are <b>0 - 65535</b> , with lower values given higher priority.
<b>padminstate</b> <b>lacpactive</b>   <b>lacptimeout</b>   <b>lacpagg</b>   <b>lacpsync</b>   <b>lacpcollect</b>   <b>lacpdist</b>   <b>lacpdef</b>   <b>lacpexpire</b>	Sets a port’s partner LACP administrative state. See <b>aadminstate</b> for valid options.

<b>padminsysid</b> <i>padminsysid</i>	Sets a default value to use as the port's partner system ID. This is a MAC address.
<b>padminsyspri</b> <i>padminsyspri</i>	Sets a default value to use as the port's partner priority. Valid values are 0 - 65535, with lower values given higher priority.

## Defaults

At least one parameter must be entered per *port-string*.

If **enable** or **disable** are not specified, port(s) will be enabled with the LACP parameters entered.

## Mode

Switch command, read-write.

## Usage

LACP commands and parameters beginning with an "a" (such as **aadminkey**) set actor values. Corresponding commands and parameters beginning with a "p" (such as **padminkey**) set corresponding partner values. Actor refers to the local device participating in LACP negotiation, while partner refers to its remote device partner at the other end of the negotiation. Actors and partners maintain current status of the other via LACPDUs containing information about their ports' LACP status and operational state.

## Example

This example shows how to set the actor admin key to 3555 for port `ge.3.16` and enable LACP on the port:

```
B5(su)->set port lacp port ge.3.16 aadminkey 3555 enable
```

# clear port lacp

Use this command to clear link aggregation settings for one or more ports.

## Syntax

```
clear port lacp port port-string {[aadminkey] [aportpri] [asyspri] [aadminstate
{lacpactive | lacptimeout | lacpagg | lacpsync | lacpcollect | lacpdist | lacpdef
| lacpexpire | all}] [padminsyspri] [padminsysid] [padminkey] [padminportpri]
[padminport] [padminstate {lacpactive | lacptimeout | lacpagg | lacpsync |
lacpcollect | lacpdist | lacpdef | lacpexpire | all}]}
```

## Parameters

<b>port</b> <i>port-string</i>	Specifies the physical port(s) on which LACP settings will be cleared. For a detailed description of possible <i>port-string</i> values, refer to " <a href="#">Port String Syntax Used in the CLI</a> " on page 7-1.
<b>aadminkey</b>	Clears a port's actor admin key.
<b>aportpri</b>	Clears a port's actor port priority.
<b>asyspri</b>	Clears the port's actor system priority.

<b>aadminstate</b> <b>lacpactive</b>   <b>lacptimeout</b>   <b>lacpagg</b>   <b>lacpsync</b>   <b>lacpcollect</b>   <b>lacpdist</b>   <b>lacpdef</b>   <b>lacpexpire</b>   <b>all</b>	Clears a port's specific actor admin state, or all actor admin state(s). For descriptions of specific states, refer to the <b>set port lacp</b> command (" <a href="#">set port lacp</a> " on page 7-54).
<b>padminsyspri</b>	Clears the port's default partner priority value.
<b>padminsysid</b>	Clears the port's default partner system ID.
<b>padminkey</b>	Clears the port's default partner admin key.
<b>padminportpri</b>	Clears the port's default partner port priority.
<b>padminport</b>	Deletes a partner port from the LACP configuration.
<b>padminstate</b> <b>lacpactive</b>   <b>lacptimeout</b>   <b>lacpagg</b>   <b>lacpsync</b>   <b>lacpcollect</b>   <b>lacpdist</b>   <b>lacpdef</b>   <b>lacpexpire</b>   <b>all</b>	Clears the port's specific partner admin state, or all partner admin state(s).

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

If you set a port to LACP passive using the command **clear port lacp port** *<port-string>* **aadminstate lacpactive**, the command **clear port lacp port** *<port-string>* **aadminstate lacptimeout** will also be added to the configuration. If you unset the first command, it will remove the second command automatically from the configuration file.

## Example

This example shows how to clear all link aggregation parameters for port `ge.3.16`:

```
B5(su)->clear port lacp port ge.3.16
```

## Configuring Protected Ports

The Protected Port feature is used to prevent ports from forwarding traffic to each other, even when they are on the same VLAN. Ports may be designated as either protected or unprotected. Ports are unprotected by default. Multiple groups of protected ports are supported.

### Protected Port Operation

Ports that are configured to be protected cannot forward traffic to other protected ports in the same group, regardless of having the same VLAN membership. However, protected ports can forward traffic to ports which are unprotected (not listed in any group). Protected ports can also forward traffic to protected ports in a different group, if they are in the same VLAN. Unprotected ports can forward traffic to both protected and unprotected ports. A port may belong to only one group of protected ports.

This feature only applies to ports within a switch or a stack. It does not apply across multiple switches in a network.

### Commands

For information about...	Refer to page...
set port protected	<a href="#">7-58</a>
show port protected	<a href="#">7-59</a>
clear port protected	<a href="#">7-59</a>
set port protected name	<a href="#">7-60</a>
show port protected name	<a href="#">7-60</a>
clear port protected name	<a href="#">7-61</a>

## set port protected

Use this command to specify a port to be protected and assign the port to a group of protected ports. A port can be assigned to only one group.

### Syntax

```
set port protected port-string group-id
```

### Parameters

<i>port-string</i>	Specifies the port or ports to be protected.
<i>group-id</i>	Specifies the id of the group to which the ports should be assigned. Id can range from 0 to 2.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to assign ports ge.1.1 through ge.1.3 to protected port group 1:

```
B5(rw)->set port protected ge.1.1-3 1
```

## show port protected

Use this command to display information about the ports configured for protected mode.

### Syntax

```
show port protected [port-string] | [group-id]
```

### Parameters

<i>port-string</i>	(Optional) Specifies the port or ports for which to display information.
<i>group-id</i>	(Optional) Specifies the id of the group for which to display information. Id can range from 0 to 2.

### Defaults

If no parameters are entered, information about all protected ports is displayed.

### Mode

Read-only.

### Example

This example shows how to display information about all protected ports:

```
B5(ro)->show port protected
Group id      Port      GroupName
-----
1             ge.1.1    group1
1             ge.1.2    group1
1             ge.1.3    group1
```

## clear port protected

Use this command to remove a port or group from protected mode.

### Syntax

```
clear port protected [port-string] | [group-id]
```

### Parameters

<i>port-string</i>	(Optional) Specifies the port or ports to remove from protected mode.
<i>group-id</i>	(Optional) Specifies the id of the group to remove from protected mode. Id can range from 0 to 2.

### Defaults

If no parameters are entered, all protected ports and groups are cleared.

## Mode

Switch command, read-write.

## Example

This example shows how to clear protected ports ge.1.1 through ge.1.3:

```
B5(rw)->clear port protected ge.1.1-3
```

# set port protected name

Use this command to assign a name to a protected port group id.

## Syntax

```
set port protected name group-id name
```

## Parameters

<i>group-id</i>	Specifies the id of this group. Id can range from 0 to 2.
<i>name</i>	Specifies a name for the group. The name can be up to 32 characters in length.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to assign the name "group1" to protected port group 1:

```
B5(rw)->set port protected name 1 group1
```

# show port protected name

Use this command to display the name for the group ids specified.

## Syntax

```
show port protected name group-id
```

## Parameters

<i>group-id</i>	Specifies the id of the group to display. Id can range from 0 to 2.
-----------------	---

## Defaults

None.

## Mode

Read-only.



## Example

This example shows how to show the name of protected port group 1:

```
B5(ro)->show port protected name 1
Group ID      Group Name
-----
1              group1
```

## clear port protected name

Use this command to clear the name of a protected group.

### Syntax

```
clear port protected name group-id
```

### Parameters

<i>group-id</i>	Specifies the id of the group for which to clear the name. Id can range from 0 to 2.
-----------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the name of protected port group 1:

```
B5(rw)->clear port protected name 1
```



## SNMP Configuration

This chapter describes the Simple Network Management Protocol (SNMP) set of commands and how to use them.

For information about...	Refer to page...
<a href="#">SNMP Configuration Summary</a>	8-1
<a href="#">Reviewing SNMP Statistics</a>	8-3
<a href="#">Configuring SNMP Users, Groups, and Communities</a>	8-8
<a href="#">Configuring SNMP Access Rights</a>	8-15
<a href="#">Configuring SNMP MIB Views</a>	8-19
<a href="#">Configuring SNMP Target Parameters</a>	8-23
<a href="#">Configuring SNMP Target Addresses</a>	8-26
<a href="#">Configuring SNMP Notification Parameters</a>	8-29
<a href="#">Creating a Basic SNMP Trap Configuration</a>	8-36
<a href="#">Configuring the SNMP Management Interface</a>	8-38



**Note:** An Enterasys Networks Feature Guide document containing an in-depth discussion of SNMP configuration is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads/>

### SNMP Configuration Summary

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Enterasys B5 devices support three versions of SNMP:

- Version 1 (SNMPv1) — This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c) — The second release of SNMP, described in RFC 1907, has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3) — This is the most recent version of SNMP, and includes significant enhancements to administration and security. SNMPv3 is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575.

## SNMPv1 and SNMPv2c

The components of SNMPv1 and SNMPv2c network management fall into three categories:

- Managed devices (such as a switch).
- SNMP agents and MIBs, including SNMP traps, community strings, and Remote Monitoring (RMON) MIBs, which run on managed devices.
- SNMP network management applications, such as the Enterasys NetSight application, which communicate with agents to get statistics and alerts from the managed devices.

## SNMPv3

SNMPv3 is an interoperable standards-based protocol that provides secure access to devices by authenticating and encrypting frames over the network. The advanced security features provided in SNMPv3 are as follows:

- Message integrity — Collects data securely without being tampered with or corrupted.
- Authentication — Determines the message is from a valid source.
- Encryption — Scrambles the contents of a frame to prevent it from being seen by an unauthorized source.

Unlike SNMPv1 and SNMPv2c, in SNMPv3, the concept of SNMP agents and SNMP managers no longer apply. These concepts have been combined into an SNMP entity. An SNMP entity consists of an SNMP engine and SNMP applications. An SNMP engine consists of the following four components:

- Dispatcher — This component sends and receives messages.
- Message processing subsystem — This component accepts outgoing PDUs from the dispatcher and prepares them for transmission by wrapping them in a message header and returning them to the dispatcher. The message processing subsystem also accepts incoming messages from the dispatcher, processes each message header, and returns the enclosed PDU to the dispatcher.
- Security subsystem — This component authenticates and encrypts messages.
- Access control subsystem — This component determines which users and which operations are allowed access to managed objects.

## About SNMP Security Models and Levels

An SNMP security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. The three levels of SNMP security are: No authentication required (NoAuthNoPriv); authentication required (AuthNoPriv); and privacy (authPriv). A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP frame. [Table 8-1](#) identifies the levels of SNMP security available on Enterasys B5 devices and authentication required within each model.

**Table 8-1 SNMP Security Levels**

Model	Security Level	Authentication	Encryption	How It Works
v1	NoAuthNoPriv	Community string	None	Uses a community string match for authentication.
v2c	NoAuthNoPriv	Community string	None	Uses a community string match for authentication.
v3	NoAuthNoPriv	User name	None	Uses a user name match for authentication.
	AuthNoPriv	MD5 or SHA	None	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

## Using SNMP Contexts to Access Specific MIBs

By default, when operating from the switch CLI, Enterasys B5 devices allow access to all SNMP MIBs or contexts. A context is a collection of MIB objects, often associated with a particular physical or logical device.

If no optional *context* parameters are configured for v1 and v2 “community” names and v3 “user” groups, these groups are able to access all SNMP MIB objects when in switch mode.

Specifying a *context* parameter when setting up SNMP user group would permit or restrict the group’s switch management access to the MIB(s) specified by the *context* (MIB object ID) value.

All SNMP contexts known to the device can be displayed using the **show snmp context** command as described in “[show snmp context](#)” on page 8-21.

### Example

This example permits the “powergroup” to manage all MIBs via SNMPv3:

```
B5(su)->set snmp access powergroup security-model usm
```

## Configuration Considerations

Commands for configuring SNMP on the Enterasys B5 device are independent during the SNMP setup process. For instance, target parameters can be specified when setting up optional notification filters — even though these parameters have not yet been created with the **set snmp targetparams** command.

## Reviewing SNMP Statistics

### Purpose

To review SNMP statistics.

## Commands

For information about...	Refer to page...
show snmp engineid	<a href="#">8-4</a>
show snmp counters	<a href="#">8-5</a>

## show snmp engineid

Use this command to display the SNMP local engine ID. This is the SNMP v3 engine's administratively unique identifier.

### Syntax

```
show snmp engineid
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display SNMP engine properties:

```
B5(su)->show snmp engineid
EngineId: 80:00:15:f8:03:00:e0:63:9d:b5:87
Engine Boots      = 12
Engine Time       = 162181
Max Msg Size     = 2048
```

[Table 8-2](#) provides an explanation of the command output.

**Table 8-2 show snmp engineid Output Details**

Output Field	What It Displays...
<b>EngineId</b>	String identifying the SNMP agent on the device.
<b>Engine Boots</b>	Number of times the SNMP engine has been started or reinitialized.
Engine Time	Time in seconds since last reboot.
Max Msg Size	Maximum accepted length, in bytes, of SNMP frame.

## show snmp counters

Use this command to display SNMP traffic counter values.

### Syntax

```
show snmp counters
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display SNMP counter values

```
B5(su)->show snmp counters

--- mib2 SNMP group counters:
snmpInPkts           = 396601
snmpOutPkts          = 396601
snmpInBadVersions    = 0
snmpInBadCommunityNames = 0
snmpInBadCommunityUses = 0
snmpInASNParseErrs  = 0
snmpInTooBigs        = 0
snmpInNoSuchNames    = 0
snmpInBadValues      = 0
snmpInReadOnlys      = 0
snmpInGenErrs        = 0
snmpInTotalReqVars   = 403661
snmpInTotalSetVars   = 534
snmpInGetRequests    = 290
snmpInGetNexts       = 396279
snmpInSetRequests    = 32
snmpInGetResponses   = 0
snmpInTraps          = 0
snmpOutTooBigs       = 0
snmpOutNoSuchNames   = 11
snmpOutBadValues     = 0
snmpOutGenErrs       = 0
snmpOutGetRequests   = 0
snmpOutGetNexts      = 0
snmpOutSetRequests   = 0
snmpOutGetResponses  = 396601
snmpOutTraps         = 0
snmpSilentDrops      = 0
snmpProxyDrops       = 0

--- USM Stats counters:
usmStatsUnsupportedSecLevels = 0
usmStatsNotInTimeWindows    = 0
usmStatsUnknownUserNames    = 0
```

```

usmStatsUnknownEngineIDs      = 0
usmStatsWrongDigests          = 0
usmStatsDecryptionErrors      = 0

```

Table 8-3 provides an explanation of the command output.

**Table 8-3 show snmp counters Output Details**

Output Field	What It Displays...
snmpInPkts	Number of messages delivered to the SNMP entity from the transport service.
snmpOutPkts	Number of SNMP messages passed from the SNMP protocol entity to the transport service.
snmpInBadVersions	Number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	Number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to the entity.
snmpInBadCommunityUses	Number of SNMP messages delivered to the SNMP entity that represented an SNMP operation not allowed by the SNMP community named in the message.
snmpInASNParseErrs	Number of ASN.1 (Abstract Syntax Notation) or BER (Basic Encoding Rules) errors encountered by the SNMP entity when decoding received SNMP messages.
snmpInTooBig	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as "tooBig."
snmpInNoSuchNames	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as "noSuchName."
snmpInBadValues	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as "badValue."
snmpInReadOnly	Number of valid SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as "readOnly."
snmpInGenErrs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as "genErr."
snmpInTotalReqVars	Number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpInTotalSetVars	Number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmpInGetRequests	Number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetNexts	Number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol entity.
snmpInSetRequests	Number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetResponses	Number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol entity.
snmpInTraps	Number of SNMP Trap PDUs accepted and processed by the SNMP protocol entity.
snmpOutTooBig	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as "tooBig."
snmpOutNoSuchNames	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status as "noSuchName."



**Table 8-3 show snmp counters Output Details (Continued)**

<b>Output Field</b>	<b>What It Displays...</b>
snmpOutBadValues	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as "badValue."
snmpOutGenErrs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as "genErr."
snmpOutGetRequests	Number of SNMP Get-Request PDUs generated by the SNMP protocol entity.
snmpOutGetNexts	Number of SNMP Get-Next PDUs generated by the SNMP protocol entity.
snmpOutSetRequests	Number of SNMP Set-Request PDUs generated by the SNMP protocol entity.
snmpOutGetResponses	Number of SNMP Get-Response PDUs generated by the SNMP protocol entity.
snmpOutTraps	Number of SNMP Trap PDUs generated by the SNMP protocol entity.
snmpSilentDrops	Number of SNMP Get, Set, or Inform request error messages that were dropped because the reply was larger than the requestor's maximum message size.
snmpProxyDrops	Number of SNMP Get, Set, or Inform request error messages that were dropped because the reply was larger than the proxy target's maximum message size.
usmStatsUnsupportedSec Levels	Number of packets received by the SNMP engine that were dropped because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
usmStatsNotInTimeWindows	Number of packets received by the SNMP engine that were dropped because they appeared outside of the authoritative SNMP engine's window.
usmStatsUnknownUserNames	Number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine.
usmStatsUnknownEngineIDs	Number of packets received by the SNMP engine that were dropped because they referenced an snmpEngineID that was not known to the SNMP engine.
usmStatsWrongDigests	Number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value.
usmStatsDecryptionErrors	Number of packets received by the SNMP engine that were dropped because they could not be decrypted.

# Configuring SNMP Users, Groups, and Communities

## Purpose

To review and configure SNMP users, groups, and v1 and v2 communities. These are defined as follows:

- User — A person registered in SNMPv3 to access SNMP management.
- Group — A collection of users who share the same SNMP access privileges.
- Community — A name used to authenticate SNMPv1 and v2 users.

## Commands

For information about...	Refer to page...
show snmp user	<a href="#">8-8</a>
set snmp user	<a href="#">8-9</a>
clear snmp user	<a href="#">8-11</a>
show snmp group	<a href="#">8-11</a>
set snmp group	<a href="#">8-12</a>
clear snmp group	<a href="#">8-13</a>
show snmp community	<a href="#">8-13</a>
set snmp community	<a href="#">8-14</a>
clear snmp community	<a href="#">8-15</a>

## show snmp user

Use this command to display information about SNMP users. These are people registered to access SNMP management.

### Syntax

```
show snmp user [list] | [user] | [remote remote] [volatile | nonvolatile | read-only]
```

### Parameters

<b>list</b>	(Optional) Displays a list of registered SNMP user names.
<b>user</b>	(Optional) Displays information about a specific user.
<b>remote remote</b>	(Optional) Displays information about users on a specific remote SNMP engine.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) Displays user information for a specified storage type.

### Defaults

If **list** is not specified, detailed SNMP information will be displayed.

If *user* is not specified, information about all SNMP users will be displayed.

If **remote** is not specified, user information about the local SNMP engine will be displayed.

If a storage type is not specified, user information for all storage types will be displayed.

## Mode

Switch command, read-only.

## Examples

This example shows how to display an SNMP user list:

```
B5(su)->show snmp user list
--- SNMP user information ---
--- List of registered users:
Guest
admin1
admin2
netops
```

This example shows how to display information for the SNMP “guest” user:

```
(su)->show snmp user guest
--- SNMP user information ---
EngineId: 00:00:00:63:00:00:00:a1:00:00:00:00
Username           = Guest
Auth protocol      = usmNoAuthProtocol
Privacy protocol   = usmNoPrivProtocol
Storage type       = nonVolatile
Row status         = active
```

[Table 8-4](#) provides an explanation of the command output.

**Table 8-4 show snmp user Output Details**

Output Field	What It Displays...
EngineId	SNMP local engine identifier.
Username	SNMPv1 or v2 community name or SNMPv3 user name.
Auth protocol	Type of authentication protocol applied to this user.
Privacy protocol	Type of encryption protocol applied to this user.
Storage type	Whether entry is stored in <b>volatile</b> , <b>nonvolatile</b> or <b>read-only</b> memory.
Row status	Status of this entry: <b>active</b> , <b>notInService</b> , or <b>notReady</b> .

## set snmp user

Use this command to create a new SNMPv3 user.

### Syntax

```
set snmp user user [remote remoteid] [encryption {des | aes}] [privacy
privpassword] [authentication {md5 | sha}] [authpassword] [volatile | nonvolatile]
```

## Parameters

<i>user</i>	Specifies a name for the SNMPv3 user.
<b>remote</b> <i>remoteid</i>	(Optional) Registers the user on a specific remote SNMP engine.
<b>encryption des</b>   <b>aes</b>	(Optional) Specifies the encryption type for this user. AES refers to the Advanced Encryption Standard using a 128 bit key size.
<b>privacy</b> <i>privopassword</i>	(Optional) Specifies an encryption password. Minimum of 8 characters. Required if encryption is specified.
<b>authentication md5</b>   <b>sha</b>	(Optional) Specifies the authentication type required for this user as MD5 or SHA.
<i>authpassword</i>	(Optional) Specifies a password for this user when authentication is required. Minimum of 8 characters.
<b>volatile</b>   <b>nonvolatile</b>	(Optional) Specifies a storage type for this user entry.

## Defaults

If **remote** is not specified, the user will be registered for the local SNMP engine.

If **encryption** is not specified, no encryption will be applied.

If **authentication** is not specified, no authentication will be applied.

If storage type is not specified, **nonvolatile** will be applied.

## Mode

Switch command, read-write.

## Usage

Although all the parameters except for the user name are optional, if you are entering any of the optional parameters, it is recommended that you enter them in the order shown in the syntax statement.

## Examples

This example shows how to create a new SNMP user named “netops”. By default, this user will be registered on the local SNMP engine without authentication and encryption. Entries related to this user will be stored in permanent (nonvolatile) memory:

```
B5(su)->set snmp user netops
```

This example creates a new SNMP user named “admin” with DES encryption and MD5 authentication required. The encryption password is “admintest1” and the authentication password is “admintest2.” By default, this user will be registered on the local SNMP engine and entries related to this user will be stored in permanent (nonvolatile) memory.

```
B5(su)->set snmp user admin encryption des privacy admintest1 authentication md5 admintest2
```

## clear snmp user

Use this command to remove a user from the SNMPv3 security-model list.

### Syntax

```
clear snmp user user [remote remote]
```

### Parameters

<i>user</i>	Specifies an SNMPv3 user to remove.
<b>remote</b> <i>remote</i>	(Optional) Removes the user from a specific remote SNMP engine.

### Defaults

If **remote** is not specified, the user will be removed from the local SNMP engine.

### Mode

Switch command, read-write.

### Example

This example shows how to remove the SNMP user named "bill":

```
B5(su)->clear snmp user bill
```

## show snmp group

Use this command to display an SNMP group configuration. An SNMP group is a collection of SNMPv3 users who share the same access privileges.

### Syntax

```
show snmp group [groupname groupname] [user user] [security-model {v1 | v2c | usm}]  
[volatile | nonvolatile | read-only]
```

### Parameters

<b>groupname</b> <i>groupname</i>	(Optional) Displays information for a specific SNMP group.
<b>user</b> <i>user</i>	(Optional) Displays information about users within the specified group.
<b>security-model</b> <b>v1</b>   <b>v2c</b>   <b>usm</b>	(Optional) Displays information about groups assigned to a specific security SNMP model.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) Displays SNMP group information for a specified storage type.

### Defaults

If *groupname* is not specified, information about all SNMP groups will be displayed.

If *user* is not specified, information about all SNMP users will be displayed.

If **security-model** is not specified, user information about all SNMP versions will be displayed.

If not specified, information for all storage types will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display SNMP group information:

```
B5(su)->show snmp group
--- SNMP group information ---
Security model           = SNMPv1
Security/user name      = public
Group name              = Anyone
Storage type            = nonVolatile
Row status              = active

Security model           = SNMPv1
Security/user name      = public.router1
Group name              = Anyone
Storage type            = nonVolatile
Row status              = active
```

[Table 8-5](#) provides an explanation of the command output.

**Table 8-5 show snmp group Output Details**

Output Field	What It Displays...
Security model	SNMP version associated with this group.
Security/user name	User belonging to the SNMP group.
Group name	Name of SNMP group.
Storage type	Whether entry is stored in <b>volatile</b> , <b>nonvolatile</b> or <b>read-only</b> memory.
Row status	Status of this entry: <b>active</b> , <b>notInService</b> , or <b>notReady</b> .

## set snmp group

Use this command to create an SNMP group. This associates SNMPv3 users to a group that shares common access privileges.

### Syntax

```
set snmp group groupname user user security-model {v1 | v2c | usm} [volatile | nonvolatile]
```

### Parameters

<i>groupname</i>	Specifies an SNMP group name to create.
<b>user</b> <i>user</i>	Specifies an SNMPv3 user name to assign to the group.
<b>security-model</b> <b>v1</b>   <b>v2c</b>   <b>usm</b>	Specifies an SNMP security model to assign to the group.
<b>volatile</b>   <b>nonvolatile</b>	(Optional) Specifies a storage type for SNMP entries associated with the group.

### Defaults

If storage type is not specified, **nonvolatile** storage will be applied.

## Mode

Switch command, read-write.

## Example

This example shows how to create an SNMP group called “anyone”, assign a user named “public” and assign SNMPv3 security to the group:

```
B5(su)->set snmp group anyone user public security-model usm
```

# clear snmp group

Use this command to clear SNMP group settings globally or for a specific SNMP group and user.

## Syntax

```
clear snmp group groupname user [security-model {v1 | v2c | usm}]
```

## Parameters

<i>groupname</i>	Specifies the SNMP group to be cleared.
<i>user</i>	Specifies the SNMP user to be cleared.
<b>security-model v1</b>   <b>v2c</b>   <b>usm</b>	(Optional) Clears the settings associated with a specific security model.

## Defaults

If not specified, settings related to all security models will be cleared.

## Mode

Switch command, read-write.

## Example

This example shows how to clear all settings assigned to the “public” user within the SNMP group “anyone”:

```
B5(su)->clear snmp group anyone public
```

# show snmp community

Use this command to display SNMP community names and status. In SNMPv1 and v2, community names act as passwords to remote management.

## Syntax

```
show snmp community [name]
```

## Parameters

<i>name</i>	(Optional) Displays SNMP information for a specific community name.
-------------	---

## Defaults

If *name* is not specified, information will be displayed for all SNMP communities.

## Mode

Switch command, read-only.

## Example

This example shows how to display information about the SNMP “public” community name. For a description of this output, refer to **set snmp community** (page 8-14).

```
B5(su)->show snmp community public

--- Configured community strings ---

Name           = *****
Security name  = public
Context        =
Transport tag  =
Storage type   = nonVolatile
Status        = active
```

## set snmp community

Use this command to configure an SNMP community group.

### Syntax

```
set snmp community community [securityname securityname] [context context]
[transport transport] [volatile | nonvolatile]
```

### Parameters

<i>community</i>	Specifies a community group name.
<b>securityname</b> <i>securityname</i>	(Optional) Specifies an SNMP security name to associate with this community.
<b>context</b> <i>context</i>	(Optional) Specifies a subset of management information this community will be allowed to access. Valid values are full or partial context names. To review all contexts configured for the device, use the <b>show snmp context</b> command as described in “ <a href="#">show snmp context</a> ” on page 8-21.
<b>transport</b> <i>transport</i>	(Optional) Specifies the set of transport endpoints from which SNMP request with this community name will be accepted. Makes a link to a target address table.
<b>volatile</b>   <b>nonvolatile</b>	(Optional) Specifies the storage type for these entries.

### Defaults

If **securityname** is not specified, the *community* name will be used.

If **context** is not specified, the default (NULL) context is applied.

If **transport** tag is not specified, none will be applied.

If storage type is not specified, **nonvolatile** will be applied.

## Mode

Switch command, read-write.



## Usage

When you configure a community name, if you don't specify a context with the **context** parameter, the default (NULL) context is applied. If you want to change a configured context back to the default (NULL) context, enter a hyphen as the value of the **context** parameter, as shown in the Examples below.

## Examples

This example shows how to set an SNMP community name called "vip."

```
B5(su)->set snmp community vip
```

The example shows how to set the context for SNMP community "vip" to the default NULL context.

```
B5(su)->set snmp community vip context -
```

## clear snmp community

Use this command to delete an SNMP community name.

### Syntax

```
clear snmp community name
```

### Parameters

---

<b>name</b>	Specifies the SNMP community name to clear.
-------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to delete the community name "vip."

```
B5(su)->clear snmp community vip
```

## Configuring SNMP Access Rights

### Purpose

To review and configure SNMP access rights, assigning viewing privileges and security levels to SNMP user groups.

## Commands

For information about...	Refer to page...
show snmp access	<a href="#">8-16</a>
set snmp access	<a href="#">8-18</a>
clear snmp access	<a href="#">8-19</a>

## show snmp access

Use this command to display access rights and security levels configured for SNMP one or more groups.

### Syntax

```
show snmp access [groupname] [security-model {v1 | v2c | usm}] [noauthentication | authentication | privacy] [context context] [volatile | nonvolatile | read-only]
```

### Parameters

<i>groupname</i>	(Optional) Displays access information for a specific SNMPv3 group.
<b>security-model</b> v1   v2c   usm	(Optional) Displays access information for SNMP security model version 1, 2c or 3 (usm).
<b>noauthentication</b>   <b>authentication</b>   <b>privacy</b>	(Optional) Displays access information for a specific security level.
<b>context</b> <i>context</i>	(Optional) Displays access information for a specific context. For a description of how to specify SNMP contexts, refer to <a href="#">“Using SNMP Contexts to Access Specific MIBs”</a> on page 8-3.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) Displays access entries for a specific storage type.

### Defaults

If *groupname* is not specified, access information for all SNMP groups will be displayed.

If **security-model** is not specified, access information for all SNMP versions will be displayed.

If **noauthentication**, **authentication** or **privacy** are not specified, access information for all security levels will be displayed.

If **context** is not specified, all contexts will be displayed.

If **volatile**, **nonvolatile** or **read-only** are not specified, all entries of all storage types will be displayed.

### Mode

Switch command, read-only.

## Example

This example shows how to display SNMP access information:

```
B5(su)->show snmp access
Group           = SystemAdmin
Security model  = USM
Security level  = noAuthNoPriv
Read View      = All
Write View     =
Notify View    = All
Context match  = exact match
Storage type   = nonVolatile
Row status     = active

Group           = NightOperator
Security model  = USM
Security level  = noAuthNoPriv
Read View      = All
Write View     =
Notify View    = All
Context match  = exact match
Storage type   = nonVolatile
Row status     = active
```

[Table 8-6](#) provides an explanation of the command output.

**Table 8-6 show snmp access Output Details**

Output Field	What It Displays...
Group	SNMP group name.
Security model	Security model applied to this group. Valid types are: <b>SNMPv1</b> , <b>SNMPv2c</b> , and SNMPv3 (User based - <b>USM</b> ).
Security level	Security level applied to this group. Valid levels are: <ul style="list-style-type: none"> <li>noAuthNoPrivacy (<b>no authentication</b> required)</li> <li>AuthNoPrivacy (<b>authentication</b> required)</li> <li>authPriv (<b>privacy</b> -- most secure level)</li> </ul>
Read View	Name of the view that allows this group to view SNMP MIB objects.
Write View	Name of the view that allows this group to configure the contents of the SNMP agent.
Notify View	Name of the view that allows this group to send an SNMP trap message.
Context match	Whether or not SNMP context match must be exact (full context name match) or a partial match with a given prefix.
Storage type	Whether access entries for this group are stored in <b>volatile</b> , <b>nonvolatile</b> or <b>read-only</b> memory.
Row status	Status of this entry: <b>active</b> , <b>notInService</b> , or <b>notReady</b> .

## set snmp access

Use this command to set an SNMP access configuration.

### Syntax

```
set snmp access groupname security-model {v1 | v2c | usm} [noauthentication |
authentication | privacy] [context context] [exact | prefix] [read read] [write
write] [notify notify] [volatile | nonvolatile]
```

### Parameters

<i>groupname</i>	Specifies a name for an SNMPv3 group.
<b>security-model</b> <i>v1</i>   <i>v2c</i>   <i>usm</i>	Specifies SNMP version 1, 2c or 3 (usm).
<b>noauthentication</b>   <b>authentication</b>   <b>privacy</b>	(Optional) Applies SNMP security level as no authentication, authentication (without privacy) or privacy. Privacy specifies that messages sent on behalf of the user are protected from disclosure.
<b>context</b> <i>context</i> <b>exact</b>   <b>prefix</b>	(Optional) Sets the context for this access configuration and specifies that the match must be exact (matching the whole context string) or a prefix match only. Context is a subset of management information this SNMP group will be allowed to access. Valid values are full or partial context names. To review all contexts configured for the device, use the <b>show snmp context</b> command as described in “ <a href="#">show snmp context</a> ” on page 8-21.
<b>read</b> <i>read</i>	(Optional) Specifies a read access view.
<b>write</b> <i>write</i>	(Optional) Specifies a write access view.
<b>notify</b> <i>notify</i>	(Optional) Specifies a notify access view.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) Stores associated SNMP entries as temporary or permanent, or read-only.

### Defaults

If security level is not specified, no authentication will be applied.

If **context** is not specified, access will be enabled for the default context. If **context** is specified without a context match, **exact** match will be applied.

If **read** view is not specified none will be applied.

If **write** view is not specified, none will be applied.

If **notify** view is not specified, none will be applied.

If storage type is not specified, entries will be stored as permanent and will be held through device reboot.

### Mode

Switch command, read-write.

### Example

This example permits the “powergroup” to manage all MIBs via SNMPv3:

```
B5(su)->set snmp access powergroup security-model usm
```

## clear snmp access

Use this command to clear the SNMP access entry of a specific group, including its set SNMP security-model, and level of security.

### Syntax

```
clear snmp access groupname security-model {v1 | v2c | usm} [noauthentication | authentication | privacy] [context context]
```

### Parameters

<i>groupname</i>	Specifies the name of the SNMP group for which to clear access.
<b>security-model</b> v1   v2c   usm	Specifies the security model to be cleared for the SNMP access group.
<b>noauthentication</b>   <b>authentication</b>   <b>privacy</b>	(Optional) Clears a specific security level for the SNMP access group.
<b>context</b> <i>context</i>	(Optional) Clears a specific context for the SNMP access group. Enter / - / to clear the default context.

### Defaults

If security level is not specified, all levels will be cleared.

If **context** is not specified, none will be applied.

### Mode

Switch command, read-write.

### Example

This example shows how to clear SNMP version 3 access for the “mis-group” via the authentication protocol:

```
B5(su)->clear snmp access mis-group security-model usm authentication
```

## Configuring SNMP MIB Views

### Purpose

To review and configure SNMP MIB views. SNMP views map SNMP objects to access rights.

### Commands

For information about...	Refer to page...
show snmp view	<a href="#">8-20</a>
show snmp context	<a href="#">8-21</a>
set snmp view	<a href="#">8-21</a>
clear snmp view	<a href="#">8-22</a>

## show snmp view

Use this command to display the MIB configuration for SNMPv3 view-based access (VACM).

### Syntax

```
show snmp view [viewname] [subtree oid-or-mibobject] [volatile | nonvolatile | read-only]
```

### Parameters

<i>viewname</i>	(Optional) Displays information for a specific MIB view.
<b>subtree</b> <i>oid-or-mibobject</i>	(Optional) Displays information for a specific MIB subtree when <i>viewname</i> is specified.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) Displays entries for a specific storage type.

### Defaults

If no parameters are specified, all SNMP MIB view configuration information will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display SNMP MIB view configuration information:

```
B5(su)->show snmp view

--- SNMP MIB View information ---
View Name      = All
Subtree OID    = 1
Subtree mask   =
View Type      = included
Storage type   = nonVolatile
Row status     = active

View Name      = All
Subtree OID    = 0.0
Subtree mask   =
View Type      = included
Storage type   = nonVolatile
Row status     = active

View Name      = Network
Subtree OID    = 1.3.6.1.2.1
Subtree mask   =
View Type      = included
Storage type   = nonVolatile
Row status     = active
```

[Table 8-7](#) provides an explanation of the command output. For details on using the **set snmp view** command to assign variables, refer to “[set snmp view](#)” on page 8-21.

**Table 8-7 show snmp view Output Details**

Output Field	What It Displays...
View Name	Name assigned to a MIB view.
Subtree OID	Name identifying a MIB subtree.
Subtree mask	Bitmask applied to a MIB subtree.
View Type	Whether or not subtree use must be <b>included</b> or <b>excluded</b> for this view.
Storage type	Whether storage is in <b>nonVolatile</b> or <b>Volatile</b> memory
Row status	Status of this entry: <b>active</b> , <b>notInService</b> , or <b>notReady</b> .

## show snmp context

Use this command to display the context list configuration for SNMP's view-based access control.

### Syntax

```
show snmp context
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Usage

An SNMP context is a collection of management information that can be accessed by an SNMP agent or entity. The default context allows all SNMP agents to access all management information (MIBs). When created using the **set snmp access** command ("[set snmp access](#)" on page 8-18), other contexts can be applied to limit access to a subset of management information.

### Example

This example shows how to display a list of all SNMP contexts known to the device:

```
B5(su)->show snmp context

--- Configured contexts:
default context (all mibs)
```

## set snmp view

Use this command to set a MIB configuration for SNMPv3 view-based access (VACM).

### Syntax

```
set snmp view viewname viewname subtree subtree [mask mask] [included | excluded]
[volatile | nonvolatile]
```

## Parameters

<b>viewname</b> <i>viewname</i>	Specifies a name for a MIB view.
<b>subtree</b> <i>subtree</i>	Specifies a MIB subtree name.
<b>mask</b> <i>mask</i>	(Optional) Specifies a bitmask for a subtree.
<b>included</b>   <b>excluded</b>	(Optional) Specifies subtree use (default) or no subtree use.
<b>volatile</b>   <b>nonvolatile</b>	(Optional) Specifies the use of temporary or permanent (default) storage.

## Defaults

If not specified, **mask** will be set to **255.255.255.255**

If not specified, subtree use will be **included**.

If storage type is not specified, **nonvolatile** (permanent) will be applied.

## Mode

Switch command, read-write.

## Example

This example shows how to set an SNMP MIB view to “public” with a subtree name of 1.3.6.1 included:

```
B5(su)->set snmp view viewname public subtree 1.3.6.1 included
```

# clear snmp view

Use this command to delete an SNMPv3 MIB view.

## Syntax

```
clear snmp view viewname subtree
```

## Parameters

<i>viewname</i>	Specifies the MIB view name to be deleted.
<i>subtree</i>	Specifies the subtree name of the MIB view to be deleted.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to delete SNMP MIB view “public”:

```
B5(su)->clear snmp view public 1.3.6.1
```



# Configuring SNMP Target Parameters

## Purpose

To review and configure SNMP target parameters. This controls where and under what circumstances SNMP notifications will be sent. A target parameter entry can be bound to a target IP address allowed to receive SNMP notification messages with the `set snmp targetaddr` command (“`set snmp targetaddr`” on page 8-27).

## Commands

For information about...	Refer to page...
<code>show snmp targetparams</code>	<a href="#">8-23</a>
<code>set snmp targetparams</code>	<a href="#">8-24</a>
<code>clear snmp targetparams</code>	<a href="#">8-25</a>

## show snmp targetparams

Use this command to display SNMP parameters used to generate a message to a target.

### Syntax

```
show snmp targetparams [targetParams] [volatile | nonvolatile | read-only]
```

### Parameters

<i>targetParams</i>	(Optional) Displays entries for a specific target parameter.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) Displays target parameter entries for a specific storage type.

### Defaults

If *targetParams* is not specified, entries associated with all target parameters will be displayed.

If not specified, entries of all storage types will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display SNMP target parameters information:

```
B5(su)->show snmp targetparams

--- SNMP TargetParams information ---
Target Parameter Name   = vlExampleParams
Security Name           = public
Message Proc. Model     = SNMPv1
Security Level          = noAuthNoPriv
Storage type            = nonVolatile
Row status               = active
```

```

Target Parameter Name = v2cExampleParams
Security Name         = public
Message Proc. Model  = SNMPv2c
Security Level       = noAuthNoPriv
Storage type        = nonVolatile
Row status          = active

```

```

Target Parameter Name = v3ExampleParams
Security Name         = CharlieDChief
Message Proc. Model  = USM
Security Level       = authNoPriv
Storage type        = nonVolatile
Row status          = active

```

Table 8-8 provides an explanation of the command output.

**Table 8-8 show snmp targetparams Output Details**

Output Field	What It Displays...
Target Parameter Name	Unique identifier for the parameter in the SNMP target parameters table. Maximum length is 32 bytes.
Security Name	Security string definition.
Message Proc. Model	SNMP version.
Security Level	Type of security level ( <b>auth</b> : security level is set to use authentication protocol, <b>noauth</b> : security level is not set to use authentication protocol, or <b>privacy</b> ).
Storage type	Whether entry is stored in <b>volatile</b> , <b>nonvolatile</b> or <b>read-only</b> memory.
Row status	Status of this entry: <b>active</b> , <b>notInService</b> , or <b>notReady</b> .

## set snmp targetparams

Use this command to set SNMP target parameters, a named set of security/authorization criteria used to generate a message to a target.

### Syntax

```

set snmp targetparams paramsname user user security-model {v1 | v2c | usm} message-  
processing {v1 | v2c | v3} [noauthentication | authentication | privacy] [volatile  
| nonvolatile]

```

### Parameters

<i>paramsname</i>	Specifies a name identifying parameters used to generate SNMP messages to a particular target.
<b>user</b> <i>user</i>	Specifies an SNMPv1 or v2 community name or an SNMPv3 user name. Maximum length is 32 bytes.
<b>security-model</b> <b>v1</b>   <b>v2c</b>   <b>usm</b>	Specifies the SNMP security model applied to this target parameter as version 1, 2c or 3 (usm).
<b>message-processing</b> <b>v1</b>   <b>v2c</b>   <b>v3</b>	Specifies the SNMP message processing model applied to this target parameter as version 1, 2c or 3.

<b>noauthentication</b>   <b>authentication</b>   <b>privacy</b>	(Optional) Specifies the SNMP security level applied to this target parameter as no authentication, authentication (without privacy) or privacy. Privacy specifies that messages sent on behalf of the user are protected from disclosure.
<b>volatile</b>   <b>nonvolatile</b>	(Optional) Specifies the storage type applied to this target parameter.

## Defaults

None.

If not specified, security level will be set to **noauthentication**.

If not specified, storage type will be set to **nonvolatile**.

## Mode

Switch command, read-write.

## Example

This example shows how to set SNMP target parameters named "v1ExampleParams" for a user named "fred" using version 3 security model and message processing, and authentication:

```
B5(su)->set snmp targetparams v1ExampleParams user fred security-model usm
message-processing v3 authentication
```

# clear snmp targetparams

Use this command to clear the SNMP target parameter configuration.

## Syntax

```
clear snmp targetparams targetParams
```

## Parameters

<i>targetParams</i>	Specifies the name of the parameter in the SNMP target parameters table to be cleared.
---------------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear SNMP target parameters named "v1ExampleParams":

```
B5(su)->clear snmp targetparams v1ExampleParams
```

# Configuring SNMP Target Addresses

## Purpose

To review and configure SNMP target addresses which will receive SNMP notification messages. An address configuration can be linked to optional SNMP transmit, or target, parameters (such as timeout, retry count, and UDP port) set with the **set snmp targetparams** command (page 8-24).

## Commands

For information about...	Refer to page...
show snmp targetaddr	<a href="#">8-26</a>
set snmp targetaddr	<a href="#">8-27</a>
clear snmp targetaddr	<a href="#">8-28</a>

## show snmp targetaddr

Use this command to display SNMP target address information.

### Syntax

```
show snmp targetaddr [targetAddr] [volatile | nonvolatile | read-only]
```

### Parameters

<i>targetAddr</i>	(Optional) Displays information for a specific target address name.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) When target address is specified, displays target address information for a specific storage type.

### Defaults

If *targetAddr* is not specified, entries for all target address names will be displayed.

If not specified, entries of all storage types will be displayed for a target address.

### Mode

Switch command, read-only.

### Example

This example shows how to display SNMP target address information:

```
B5(su)->show snmp targetaddr
Target Address Name      = labmachine
Tag List                 = v2cTrap
IP Address               = 10.2.3.116
UDP Port#               = 162
Target Mask              = 255.255.255.255
Timeout                 = 1500
Retry count              = 4
Parameters               = v2cParams
Storage type             = nonVolatile
```

Row status = active

Table 8-9 provides an explanation of the command output.

**Table 8-9 show snmp targetaddr Output Details**

Output Field	What It Displays...
Target Address Name	Unique identifier in the snmpTargetAddressTable.
Tag List	Tags a location to the target address as a place to send notifications.
IP Address	Target IP address.
UDP Port#	Number of the UDP port of the target host to use.
Target Mask	Target IP address mask.
Timeout	Timeout setting for the target address.
Retry count	Retry setting for the target address.
Parameters	Entry in the snmpTargetParamsTable.
Storage type	Whether entry is stored in <b>volatile</b> , <b>nonvolatile</b> or <b>read-only</b> memory.
Row status	Status of this entry: <b>active</b> , <b>notInService</b> , or <b>notReady</b> .

## set snmp targetaddr

Use this command to configure an SNMP target address. The target address is a unique identifier and a specific IP address that will receive SNMP notification messages and determine which community strings will be accepted. This address configuration can be linked to optional SNMP transmit parameters (such as timeout, retry count, and UDP port).

### Syntax

```
set snmp targetaddr targetaddr ipaddr param param [udpport udpport] [mask mask]
[timeout timeout] [retries retries] [taglist taglist] [volatile | nonvolatile]
```

### Parameters

<i>targetaddr</i>	Specifies a unique identifier to index the snmpTargetAddrTable. Maximum length is 32 bytes.
<i>ipaddr</i>	Specifies the IP address of the target.
<b>param</b> <i>param</i>	Specifies an entry in the SNMP target parameters table, which is used when generating a message to the target. Maximum length is 32 bytes.
<b>udpport</b> <i>udpport</i>	(Optional) Specifies which UDP port of the target host to use.
<b>mask</b> <i>mask</i>	(Optional) Specifies the IP mask of the target.
<b>timeout</b> <i>timeout</i>	(Optional) Specifies the maximum round trip time allowed to communicate to this target address. This value is in .01 seconds and the default is 1500 (15 seconds.)
<b>retries</b> <i>retries</i>	(Optional) Specifies the number of message retries allowed if a response is not received. Default is 3.

<b>taglist</b> <i>taglist</i>	(Optional) Specifies a list of SNMP notify tag values. This tags a location to the target address as a place to send notifications. List must be enclosed in quotes and tag values must be separated by a space (for example, "tag 1 tag 2").
<b>volatile</b>   <b>nonvolatile</b>	(Optional) Specifies temporary (default), or permanent storage for SNMP entries.

## Defaults

If not specified, *udpport* will be set to **162**.

If not specified, *mask* will be set to **255.255.255.255**

If not specified, *timeout* will be set to **1500**.

If not specified, number of *retries* will be set to **3**.

If **taglist** is not specified, none will be set.

If not specified, storage type will be **nonvolatile**.

## Mode

Switch command, read-write.

## Example

This example shows how to configure a trap notification called "TrapSink." This trap notification will be sent to the workstation 192.168.190.80 (which is target address "tr"). It will use security and authorization criteria contained in a target parameters entry called "v2cExampleParams". For more information on configuring a basic SNMP trap, refer to "Creating a Basic SNMP Trap Configuration" on page 8-36:

```
B5(su)->set snmp targetaddr tr 192.168.190.80 param v2cExampleParams taglist
TrapSink
```

# clear snmp targetaddr

Use this command to delete an SNMP target address entry.

## Syntax

```
clear snmp targetaddr targetAddr
```

## Parameters

<i>targetAddr</i>	Specifies the target address entry to delete.
-------------------	---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear SNMP target address entry “tr”:

```
B5(su)->clear snmp targetaddr tr
```

# Configuring SNMP Notification Parameters

## About SNMP Notify Filters

Profiles indicating which targets should not receive SNMP notification messages are kept in the NotifyFilter table. If this table is empty, meaning that no filtering is associated with any SNMP target, then no filtering will take place. “Traps” or “informs” notifications will be sent to all destinations in the SNMP targetAddrTable that have tags matching those found in the NotifyTable.

When the NotifyFilter table contains profile entries, the SNMP agent will find any filter profile name that corresponds to the target parameter name contained in an outgoing notification message. It will then apply the appropriate subtree-specific filter when generating notification messages.

## Purpose

To configure SNMP notification parameters and optional filters. Notifications are entities which handle the generation of SNMP v1 and v2 “traps” or SNMP v3 “informs” messages to select management targets. Optional notification filters identify which targets should not receive notifications. For a sample SNMP trap configuration showing how SNMP notification parameters are associated with security and authorization criteria (target parameters) and mapped to a management target address, refer to [“Creating a Basic SNMP Trap Configuration”](#) on page 8-36.

## Commands

For information about...	Refer to page...
show snmp notify	<a href="#">8-30</a>
set snmp notify	<a href="#">8-31</a>
clear snmp notify	<a href="#">8-31</a>
show snmp notifyfilter	<a href="#">8-32</a>
set snmp notifyfilter	<a href="#">8-33</a>
clear snmp notifyfilter	<a href="#">8-33</a>
show snmp notifyprofile	<a href="#">8-34</a>
set snmp notifyprofile	<a href="#">8-35</a>
clear snmp notifyprofile	<a href="#">8-35</a>

## show snmp notify

Use this command to display the SNMP notify configuration, which determines the management targets that will receive SNMP notifications.

### Syntax

```
show snmp notify [notify] [volatile | nonvolatile | read-only]
```

### Parameters

<i>notify</i>	(Optional) Displays notify entries for a specific notify name.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) Displays notify entries for a specific storage type.

### Defaults

If a *notify* name is not specified, all entries will be displayed.

If **volatile**, **nonvolatile**, or **read-only** are not specified, all storage type entries will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display the SNMP notify information:

```
B5(su)->show snmp notify

--- SNMP notifyTable information ---
Notify name      = 1
Notify Tag       = Console
Notify Type      = trap
Storage type     = nonVolatile
Row status       = active

Notify name      = 2
Notify Tag       = TrapSink
Notify Type      = trap
Storage type     = nonVolatile
Row status       = active
```

[Table 8-10](#) provides an explanation of the command output.

**Table 8-10 show snmp notify Output Details**

Output Field	What It Displays...
Notify name	A unique identifier used to index the SNMP notify table.
Notify Tag	Name of the entry in the SNMP notify table.
Notify Type	Type of notification: SNMPv1 or v2 <b>trap</b> or SNMPv3 <b>InformRequest</b> message.
Storage type	Whether access entry is stored in <b>volatile</b> , <b>nonvolatile</b> , or <b>read-only</b> memory.
Row status	Status of this entry: <b>active</b> , <b>notInService</b> , or <b>notReady</b> .



## set snmp notify

Use this command to set the SNMP notify configuration. This creates an entry in the SNMP notify table, which is used to select management targets who should receive notification messages. This command's **tag** parameter can be used to bind each entry to a target address using the **set snmp targetaddr** command ("[set snmp targetaddr](#)" on page 8-27).

### Syntax

```
set snmp notify notify tag tag [trap | inform] [volatile | nonvolatile]
```

### Parameters

<i>notify</i>	Specifies an SNMP notify name.
tag <i>tag</i>	Specifies an SNMP notify tag. This binds the notify name to the SNMP target address table.
<b>trap</b>   <b>inform</b>	(Optional) Specifies SNMPv1 or v2 Trap messages (default) or SNMP v3 InformRequest messages.
<b>volatile</b>   <b>nonvolatile</b>	(Optional) Specifies temporary (default), or permanent storage for SNMP entries.

### Defaults

If not specified, message type will be set to **trap**.

If not specified, storage type will be set to **nonvolatile**.

### Mode

Switch command, read-write.

### Example

This example shows how to set an SNMP notify configuration with a notify name of "hello" and a notify tag of "world". Notifications will be sent as trap messages and storage type will automatically default to permanent:

```
B5(su)->set snmp notify hello tag world trap
```

## clear snmp notify

Use this command to clear an SNMP notify configuration.

### Syntax

```
clear snmp notify notify
```

### Parameters

<i>notify</i>	Specifies an SNMP notify name to clear.
---------------	---

### Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear the SNMP notify configuration for “hello”:

```
B5(su)->clear snmp notify hello
```

# show snmp notifyfilter

Use this command to display SNMP notify filter information, identifying which profiles will not receive SNMP notifications.

## Syntax

```
show snmp notifyfilter [profile] [subtree oid-or-mibobject] [volatile |  
nonvolatile | read-only]
```

## Parameters

<i>profile</i>	(Optional) Displays a specific notify filter.
<b>subtree</b> <i>oid-or-mibobject</i>	(Optional) Displays a notify filter within a specific subtree.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) Displays notify filter entries of a specific storage type.

## Defaults

If no parameters are specified, all notify filter information will be displayed.

## Mode

Switch command, read-only.

## Usage

See “[About SNMP Notify Filters](#)” on page 8-29 for more information about notify filters.

## Example

This example shows how to display SNMP notify filter information. In this case, the notify profile “pilot1” in subtree 1.3.6 will not receive SNMP notification messages:

```
B5(su)->show snmp notifyfilter

--- SNMP notifyFilter information ---
Profile           = pilot1
Subtree           = 1.3.6
Filter type       = included
Storage type      = nonVolatile
Row status        = active
```

## set snmp notifyfilter

Use this command to create an SNMP notify filter configuration. This identifies which management targets should NOT receive notification messages, which is useful for fine-tuning the amount of SNMP traffic generated.

### Syntax

```
set snmp notifyfilter profile subtree oid-or-mibobject [mask mask] [included | excluded] [volatile | nonvolatile]
```

### Parameters

<i>profile</i>	Specifies an SNMP filter notify name.
<b>subtree</b> <i>oid-or-mibobject</i>	Specifies a MIB subtree ID target for the filter.
<b>mask</b> <i>mask</i>	(Optional) Applies a subtree mask.
<b>included</b>   <b>excluded</b>	(Optional) Specifies that subtree is included or excluded.
<b>volatile</b>   <b>nonvolatile</b>	(Optional) Specifies a storage type.

### Defaults

If not specified, **mask** is not set.

If not specified, subtree will be **included**.

If storage type is not specified, **nonvolatile** (permanent) will be applied.

### Mode

Switch command, read-write.

### Usage

See [“About SNMP Notify Filters”](#) on page 8-29 for more information about notify filters.

### Example

This example shows how to create an SNMP notify filter called “pilot1” with a MIB subtree ID of 1.3.6:

```
B5(su)->set snmp notifyfilter pilot1 subtree 1.3.6
```

## clear snmp notifyfilter

Use this command to delete an SNMP notify filter configuration.

### Syntax

```
clear snmp notifyfilter profile subtree oid-or-mibobject
```

## Parameters

<i>profile</i>	Specifies an SNMP filter notify name to delete.
<b>subtree</b> <i>oid-or-mibobject</i>	Specifies a MIB subtree ID containing the filter to be deleted.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to delete the SNMP notify filter “pilot1”:

```
B5(su)->clear snmp notifyfilter pilot1 subtree 1.3.6
```

# show snmp notifyprofile

Use this command to display SNMP notify profile information. This associates target parameters to an SNMP notify filter to determine who should not receive SNMP notifications.

## Syntax

```
show snmp notifyprofile [profile] [targetparam targetparam] [volatile | nonvolatile | read-only]
```

## Parameters

<i>profile</i>	(Optional) Displays a specific notify profile.
<b>targetparam</b> <i>targetparam</i>	(Optional) Displays entries for a specific target parameter.
<b>volatile</b>   <b>nonvolatile</b>   <b>read-only</b>	(Optional) Displays notify filter entries of a specific storage type.

## Defaults

If no parameters are specified, all notify profile information will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display SNMP notify information for the profile named “area51”:

```
B5(su)->show snmp notifyprofile area51

--- SNMP notifyProfile information ---
Notify Profile    = area51
TargetParam      = v3ExampleParams
Storage type     = nonVolatile
```

Row status = active

## set snmp notifyprofile

Use this command to create an SNMP notify filter profile configuration. This associates a notification filter, created with the **set snmp notifyfilter** command (“[set snmp notifyfilter](#)” on page 8-33), to a set of SNMP target parameters to determine which management targets should not receive SNMP notifications.

### Syntax

```
set snmp notifyprofile profile targetparam targetparam [volatile | nonvolatile]
```

### Parameters

<i>profile</i>	Specifies an SNMP filter notify name.
<b>targetparam</b> <i>targetparam</i>	Specifies an associated entry in the SNMP Target Params Table.
<b>volatile</b>   <b>nonvolatile</b>	(Optional) Specifies a storage type.

### Defaults

If storage type is not specified, **nonvolatile** (permanent) will be applied.

### Mode

Switch command, read-write.

### Example

This example shows how to create an SNMP notify profile named area51 and associate a target parameters entry.

```
B5(su)->set snmp notifyprofile area51 targetparam v3ExampleParams
```

## clear snmp notifyprofile

Use this command to delete an SNMP notify profile configuration.

### Syntax

```
clear snmp notifyprofile profile targetparam targetparam
```

### Parameters

<i>profile</i>	Specifies an SNMP filter notify name to delete.
<b>targetparam</b> <i>targetparam</i>	Specifies an associated entry in the snmpTargetParamsTable.

### Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to delete SNMP notify profile “area51”:

```
B5(su)->clear snmp notifyprofile area51 targetparam v3ExampleParams
```

# Creating a Basic SNMP Trap Configuration

Traps are notification messages sent by an SNMPv1 or v2 agent to a network management station, a console, or a terminal to indicate the occurrence of a significant event, such as when a port or device goes up or down, when there are authentication failures, and when power supply errors occur. The following configuration example shows how to use CLI commands to associate SNMP notification parameters with security and authorization criteria (target parameters), and map the parameters to a management target address.



**Note:** This example illustrates how to configure an SNMPv2 trap notification. Creating an SNMPv1 or v3 Trap, or an SNMPv3 Inform notification would require using the same commands with different parameters, where appropriate. Always ensure that v1/v2 communities or v3 users used for generating traps or informs are pre-configured with enough privileges to access corresponding MIBs.

Complete an SNMPv2 trap configuration on a Enterasys B5 device as follows:

1. Create a community name that will act as an SNMP user password.
2. Create an SNMP target parameters entry to associate security and authorization criteria to the users in the community created in Step 1.
3. Verify if any applicable SNMP notification entries exist, or create a new one. You will use this entry to send SNMP notification messages to the appropriate management targets created in Step 2.
4. Create a target address entry to bind a management IP address to:
  - The notification entry and tag name created in Step 3 and
  - The target parameters entry created in Step 2.

Table 8-11 shows the commands used to complete an SNMPv2 trap configuration on a Enterasys B5 device.

**Table 8-11 Basic SNMP Trap Configuration**

To do this...	Use these commands...
Create a community name.	<code>set snmp community</code>
Create an SNMP target parameters entry.	<code>set snmp targetparams</code>
Verify if any applicable SNMP notification entries exist.	<code>show snmp notify</code>
Create a new notification entry.	<code>set snmp notify</code>
Create a target address entry.	<code>set snmp targetaddr</code>

## Example

This example shows how to:

- Create an SNMP community called **mgmt**.
- Configure a trap notification called **TrapSink**.

This trap notification will be sent with the community name **mgmt** to the workstation **192.168.190.80** (which is target address **tr**). It will use security and authorization criteria contained in a target parameters entry called **v2cExampleParams**.

```
B5(su)->set snmp community mgmt
B5(su)->set snmp targetparams v2cExampleParams user mgmt
security-model v2c message-processing v2c
B5(su)->set snmp notify entry1 tag TrapSink
B5(su)->set snmp targetaddr tr 192.168.190.80 param v2cExampleParams taglist
TrapSink
```

## How SNMP Will Use This Configuration

In order to send a trap/notification requested by a MIB code, the SNMP agent requires the equivalent of a trap “door”, a “key” to unlock the door, and a “procedure” for crossing the doorstep. To determine if all these elements are in place, the SNMP agent proceeds as follows:

1. Determines if the “keys” for trap “doors” do exist. In the example configuration above, the key that SNMP is looking for is the notification entry created with the **set snmp notify** command which, in this case, is a key labeled **entry1**.
2. Searches for the doors matching such a key. For example, the parameters set for the **entry1** key shows that it opens only the door **TrapSink**.
3. Verifies that the specified door **TrapSink** is, in fact, available. In this case it was built using the **set snmp targetaddr** command. This command also specifies that this door leads to the management station **192.168.190.80**, and the “procedure” (**targetparams**) to cross the doorstep is called **v2ExampleParams**.
4. Verifies that the **v2ExampleParams** description of how to step through the door is, in fact, there. The agent checks **targetparams** entries and determines this description was made with the **set snmp targetparams** command, which tells exactly which SNMP protocol to use and what community name to provide. In this case, the community name is **mgmt**.
5. Verifies that the **mgmt** community name is available. In this case, it has been configured using the **set snmp community** command.
6. Sends the trap notification message.

# Configuring the SNMP Management Interface

## Purpose

To configure the source IP address used by the SNMP agent when generating SNMP traps.

## Commands

For information about...	Refer to page...
<a href="#">show snmp interface</a>	<a href="#">8-38</a>
<a href="#">set snmp interface</a>	<a href="#">8-38</a>
<a href="#">clear snmp interface</a>	<a href="#">8-40</a>

## show snmp interface

Use this command to display the interface used for the source IP address of the SNMP agent when generating SNMP traps.

### Syntax

```
show snmp interface
```

### Parameters

None.

### Defaults

None.

### Mode

Switch mode, read-only.

### Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the SNMP agent.

```
B5(rw)->show snmp interface
loopback 1 192.168.10.1
```

## set snmp interface

Use this command to specify the interface used for the source IP address of the SNMP agent when generating SNMP traps.

### Syntax

```
set snmp interface {loopback loop-ID | vlan vlan-ID}
```



## Parameters

<b>loopback</b> <i>loop-ID</i>	Specifies the loopback interface to be used. The value of <i>loop-ID</i> can range from 0 to 7.
<b>vlan</b> <i>vlan-ID</i>	Specifies the VLAN interface to be used. The value of <i>vlan-ID</i> can range from 1 to 4093.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command allows you to configure the source IP address used by the SNMP agent when generating SNMP traps. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the SNMP agent.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface will be used.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

## Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the SNMP agent source IP address.

```
B5(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
B5(rw)->router(Config-if(Vlan 100))#exit
B5(rw)->router(Config)#exit
B5(rw)->router#exit
B5(rw)->router>exit
B5(rw)->set snmp interface vlan 100

B5(rw)->show snmp interface
vlan 100 192.168.10.1
```

## clear snmp interface

Use this command to clear the interface used for the source IP address of the SNMP agent back to the default of the Host interface.

### Syntax

```
clear snmp interface
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This command returns the interface used for the source IP address of the SNMP agent back to the default of the Host interface.

```
B5(rw)->show snmp interface
vlan 100 192.168.10.1
B5(rw)->clear snmp interface
B5(rw)->
```

## Spanning Tree Configuration

This chapter describes the Spanning Tree Configuration set of commands and how to use them.

For information about...	Refer to page...
<a href="#">Spanning Tree Configuration Summary</a>	9-1
<a href="#">Configuring Spanning Tree Bridge Parameters</a>	9-3
<a href="#">Configuring Spanning Tree Port Parameters</a>	9-34
<a href="#">Configuring Spanning Tree Loop Protect Parameters</a>	9-42



**Caution:** Spanning Tree configuration should be performed only by personnel who are very knowledgeable about Spanning Trees and the configuration of the Spanning Tree Algorithm. Otherwise, the proper operation of the network could be at risk.

### Spanning Tree Configuration Summary



**Note:** An Enterasys Networks Feature Guide document containing an in-depth discussion of Spanning Tree configuration is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads/>

### Overview: Single, Rapid, and Multiple Spanning Tree Protocols

The IEEE 802.1D Spanning Tree Protocol (STP) resolves the problems of physical loops in a network by establishing one primary path between any two devices in a network. Any duplicate paths are barred from use and become standby or blocked paths until the original path fails, at which point they can be brought into service.

#### RSTP

The IEEE 802.1w Rapid Spanning Protocol (RSTP), an evolution of 802.1D, can achieve much faster convergence than legacy STP in a properly configured network. RSTP significantly reduces the time to reconfigure the network's active topology when physical topology or configuration parameter changes occur. It selects one switch as the root of a Spanning Tree-connected active topology and assigns port roles to individual ports on the switch, depending on whether that port is part of the active topology.

RSTP provides rapid connectivity following the failure of a switch, switch port, or a LAN. A new root port and the designated port on the other side of the bridge transition to forwarding through an explicit handshake between them. By default, user ports are configured to rapidly transition to forwarding in RSTP.

## MSTP

The IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) builds upon 802.1D and RSTP by optimizing utilization of redundant links between switches in a network. When redundant links exist between a pair of switches running single STP, one link is forwarding while the others are blocking for all traffic flowing between the two switches. The blocking links are effectively used only if the forwarding link goes down. MSTP assigns each VLAN present on the network to a particular Spanning Tree instance, allowing each switch port to be in a distinct state for each such instance: blocking for one Spanning Tree while forwarding for another. Thus, traffic associated with one set of VLANs can traverse a particular inter-switch link, while traffic associated with another set of VLANs can be blocked on that link. If VLANs are assigned to Spanning Trees wisely, no inter-switch link will be completely idle, maximizing network utilization.

For details on creating Spanning Tree instances, refer to “[set spantree msti](#)” on page 9-12.

For details on mapping Spanning Tree instances to VLANs, refer to “[set spantree mstmap](#)” on page 9-14.



**Note:** MSTP and RSTP are fully compatible and interoperable with each other and with legacy STP 802.1D.

## Spanning Tree Features

The Enterasys B5 device meets the requirements of the Spanning Tree Protocols by performing the following functions:

- Creating a single Spanning Tree from any arrangement of switching or bridging elements.
- Compensating automatically for the failure, removal, or addition of any device in an active data path.
- Achieving port changes in short time intervals, which establishes a stable active topology quickly with minimal network disturbance.
- Using a minimum amount of communications bandwidth to accomplish the operation of the Spanning Tree Protocol.
- Reconfiguring the active topology in a manner that is transparent to stations transmitting and receiving data packets.
- Managing the topology in a consistent and reproducible manner through the use of Spanning Tree Protocol parameters.



**Note:** The term “bridge” is used as an equivalent to the term “switch” or “device” in this document.

## Loop Protect

The Loop Protect feature prevents or short circuits loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point-to-point inter-switch links (ISLs) before their states are allowed to become forwarding. Further, if a BPDU timeout occurs on a port, its state becomes listening until a BPDU is received.

Both upstream and downstream facing ports are protected. When a root or alternate port loses its path to the root bridge due to a message age expiration it takes on the role of designated port. It will not forward traffic until a BPDU is received. When a port is intended to be the designated port in an ISL it constantly proposes and will not forward until a BPDU is received, and will revert to

listening if it fails to get a response. This protects against misconfiguration and protocol failure by the connected bridge.

The Disputed BPDU mechanism protects against looping in situations where there is one way communication. A disputed BPDU is one in which the flags field indicates a designated role and learning and the priority vector is worse than that already held by the port. If a disputed BPDU is received, the port is forced to the listening state. When an inferior designated BPDU with the learning bit set is received on a designated port, its state is set to discarding to prevent loop formation. Note that the Dispute mechanism is always active regardless of the configuration setting of Loop Protection.

Loop Protect operates as a per port, per MST instance feature. It should be set on inter-switch links. It is comprised of several related functions:

- Control of port forwarding state based on reception of agreement BPDUs
- Control of port forwarding state based on reception of disputed BPDUs
- Communicating port non-forwarding status through traps and syslog messages
- Disabling a port based on frequency of failure events

Port forwarding state in the designated port is gated by a timer that is set upon BPDU reception. It is analogous to the rcvdInfoWhile timer the port uses when receiving root information in the root/alternate/backup role.

There are two operational modes for Loop Protect on a port. If the port is connected to a device known to implement Loop Protect, it uses full functional mode. Otherwise the port operates in limited functional mode.

Connection to a Loop Protect switch guarantees that the alternate agreement mechanism is implemented. This means the designated port can rely on receiving a response to its proposal regardless of the role of the connected port, which has two important implications. First, the designated port connected to a non-root port may transition to forwarding. Second, there is no ambiguity when a timeout happens; a Loop Protect event has occurred.

In full functional mode, when a type 2 BPDU is received and the port is designated and point-to-point, the timer is set to 3 times helloTime. In limited functional mode there is the additional requirement that the flags field indicate a root role. If the port is a boundary port the MSTIs for that port follow the CIST, that is, the MSTI port timers are set according to the CIST port timer. If the port is internal to the region then the MSTI port timers are set independently using the particular MSTI message.

Message age expiration and the expiration of the Loop Protect timer are both Loop Protect events. A notice level syslog message is produced for each such event. Traps may be configured to report these events as well. A syslog message and trap may be configured for disputed BPDUs.

It is also configurable to force the locking of a SID/port for the occurrence of one or more events. When the configured number of events happen within a given window of time, the port is forced into blocking and held there until it is manually unlocked via management.

## Configuring Spanning Tree Bridge Parameters

### Purpose

To display and set Spanning Tree bridge parameters, including device priorities, hello time, maximum wait time, forward delay, path cost, and topology change trap suppression.

## Commands

For information about...	Refer to page...
show spantree stats	<a href="#">9-5</a>
set spantree	<a href="#">9-7</a>
show spantree version	<a href="#">9-7</a>
set spantree version	<a href="#">9-8</a>
clear spantree version	<a href="#">9-9</a>
show spantree bpdu-forwarding	<a href="#">9-9</a>
set spantree bpdu-forwarding	<a href="#">9-10</a>
show spantree bridgeprioritymode	<a href="#">9-10</a>
set spantree bridgeprioritymode	<a href="#">9-11</a>
clear spantree bridgeprioritymode	<a href="#">9-11</a>
show spantree mstlist	<a href="#">9-12</a>
set spantree msti	<a href="#">9-12</a>
clear spantree msti	<a href="#">9-13</a>
show spantree mstmap	<a href="#">9-13</a>
set spantree mstmap	<a href="#">9-14</a>
clear spantree mstmap	<a href="#">9-14</a>
show spantree vlanlist	<a href="#">9-15</a>
show spantree mstcfgid	<a href="#">9-15</a>
set spantree mstcfgid	<a href="#">9-16</a>
clear spantree mstcfgid	<a href="#">9-16</a>
set spantree priority	<a href="#">9-17</a>
clear spantree priority	<a href="#">9-17</a>
set spantree hello	<a href="#">9-18</a>
clear spantree hello	<a href="#">9-18</a>
set spantree maxage	<a href="#">9-19</a>
clear spantree maxage	<a href="#">9-20</a>
set spantree fwddelay	<a href="#">9-20</a>
clear spantree fwddelay	<a href="#">9-21</a>
show spantree backuproot	<a href="#">9-21</a>
set spantree backuproot	<a href="#">9-22</a>
clear spantree backuproot	<a href="#">9-22</a>
show spantree tctrapsuppress	<a href="#">9-23</a>
set spantree tctrapsuppress	<a href="#">9-23</a>
clear spantree tctrapsuppress	<a href="#">9-24</a>

For information about...	Refer to page...
set spantree protomigration	<a href="#">9-24</a>
show spantree spanguard	<a href="#">9-25</a>
set spantree spanguard	<a href="#">9-25</a>
clear spantree spanguard	<a href="#">9-26</a>
show spantree spanguardtimeout	<a href="#">9-27</a>
set spantree spanguardtimeout	<a href="#">9-27</a>
clear spantree spanguardtimeout	<a href="#">9-28</a>
show spantree spanguardlock	<a href="#">9-28</a>
clear/set spantree spanguardlock	<a href="#">9-29</a>
show spantree spanguardtrapenable	<a href="#">9-29</a>
set spantree spanguardtrapenable	<a href="#">9-30</a>
clear spantree spanguardtrapenable	<a href="#">9-30</a>
show spantree legacypathcost	<a href="#">9-31</a>
set spantree legacypathcost	<a href="#">9-31</a>
clear spantree legacypathcost	<a href="#">9-32</a>
show spantree autoedge	<a href="#">9-32</a>
set spantree autoedge	<a href="#">9-32</a>
clear spantree autoedge	<a href="#">9-33</a>

## show spantree stats

Use this command to display Spanning Tree information for one or more ports.

### Syntax

```
show spantree stats [port port-string] [sid sid] [active]
```

### Parameters

<b>port</b> <i>port-string</i>	(Optional) Displays information for the specified port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>sid</b> <i>sid</i>	(Optional) Displays information for a specific Spanning Tree identifier. If not specified, SID 0 is assumed.
<b>active</b>	(Optional) Displays information for ports that have received STP BPDUs since boot.

### Defaults

If *port-string* is not specified, Spanning Tree information for all ports will be displayed.

If *sid* is not specified, information for Spanning Tree 0 will be displayed.

If **active** is not specified information for all ports will be displayed regardless of whether or not they have received BPDUs.

## Mode

Switch command, read-only.

## Example

This example shows how to display the device's Spanning Tree configuration:

```
B5(su)->show spantree stats
```

```
Spanning tree status          - enabled
Spanning tree instance       - 0
Designated Root MacAddr      - 00-e0-63-9d-c1-c8
Designated Root Priority      - 0
Designated Root Cost         - 10000
Designated Root Port         - lag.0.1
Root Max Age                  - 20 sec
Root Hello Time               - 2 sec
Root Forward Delay           - 15 sec
Bridge ID MAC Address         - 00-01-f4-da-5e-3d
Bridge ID Priority            - 32768
Bridge Max Age                - 20 sec
Bridge Hello Time            - 2 sec
Bridge Forward Delay         - 15 sec
Topology Change Count        - 7
Time Since Top Change        - 00 days 03:19:15
Max Hops                      - 20
```

[Table 9-1](#) shows a detailed explanation of command output.

**Table 9-1 show spantree Output Details**

Output	What It Displays...
Spanning tree instance	Spanning Tree ID.
Spanning tree status	Whether Spanning Tree is enabled or disabled.
Designated Root MacAddr	MAC address of the designated Spanning Tree root bridge.
Designated Root Port	Port through which the root bridge can be reached.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Root Max Age	Amount of time (in seconds) a BPDU packet should be considered valid.
Root Hello Time	Interval (in seconds) at which the root device sends BPDU (Bridge Protocol Data Unit) packets.
Root Forward Delay	Amount of time (in seconds) the root device spends in listening or learning mode.
Bridge ID MAC Address	Unique bridge MAC address, recognized by all bridges in the network.
Bridge ID Priority	Bridge priority, which is a default value, or is assigned using the <b>set spantree priority</b> command. For details, refer to " <a href="#">set spantree priority</a> " on page 9-17.
Bridge Max Age	Maximum time (in seconds) the bridge can wait without receiving a configuration message (bridge "hello") before attempting to reconfigure. This is a default value, or is assigned using the <b>set spantree maxage</b> command. For details, refer to " <a href="#">set spantree maxage</a> " on page 9-19.



**Table 9-1 show spantree Output Details (Continued)**

Output	What It Displays...
Bridge Hello Time	Amount of time (in seconds) the bridge sends BPDUs. This is a default value, or is assigned using the <b>set spantree hello</b> command. For details, refer to “ <a href="#">set spantree hello</a> ” on page 9-18.
Bridge Forward Delay	Amount of time (in seconds) the bridge spends in listening or learning mode. This is a default value, or is assigned using the <b>set spantree fwddelay</b> command. For details, refer to “ <a href="#">set spantree fwddelay</a> ” on page 9-20.
Topology Change Count	Number of times topology has changed on the bridge.
Time Since Top Change	Amount of time (in days, hours, minutes and seconds) since the last topology change.
Max Hops	Maximum number of hops information for a particular Spanning Tree instance may traverse (via relay of BPDUs within the applicable MST region) before being discarded.

## set spantree

Use this command to globally enable or disable the Spanning Tree protocol on the switch.

### Syntax

```
set spantree {disable | enable}
```

### Parameters

---

**disable | enable** Globally disables or enables Spanning Tree.

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to disable Spanning Tree on the device:

```
B5(su)->set spantree disable
```

## show spantree version

Use this command to display the current version of the Spanning Tree protocol running on the device.

### Syntax

```
show spantree version
```

### Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to display Spanning Tree version information for the device:

```
B5(su)->show spantree version
Force Version is mstp
```

# set spantree version

Use this command to set the version of the Spanning Tree protocol to MSTP (Multiple Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) or to STP 802.1D-compatible.

## Syntax

```
set spantree version {mstp | stpcompatible | rstp}
```

## Parameters

<b>mstp</b>	Sets the version to STP 802.1s-compatible.
<b>stpcompatible</b>	Sets the version to STP 802.1D-compatible.
<b>rstp</b>	Sets the version to 802.1w-compatible.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

In most networks, Spanning Tree version should not be changed from its default setting of **mstp** (Multiple Spanning Tree Protocol) mode. MSTP mode is fully compatible and interoperable with legacy STP 802.1D and Rapid Spanning Tree (RSTP) bridges. Setting the version to **stpcompatible** mode will cause the bridge to transmit only 802.1D BPDUs, and will prevent non-edge ports from rapidly transitioning to forwarding state.

## Example

This example shows how to globally change the Spanning Tree version from the default of MSTP to RSTP:

```
B5(su)->set spantree version rstp
```

## clear spantree version

Use this command to reset the Spanning Tree version to MSTP mode.

### Syntax

```
clear spantree version
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to reset the Spanning Tree version:

```
B5(su)->clear spantree version
```

## show spantree bpdu-forwarding

Use this command to display the Spanning Tree BPDU forwarding mode.

### Syntax

```
show spantree bpdu-forwarding
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the Spanning Tree BPDU forwarding mode:

```
B5(su)->show spantree bpdu-forwarding  
BPDU forwarding is disabled.
```

## set spantree bpdu-forwarding

Use this command to enable or disable Spanning Tree BPDU forwarding. By default BPDU forwarding is disabled.

### Syntax

```
set spantree bpdu-forwarding {disable | enable}
```

### Parameters

---

<b>disable</b>   <b>enable</b>	Disables or enables BPDU forwarding;.
--------------------------------	---------------------------------------

---

### Defaults

By default BPDU forwarding is disabled.

### Mode

Switch command, read-write.

### Usage

The Spanning Tree protocol must be disabled ([set spantree disable](#)) for this feature to take effect.

### Example

This example shows how to enable BPDU forwarding:

```
B5(rw)-> set spantree bpdu-forwarding enable
```

## show spantree bridgeprioritymode

Use this command to display the Spanning Tree bridge priority mode setting.

### Syntax

```
show spantree bridgeprioritymode
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the Spanning Tree bridge priority mode setting:

```
B5(rw)->show spantree bridgeprioritymode  
Bridge Priority Mode is set to IEEE802.1t mode.
```

## set spantree bridgeprioritymode

Use this command to set the Spanning Tree bridge priority mode to 802.1D (legacy) or 802.1t.

### Syntax

```
set spantree bridgeprioritymode {8021d | 8021t}
```

### Parameters

<b>8021d</b>	Sets the bridge priority mode to use 802.1D (legacy) values, which are 0 - 65535.
<b>8021t</b>	Sets the bridge priority mode to use 802.1t values, which are 0 to 61440, in increments of 4096. Values will automatically be rounded up or down, depending on the 802.1t value to which the entered value is closest.  This is the default bridge priority mode.

### Defaults

None

### Mode

Switch command, read-write.

### Usage

The mode affects the range of priority values used to determine which device is selected as the Spanning Tree root as described in **set spantree priority** ("[set spantree priority](#)" on page 9-17). The default for the switch is to use 802.1t bridge priority mode.

### Example

This example shows how to set the bridge priority mode to 802.1D:

```
B5(rw)->set spantree bridgeprioritymode 8021d
```

## clear spantree bridgeprioritymode

Use this command to reset the Spanning Tree bridge priority mode to the default setting of 802.1t.

### Syntax

```
clear spantree bridgeprioritymode
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to reset the bridge priority mode to 802.1t:

```
B5(rw)->clear spantree bridgeprioritymode
```

## show spantree mstlist

Use this command to display a list of Multiple Spanning Tree (MST) instances configured on the device.

### Syntax

```
show spantree mstlist
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display a list of MST instances. In this case, SID 2 has been configured:

```
B5(su)->show spantree mstlist
Configured Multiple Spanning Tree instances:
 2
```

## set spantree msti

Use this command to create or delete a Multiple Spanning Tree instance.

### Syntax

```
set spantree msti sid sid {create | delete}
```

### Parameters

<b>sid sid</b>	Sets the Multiple Spanning Tree ID. Valid values are <b>1 - 4094</b> . Enterasys B5 devices will support up to 4 MST instances.
<b>create   delete</b>	Creates or deletes an MST instance.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to create an MST instance 2:

```
B5(su)->set spantree msti sid 2 create
```

## clear spantree msti

Use this command to delete one or more Multiple Spanning Tree instances.

### Syntax

```
clear spantree msti [sid sid]
```

### Parameters

---

<i>sid sid</i>	(Optional) Deletes a specific multiple Spanning Tree ID.
----------------	--

---

### Defaults

If *sid* is not specified, all MST instances will be cleared.

### Mode

Switch command, read-write.

### Example

This example shows how to delete all MST instances:

```
B5(su)->clear spantree msti
```

## show spantree mstmap

Use this command to display the mapping of a filtering database ID (FID) to a Spanning Trees. Since VLANs are mapped to FIDs, this shows to which SID a VLAN is mapped.

### Syntax

```
show spantree mstmap [fid fid]
```

### Parameters

---

<i>fid fid</i>	(Optional) Displays information for specific FIDs.
----------------	--

---

### Defaults

If *fid* is not specified, information for all assigned FIDs will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display SID to FID mapping information for FID 1. In this case, no new mappings have been configured:

```
B5(su)->show spantree mstmap fid 1
```

FID:	SID:
1	0

## set spantree mstmap

Use this command to map one or more filtering database IDs (FIDs) to a SID. Since VLANs are mapped to FIDs, this essentially maps one or more VLAN IDs to a Spanning Tree (SID).



**Note:** Since any MST maps that are associated with GVRP-generated VLANs will be removed from the configuration if GVRP communication is lost, it is recommended that you only create MST maps on statically-created VLANs.

### Syntax

```
set spantree mstmap fid [sid sid]
```

### Parameters

<i>fid</i>	Specifies one or more FIDs to assign to the MST. Valid values are 1 - 4093, and must correspond to a VLAN ID created using the <b>set vlan</b> command.
<i>sid sid</i>	(Optional) Specifies a Multiple Spanning Tree ID. Valid values are 1 - 4094, and must correspond to a SID created using the <b>set msti</b> command.

### Defaults

If *sid* is not specified, FID(s) will be mapped to Spanning Tree 0.

### Mode

Switch command, read-write.

### Example

This example shows how to map FID 3 to SID 2:

```
B5(su)->set spantree mstmap 3 sid 2
```

## clear spantree mstmap

Use this command to map a FID back to SID 0.

### Syntax

```
clear spantree mstmap fid
```

### Parameters

<i>fid</i>	Specifies one or more FIDs to reset to 0.
------------	---

### Defaults

If *fid* is not specified, all SID to FID mappings will be reset.

### Mode

Switch command, read-write.



## Example

This example shows how to map FID 2 back to SID 0:

```
B5(su)->clear spantree mstmap 2
```

## show spantree vlanlist

Use this command to display the Spanning Tree ID(s) assigned to one or more VLANs.

### Syntax

```
show spantree vlanlist [vlan-list]
```

### Parameters

---

<i>vlan-list</i>	(Optional) Displays SIDs assigned to specific VLAN(s).
------------------	--

---

### Defaults

If not specified, SID assignment will be displayed for all VLANs.

### Mode

Switch command, read-only.

### Example

This example shows how to display the SIDs mapped to VLAN 1. In this case, SIDs 2, 16 and 42 are mapped to VLAN 1. For this information to display, the SID instance must be created using the **set spantree msti** command as described in “[set spantree msti](#)” on page 9-12, and the FIDs must be mapped to SID 1 using the **set spantree mstmap** command as described in “[set spantree mstmap](#)” on page 9-14:

```
B5(su)->show spantree vlanlist 1
The following SIDS are assigned to VLAN 1: 2 16 42
```

## show spantree mstcfgid

Use this command to display the MST configuration identifier elements, including format selector, configuration name, revision level, and configuration digest.

### Syntax

```
show spantree mstcfgid
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

## Example

This example shows how to display the MST configuration identifier elements. In this case, the default revision level of 0, and the default configuration name (a string representing the bridge MAC address) have not been changed. For information on using the **set spantree mstcfgid** command to change these settings, refer to “[set spantree mstcfgid](#)” on page 9-16:

```
B5(su)->show spantree mstcfgid
MST Configuration Identifier:
Format Selector: 0
Configuration Name: 00:01:f4:89:51:94
Revision Level: 0
Configuration Digest: ac:36:17:7f:50:28:3c:d4:b8:38:21:d8:ab:26:de:62
```

## set spantree mstcfgid

Use this command to set the MST configuration name and/or revision level.

### Syntax

```
set spantree mstcfgid {cfgname name | rev level}
```

### Parameters

<b>cfgname</b> <i>name</i>	Specifies an MST configuration name.
<b>rev</b> <i>level</i>	Specifies an MST revision level. Valid values are 0 - 65535.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the MST configuration name to “mstconfig”:

```
B5(su)->set spantree mstconfigid cfgname mstconfig
```

## clear spantree mstcfgid

Use this command to reset the MST revision level to a default value of 0, and the configuration name to a default string representing the bridge MAC address.

### Syntax

```
clear spantree mstcfgid
```

### Parameters

None.

### Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the MST configuration identifier elements to default values:

```
B5(su)->clear spantree mstcfgid
```

# set spantree priority

Use this command to set the device's Spanning Tree priority.

## Syntax

```
set spantree priority priority [sid]
```

## Parameters

<i>priority</i>	Specifies the priority of the bridge. Valid values are from <b>0</b> to <b>61440</b> (in increments of 4096), with 0 indicating highest priority and 61440 lowest priority.
<i>sid</i>	(Optional) Sets the priority on a specific Spanning Tree. Valid values are <b>0</b> - <b>4094</b> . If not specified, SID 0 is assumed.

## Defaults

If *sid* is not specified, priority will be set on Spanning Tree 0.

## Mode

Switch command, read-write.

## Usage

The device with the highest priority (lowest numerical value) becomes the Spanning Tree root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device. Depending on the bridge priority mode (set with the **set spantree bridgeprioritymode** command described in "[set spantree bridgeprioritymode](#)" on page 9-11, some priority values may be rounded up or down.

## Example

This example shows how to set the bridge priority to 4096 on SID 1:

```
B5(su)->set spantree priority 4096 1
```

# clear spantree priority

Use this command to reset the Spanning Tree priority to the default value of 32768.

## Syntax

```
clear spantree priority [sid]
```

## Parameters

---

<i>sid</i>	(Optional) Resets the priority on a specific Spanning Tree. Valid values are <b>0 - 4094</b> . If not specified, SID 0 is assumed.
------------	--

---

## Defaults

If *sid* is not specified, priority will be reset on Spanning Tree 0.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the bridge priority on SID 1:

```
B5(su)->clear spantree priority 1
```

# set spantree hello

Use this command to set the device's Spanning Tree hello time. This is the time interval (in seconds) the device will transmit BPDUs indicating it is active.

## Syntax

```
set spantree hello interval
```

## Parameters

---

<i>interval</i>	Specifies the number of seconds the system waits before broadcasting a bridge hello message (a multicast message indicating that the system is active). Valid values are <b>1 - 10</b> .
-----------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to globally set the Spanning Tree hello time to 10 seconds:

```
B5(su)->set spantree hello 10
```

# clear spantree hello

Use this command to reset the Spanning Tree hello time to the default value of 2 seconds.

## Syntax

```
clear spantree hello
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to globally reset the Spanning Tree hello time:

```
B5(su)->clear spantree hello
```

# set spantree maxage

Use this command to set the bridge maximum aging time.

## Syntax

```
set spantree maxage agingtime
```

## Parameters

<i>agingtime</i>	Specifies the maximum number of seconds that the system retains the information received from other bridges through STP. Valid values are 6 - 40.
------------------	---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The bridge maximum aging time is the maximum time (in seconds) a device can wait without receiving a configuration message (bridge "hello") before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information provided in the last configuration message becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

## Example

This example shows how to set the maximum aging time to 25 seconds:

```
B5(su)->set spantree maxage 25
```

## clear spantree maxage

Use this command to reset the maximum aging time for a Spanning Tree to the default value of 20 seconds.

### Syntax

```
clear spantree maxage
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to globally reset the maximum aging time:

```
B5(su)->clear spantree maxage
```

## set spantree fwddelay

Use this command to set the Spanning Tree forward delay.

### Syntax

```
set spantree fwddelay delay
```

### Parameters

---

<i>delay</i>	Specifies the number of seconds for the bridge forward delay. Valid values are 4 - 30.
--------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The forward delay is the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.

### Example

This example shows how to globally set the bridge forward delay to 16 seconds:

```
B5(su)->set spantree fwddelay 16
```

## clear spantree fwddelay

Use this command to reset the Spanning Tree forward delay to the default setting of 15 seconds.

### Syntax

```
clear spantree fwddelay
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to globally reset the bridge forward delay:

```
B5(su)->clear spantree fwddelay
```

## show spantree backuproot

Use this command to display the backup root status for an MST instance.

### Syntax

```
show spantree backuproot [sid]
```

### Parameters

---

<i>sid</i>	(Optional) Display backup root status for a specific Spanning Tree identifier. Valid values are 0 - 4094. If not specified, SID 0 is assumed.
------------	---

---

### Defaults

If a SID is not specified, then status will be shown for Spanning Tree instance 0.

### Mode

Switch command, read-only.

### Example

This example shows how to display the status of the backup root function on SID 0:

```
B5(rw)->show spantree backuproot  
Backup root is set to disable on sid 0
```

## set spantree backuproot

Use this command to enable or disable the Spanning Tree backup root function on the switch.

### Syntax

```
set spantree backuproot sid {disable | enable}
```

### Parameters

---

<i>sid</i>	Specifies the Spanning Tree instance on which to enable or disable the backup root function. Valid values are <b>0 - 4094</b> .
disable   enable	Enables or disables the backup root function.

---

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The Spanning Tree backup root function is disabled by default on the Enterasys B5. When this feature is enabled and the switch is directly connected to the root bridge, stale Spanning Tree information is prevented from circulating if the root bridge is lost. If the root bridge is lost, the backup root will dynamically lower its bridge priority so that it will be selected as the new root over the lost root bridge.

### Example

This example shows how to enable the backup root function on SID 2:

```
B5(rw)->set spantree backuproot 2 enable
```

## clear spantree backuproot

Use this command to reset the Spanning Tree backup root function to the default state of disabled.

### Syntax

```
clear spantree backuproot sid
```

### Parameters

---

<i>sid</i>	Specifies the Spanning Tree on which to clear the backup root function. Valid values are <b>0 - 4094</b> .
------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.



## Example

This example shows how to reset the backup root function to disabled on SID 2:

```
B5(rw)->clear spantree backuproot 2
```

## show spantree tctrapsuppress

Use this command to display the status of topology change trap suppression on Rapid Spanning Tree edge ports.

### Syntax

```
show spantree tctrapsuppress
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

## Example

This example shows how to display the status of topology change trap suppression:

```
B5(rw)->show spantree tctrapsuppress
```

```
Topology change Trap Suppression is set to enabled
```

## set spantree tctrapsuppress

Use this command to disable or enable topology change trap suppression on Rapid Spanning Tree edge ports.

### Syntax

```
set spantree tctrapsuppress {disable | enable}
```

### Parameters

---

<b>disable   enable</b>	Disables or enables topology change trap suppression.
-------------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

## Usage

By default, RSTP non-edge (bridge) ports that transition to forwarding or blocking cause the switch to issue a topology change trap. When topology change trap suppression is enabled, which is the device default, edge ports (such as end station PCs) are prevented from sending topology change traps. This is because there is usually no need for network management to monitor edge port STP transition states, such as when PCs are powered on. When topology change trap suppression is disabled, all ports, including edge and bridge ports, will transmit topology change traps.

## Example

This example shows how to allow Rapid Spanning Tree edge ports to transmit topology change traps:

```
B5(rw)->set spantree tctrapsuppress disable
```

## clear spantree tctrapsuppress

Use this command to clear the status of topology change trap suppression on Rapid Spanning Tree edge ports to the default state of enabled (edge port topology changes do not generate traps).

### Syntax

```
clear spantree tctrapsuppress
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear topology change trap suppression setting:

```
B5(rw)->clear spantree tctrapsuppress
```

## set spantree protomigration

Use this command to reset the protocol state migration machine for one or more Spanning Tree ports. When operating in RSTP mode, this forces a port to transmit MSTP BPDUs.

### Syntax

```
set spantree protomigration <port-string>
```

### Parameters

---

<i>port-string</i>	Reset the protocol state migration machine for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the protocol state migration machine on port 20:

```
B5(su)->set spantree protomigration ge.1.20
```

# show spantree spanguard

Use this command to display the status of the Spanning Tree SpanGuard function.

## Syntax

```
show spantree spanguard
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to display the SpanGuard function status:

```
B5(su)->show spantree spanguard  
Spanguard is disabled
```

# set spantree spanguard

Use this command to enable or disable the Spanning Tree SpanGuard function.

## Syntax

```
set spantree spanguard {enable | disable}
```

## Parameters

---

<b>enable   disable</b>	Enables or disables the SpanGuard function.
-------------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

SpanGuard is designed to disable, or lock out an “edge” port when an unexpected BPDU is received. The port can be configured to be re-enabled after a set time period, or only after manual intervention.

A port can be defined as an edge (user) port using the **set spantree adminedge** command, described in “[set spantree adminedge](#)” on page 9-40. A port designated as an edge port is expected to be connected to a workstation or other end-user type of device, and not to another switch in the network. When SpanGuard is enabled, if a non-loopback BPDU is received on an edge port, the Spanning Tree state of that port will be changed to “blocking” and will no longer forward traffic. The port will remain disabled until the amount of time defined by **set spantree spanguardtimeout** (“[set spantree spanguardtimeout](#)” on page 9-27) has passed since the last seen BPDU, the port is manually unlocked (**set** or **clear spantree spanguardlock**, “[clear / set spantree spanguardlock](#)” on page 9-29), the configuration of the port is changed so it is not longer an edge port, or the SpanGuard function is disabled.

SpanGuard is enabled and disabled only on a global basis (across the stack, if applicable). By default, SpanGuard is disabled and SpanGuard traps are enabled.

## Example

This example shows how to enable the SpanGuard function:

```
B5(rw)->set spantree spanguard enable
```

# clear spantree spanguard

Use this command to reset the status of the Spanning Tree SpanGuard function to disabled.

## Syntax

```
clear spantree spanguard
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the status of the SpanGuard function to disabled:

```
B5(rw)->clear spantree spanguard
```

## show spantree spanguardtimeout

Use this command to display the Spanning Tree SpanGuard timeout setting.

### Syntax

```
show spantree spanguardtimeout
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the SpanGuard timeout setting:

```
B5(su)->show spantree spanguardtimeout
Spanguard timeout: 300
```

## set spantree spanguardtimeout

Use this command to set the amount of time (in seconds) an edge port will remain locked by the SpanGuard function.

### Syntax

```
set spantree spanguardtimeout timeout
```

### Parameters

---

<i>timeout</i>	Specifies a timeout value in seconds. Valid values are <b>0</b> to <b>65535</b> . A value of 0 will keep the port locked until manually unlocked. The default value is 300 seconds.
----------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the SpanGuard timeout to 600 seconds:

```
B5(su)->set spantree spanguardtimeout 600
```

## clear spantree spanguardtimeout

Use this command to reset the Spanning Tree SpanGuard timeout to the default value of 300 seconds.

### Syntax

```
clear spantree spanguardtimeout
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to reset the SpanGuard timeout to 300 seconds:

```
B5(rw)->clear spantree spanguardtimeout
```

## show spantree spanguardlock

Use this command to display the SpanGuard lock status of one or more ports.

### Syntax

```
show spantree spanguardlock [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Specifies the port(s) for which to show SpanGuard lock status. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

---

### Defaults

If no port string is specified, the SpanGuard lock status for all ports is displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display the SpanGuard lock status for ge.1.1:

```
B5(su)->show spantree spanguardlock ge.1.1  
Port ge.1.1 is Unlocked
```

## clear / set spantree spanguardlock

Use either of these commands to unlock one or more ports locked by the Spanning Tree SpanGuard function. When SpanGuard is enabled, it locks ports that receive BPDUs when those ports have been defined as edge (user) ports (as described in “[set spantree admingedge](#)” on page 9-40).

### Syntax

```
clear spantree spanguardlock port-string
set spantree spanguardlock port-string
```

### Parameters

<i>port-string</i>	Specifies port(s) to unlock. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
--------------------	---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to unlock port ge.1.16:

```
B5(rw)->clear spantree spanguardlock ge.1.16
```

## show spantree spanguardtrapenable

Use this command to display the state of the Spanning Tree SpanGuard trap function.

### Syntax

```
show spantree spanguardtrapenable
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the state of the SpanGuard trap function:

```
B5(ro)->show spantree spanguardtrapenable
Spanguard SNMP traps are enabled
```

## set spantree spanguardtrapenable

Use this command to enable or disable the sending of an SNMP trap message when SpanGuard has locked a port.

### Syntax

```
set spantree spanguardtrapenable {disable | enable}
```

### Parameters

---

<b>disable   enable</b>	Disables or enables sending SpanGuard traps. By default, sending traps is enabled.
-------------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to disable the SpanGuard trap function:

```
B5(su)->set spantree spanguardtrapenable disable
```

## clear spantree spanguardtrapenable

Use this command to reset the Spanning Tree SpanGuard trap function back to the default state of enabled.

### Syntax

```
clear spantree spanguardtrapenable
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to reset the SpanGuard trap function to enabled:

```
B5(rw)->clear spantree spanguardtrapenable
```



## show spantree legacypathcost

Use this command to display the default Spanning Tree path cost setting.

### Syntax

```
show spantree legacypathcost
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the default Spanning Tree path cost setting.

```
B5(su)->show spantree legacypathcost
Legacy Path Cost is disabled.
```

## set spantree legacypathcost

Use this command to enable or disable legacy (802.1D) path cost values.

### Syntax

```
set spantree legacypathcost {disable | enable}
```

### Parameters

<b>disable</b>	Use 802.1t2001 values to calculate path cost.
<b>enable</b>	Use 802.1d1998 values to calculate path cost.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

By default, legacy path cost is disabled. Enabling the device to calculate legacy path costs affects the range of valid values that can be entered in the **set spantree adminpathcost** command.

### Example

This example shows how to set the default path cost values to 802.1D.

```
B5(rw)->set spantree legacypathcost enable
```

## clear spantree legacypathcost

Use this command to set the Spanning Tree default value for legacy path cost to 802.1t values.

### Syntax

```
clear spantree legacypathcost
```

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example clears the legacy path cost to 802.1t values.

```
B5(rw)->clear spantree legacypathcost
```

## show spantree autoedge

Use this command to display the status of automatic edge port detection.

### Syntax

```
show spantree autoedge
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the status of the automatic edge port detection function:

```
B5(rw)->show spantree autoedge  
autoEdge is currently enabled.
```

## set spantree autoedge

Use this command to enable or disable the automatic edge port detection function.

### Syntax

```
set spantree autoedge {disable | enable}
```

---

## Parameters

---

<b>disable</b>   <b>enable</b>	Disables or enables automatic edge port detection.
--------------------------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to disable automatic edge port detection:

```
B5(rw)->set spantree autoedge disable
```

# clear spantree autoedge

Use this command to reset automatic edge port detection to the default state of enabled.

## Syntax

```
clear spantree autoedge
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, Read-Write.

## Example

This example shows how to reset automatic edge port detection to enabled:

```
B5(rw)->clear spantree autoedge
```

# Configuring Spanning Tree Port Parameters

## Purpose

To display and set Spanning Tree port parameters.

## Commands

For information about...	Refer to page...
set spantree portadmin	<a href="#">9-34</a>
clear spantree portadmin	<a href="#">9-35</a>
show spantree portadmin	<a href="#">9-35</a>
show spantree portpri	<a href="#">9-36</a>
set spantree portpri	<a href="#">9-36</a>
clear spantree portpri	<a href="#">9-37</a>
show spantree adminpathcost	<a href="#">9-38</a>
set spantree adminpathcost	<a href="#">9-38</a>
clear spantree adminpathcost	<a href="#">9-39</a>
show spantree admiedge	<a href="#">9-39</a>
set spantree admiedge	<a href="#">9-39</a>
clear spantree admiedge	<a href="#">9-40</a>
show spantree operedge	<a href="#">9-41</a>

## set spantree portadmin

Use this command to disable or enable the Spanning Tree algorithm on one or more ports.

### Syntax

```
set spantree portadmin port-string {disable | enable}
```

### Parameters

<i>port-string</i>	Specifies the port(s) for which to enable or disable Spanning Tree. For a detailed description of possible <i>port-string</i> values, refer to " <a href="#">Port String Syntax Used in the CLI</a> " on page 7-1.
<b>disable   enable</b>	Disables or enables Spanning Tree.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to disable Spanning Tree on ge.1.5:

```
B5(rw)->set spantree portadmin ge.1.5 disable
```

## clear spantree portadmin

Use this command to reset the default Spanning Tree admin status to enable on one or more ports.

### Syntax

```
clear spantree portadmin port-string
```

### Parameters

<i>port-string</i>	Resets the default admin status on specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to reset the default Spanning Tree admin state to enable on ge.1.12:

```
B5(rw)->clear spantree portadmin ge.1.12
```

## show spantree portadmin

Use this command to display the status of the Spanning Tree algorithm on one or more ports.

### Syntax

```
show spantree portadmin [port port-string]
```

### Parameters

<b>port</b> <i>port-string</i>	(Optional) Displays status for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------------------	---

### Defaults

If *port-string* is not specified, status will be displayed for all ports.

### Mode

Switch command, read-only.

## Example

This example shows how to display port admin status for ge.1.1:

```
B5(ro)->show spantree portadmin port ge.1.1
Port ge.1.1 has portadmin set to enabled
```

## show spantree portpri

Use this command to show the Spanning Tree priority for one or more ports. Port priority is a component of the port ID, which is one element used in determining Spanning Tree port roles.

### Syntax

```
show spantree portpri [port port-string] [sid sid]
```

### Parameters

<b>port</b> <i>port-string</i>	(Optional) Specifies the port(s) for which to display Spanning Tree priority. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
<b>sid</b> <i>sid</i>	(Optional) Displays port priority for a specific Spanning Tree identifier. Valid values are 0 - 4094. If not specified, SID 0 is assumed.

### Defaults

If *port-string* is not specified, port priority will be displayed for all Spanning Tree ports.

If *sid* is not specified, port priority will be displayed for Spanning Tree 0.

### Mode

Switch command, read-only.

### Example

This example shows how to display the port priority for ge.2.7:

```
B5(su)->show spantree portpri port ge.2.7
Port ge.2.7 has a Port Priority of 128 on SID 0
```

## set spantree portpri

Use this command to set a port’s Spanning Tree priority.

### Syntax

```
set spantree portpri port-string priority [sid sid]
```

## Parameters

<i>port-string</i>	Specifies the port(s) for which to set Spanning Tree port priority. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
<i>priority</i>	Specifies a number that represents the priority of a link in a Spanning Tree bridge. Valid values are from <b>0 to 240 (in increments of 16)</b> with 0 indicating high priority.
<b>sid</b> <i>sid</i>	(Optional) Sets port priority for a specific Spanning Tree identifier. Valid values are <b>0 - 4094</b> . If not specified, SID 0 is assumed.

## Defaults

If *sid* is not specified, port priority will be set for Spanning Tree 0.

## Mode

Switch command, read-write.

## Example

This example shows how to set the priority of ge.1.3 to 240 on SID 1

```
B5(su)->set spantree portpri ge.1.3 240 sid 1
```

# clear spantree portpri

Use this command to reset the bridge priority of a Spanning Tree port to a default value of 128.

## Syntax

```
clear spantree portpri port-string [sid sid]
```

## Parameters

<i>port-string</i>	Specifies the port(s) for which to set Spanning Tree port priority. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
<b>sid</b> <i>sid</i>	(Optional) Resets the port priority for a specific Spanning Tree identifier. Valid values are <b>0 - 4094</b> . If not specified, SID 0 will be assumed.

## Defaults

If *sid* is not specified, port priority will be set for Spanning Tree 0.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the priority of ge.1.3 to 128 on SID 1

```
B5(su)->clear spantree portpri ge.1.3 sid 1
```

## show spantree adminpathcost

Use this command to display the admin path cost for a port on one or more Spanning Trees.

### Syntax

```
show spantree adminpathcost [port port-string] [sid sid]
```

### Parameters

<b>port</b> <i>port-string</i>	(Optional) Displays the admin path cost value for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>sid</b> <i>sid</i>	(Optional) Displays the admin path cost for a specific Spanning Tree identifier. Valid values are 0 - 4094. If not specified, SID 0 will be assumed.

### Defaults

If *port-string* is not specified, admin path cost for all Spanning Tree ports will be displayed.

If *sid* is not specified, admin path cost for Spanning Tree 0 will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display the admin path cost for ge.3.4 on SID 1:

```
B5(su)->show spantree adminpathcost port ge.3.4 sid 1
Port ge.3.4 has a Port Admin Path Cost of 0 on SID 1
```

## set spantree adminpathcost

Use this command to set the administrative path cost on a port and one or more Spanning Trees.

### Syntax

```
set spantree adminpathcost port-string cost [sid sid]
```

### Parameters

<i>port-string</i>	Specifies the port(s) on which to set an admin path cost. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<i>cost</i>	Specifies the port path cost. Valid values are 0 - 20000000.
<b>sid</b> <i>sid</i>	(Optional) Sets the admin path cost for a specific Spanning Tree identifier. Valid values are 0 - 4094. If not specified, SID 0 will be assumed.

### Defaults

If *sid* is not specified, admin path cost will be set for Spanning Tree 0.

### Mode

Switch command, read-write.



## Example

This example shows how to set the admin path cost to 200 for ge.3.2 on SID 1:

```
B5(su)->set spantree adminpathcost ge.3.2 200 sid 1
```

## clear spantree adminpathcost

Use this command to reset the Spanning Tree default value for port admin path cost to 0.

### Syntax

```
clear spantree adminpathcost port-string [sid sid]
```

### Parameters

<i>port-string</i>	Specifies the port(s) for which to reset admin path cost. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<i>sid sid</i>	(Optional) Resets the admin path cost for specific Spanning Tree(s). Valid values are 0 - 4094. If not specified, SID 0 is assumed.

### Defaults

If *sid* is not specified, admin path cost will be reset for Spanning Tree 0.

### Mode

Switch command, read-write.

### Example

This example shows how to reset the admin path cost to 0 for ge.3.2 on SID 1:

```
B5(su)->clear spantree adminpathcost ge.3.2 sid 1
```

## show spantree adminedge

Use this command to display the edge port administrative status for a port.

### Syntax

```
show spantree adminedge [port port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays edge port administrative status for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

### Defaults

If *port-string* is not specified edge port administrative status will be displayed for all Spanning Tree ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display the edge port status for ge.3.2:

```
B5(su)->show spantree adminedge port ge.3.2
Port ge.3.2 has a Port Admin Edge of Edge-Port
```

# set spantree adminedge

Use this command to set the edge port administrative status on a Spanning Tree port.

## Syntax

```
set spantree adminedge port-string {true | false}
```

## Parameters

<i>port-string</i>	Specifies the edge port. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
true   false	Enables ( <b>true</b> ) or disables ( <b>false</b> ) the specified port as a Spanning Tree edge port.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The default behavior of the edge port administrative status begins with the value set to **false** initially after the device is powered up. If a Spanning Tree BPDU is not received on the port within a few seconds, the status setting changes to **true**.

## Example

This example shows how to set ge.1.11 as an edge port:

```
B5(su)->set spantree adminedge ge.1.11 true
```

# clear spantree adminedge

Use this command to reset a Spanning Tree port to non-edge status.

## Syntax

```
clear spantree adminedge port-string
```

## Parameters

---

<i>port-string</i>	Specifies port(s) on which to reset edge port status. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset ge.1.11 as a non-edge port:

```
B5(su)->clear spantree adminedge ge.1.11
```

# show spantree operedge

Use this command to display the Spanning Tree edge port operating status for a port.

## Syntax

```
show spantree operedge [port port-string]
```

## Parameters

---

<b>port</b> <i>port-string</i>	Displays edge port operating status for specific port(s).
--------------------------------	---

---

## Defaults

If *port-string* is not specified, edge port operating status will be displayed for all Spanning Tree ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display the edge port status for ge.2.7:

```
B5(rw)->show spantree operedge port ge.2.7
Port ge.2.7 has a Port Oper Edge of Edge-Port
```

# Configuring Spanning Tree Loop Protect Parameters

## Purpose

To display and set Spanning Tree Loop Protect parameters, including the global parameters of Loop Protect threshold, window, enabling traps, and disputed BPDU threshold, as well as per port and port/SID parameters. See “[Loop Protect](#)” on page 9-2 for more information about the Loop Protect feature.

## Commands

For information about...	Refer to page...
set spantree lp	<a href="#">9-43</a>
show spantree lp	<a href="#">9-43</a>
clear spantree lp	<a href="#">9-44</a>
show spantree lpblood	<a href="#">9-44</a>
clear spantree lpblood	<a href="#">9-45</a>
set spantree lpcapablepartner	<a href="#">9-46</a>
show spantree lpcapablepartner	<a href="#">9-46</a>
clear spantree lpcapablepartner	<a href="#">9-47</a>
set spantree lpthreshold	<a href="#">9-47</a>
show spantree lpthreshold	<a href="#">9-48</a>
clear spantree lpthreshold	<a href="#">9-48</a>
set spantree lpwindow	<a href="#">9-49</a>
show spantree lpwindow	<a href="#">9-49</a>
clear spantree lpwindow	<a href="#">9-50</a>
set spantree lptrapenable	<a href="#">9-50</a>
show spantree lptrapenable	<a href="#">9-51</a>
clear spantree lptrapenable	<a href="#">9-51</a>
set spantree disputedbpduthreshold	<a href="#">9-52</a>
show spantree disputedbpduthreshold	<a href="#">9-53</a>
clear spantree disputedbpduthreshold	<a href="#">9-53</a>
show spantree nonforwardingreason	<a href="#">9-54</a>

## set spantree lp

Use this command to enable or disable the Loop Protect feature per port and optionally, per SID. The Loop Protect feature is disabled by default. See “Loop Protect” on page 2. for more information.

### Syntax

```
set spantree lp port-string {enable | disable} [sid sid]
```

### Parameters

<i>port-string</i>	Specifies port(s) on which to enable or disable the Loop Protect feature.
<b>enable</b>   <b>disable</b>	Enables or disables the feature on the specified port.
<b>sid</b> <i>sid</i>	(Optional) Enables or disables the feature for specific Spanning Tree(s). Valid values are 0 - 4094. If not specified, SID 0 is assumed.

### Defaults

If no SID is specified, SID 0 is assumed.

### Mode

Switch command, read-write.

### Usage

Loop Protect takes precedence over per port STP enable/disable (portAdmin). Normally portAdmin disabled would cause a port to go immediately to forwarding. If Loop Protect is enabled, that port should go to listening and remain there.



**Note:** The Loop Protect enable/disable settings for an MSTI port should match those for the CIST port.

### Example

This example shows how to enable Loop Protect on ge.2.3:

```
B5(su)->set spantree lp ge.1.11 enable
```

## show spantree lp

Use this command to display the Loop Protect status per port and/or per SID.

### Syntax

```
show spantree lp [port port-string] [sid sid]
```

### Parameters

<i>port-string</i>	(Optional) Specifies port(s) for which to display the Loop Protect feature status.
<b>sid</b> <i>sid</i>	(Optional) Specifies the specific Spanning Tree(s) for which to display the Loop Protect feature status. Valid values are 0 - 4094. If not specified, SID 0 is assumed.

## Defaults

If no *port-string* is specified, status is displayed for all ports.

If no SID is specified, SID 0 is assumed.

## Mode

Switch command, read-only.

## Example

This example shows how to display Loop Protect status on ge.2.3:

```
B5(su)->show spantree lp port ge.2.3
LoopProtect is disabled on port ge.2.3      , SI
```

# clear spantree lp

Use this command to return the Loop Protect status per port and optionally, per SID, to its default state of disabled.

## Syntax

```
clear spantree lp port-string [sid sid]
```

## Parameters

<i>port-string</i>	Specifies port(s) for which to clear the Loop Protect feature status.
<i>sid sid</i>	(Optional) Specifies the specific Spanning Tree(s) for which to clear the Loop Protect feature status. Valid values are 0 - 4094. If not specified, SID 0 is assumed.

## Defaults

If no SID is specified, SID 0 is assumed.

## Mode

Switch command, read-write.

## Example

This example shows how to return the Loop Protect state on ge.2.3 to disabled:

```
B5(rw)->clear spantree lp port ge.2.3
```

# show spantree lpllock

Use this command to display the Loop Protect lock status per port and/or per SID. A port can become locked if a configured number of Loop Protect events occur during the configured window of time. See the [set spantree lpthreshold](#) and [set spantree lpwindow](#) commands. Once a port is forced into blocking (locked), it remains locked until manually unlocked with the [clear spantree lpllock](#) command.

## Syntax

```
show spantree lpllock [port port-string] [sid sid]
```

## Parameters

<i>port-string</i>	(Optional) Specifies port(s) for which to display the Loop Protect lock status.
<b>sid</b> <i>sid</i>	(Optional) Specifies the specific Spanning Tree(s) for which to display the Loop Protect lock status. Valid values are <b>0 - 4094</b> . If not specified, SID 0 is assumed.

## Defaults

If no *port-string* is specified, status is displayed for all ports.

If no SID is specified, SID 0 is assumed.

## Mode

Switch command, read-only.

## Example

This example shows how to display Loop Protect lock status on ge.1.1:

```
B5(rw)->show spantree lprotect port ge.1.1
The LoopProtect lock status for port ge.1.1      , SID 0 is UNLOCKED
```

# clear spantree lprotect

Use this command to manually unlock a blocked port and optionally, per SID. The default state is unlocked.

## Syntax

```
clear spantree lprotect port-string [sid sid]
```

## Parameters

<i>port-string</i>	Specifies port(s) for which to clear the Loop Protect lock.
<b>sid</b> <i>sid</i>	(Optional) Specifies the specific Spanning Tree(s) for which to clear the Loop Protect lock. Valid values are <b>0 - 4094</b> . If not specified, SID 0 is assumed.

## Defaults

If no SID is specified, SID 0 is assumed.

## Mode

Switch command, read-only.

## Example

This example shows how to clear Loop Protect lock from ge.1.1:

```
B5(rw)->show spantree lprotect port ge.1.1
The LoopProtect lock status for port ge.1.1      , SID 0 is LOCKED
B5(rw)->clear spantree lprotect ge.1.1
B5(rw)->show spantree lprotect port ge.1.1
The LoopProtect lock status for port ge.1.1      , SID 0 is UNLOCKED
```

## set spantree lpcapablepartner

Use this command to specify per port whether the link partner is Loop Protect capable. See “Loop Protect” on page 2. for more information.

### Syntax

```
set spantree lpcapablepartner port-string {true | false}
```

### Parameters

<i>port-string</i>	Specifies port(s) for which to configure a Loop Protect capable link partner.
<b>true   false</b>	Specifies whether the link partner is capable (true) or not (false).

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The default value for Loop Protect capable partner is false. If the port is configured with a Loop Protect capable partner (true), then the full functionality of the Loop Protect feature is used. If the value is false, then there is some ambiguity as to whether an Active Partner timeout is due to a loop protection event or is a normal situation due to the fact that the partner port does not transmit Alternate Agreement BPDUs. Therefore, a conservative approach is taken in that designated ports will not be allowed to forward unless receiving agreements from a port with root role.

This type of timeout will not be considered a loop protection event. Loop protection is maintained by keeping the port from forwarding but since this is not considered a loop event it will not be factored into locking the port.

### Example

This example shows how to set the Loop Protect capable partner to true for ge.1.1:

```
B5(rw)->set spantree lpcapablepartner ge.1.1 true
```

## show spantree lpcapablepartner

Use this command to the Loop Protect capability of a link partner for one or more ports.

### Syntax

```
show spantree lpcapablepartner [port port-string]
```

### Parameters

<i>port-string</i>	(Optional) Specifies port(s) for which to display Loop Protect capability for its link partner.
--------------------	---



## Defaults

If no *port-string* is specified, Loop Protect capability for link partners is displayed for all ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display the Loop Protect partner capability for ge.1.1:

```
B5(rw)->show spantree lpcapablepartner port ge.1.1
Link partner of port ge.1.1 is not LoopProtect-capable
```

# clear spantree lpcapablepartner

Use this command to reset the Loop Protect capability of port link partners to the default state of false.

## Syntax

```
clear spantree lpcapablepartner port-string
```

## Parameters

<i>port-string</i>	Specifies port(s) for which to clear their link partners' Loop Protect capability (reset to false).
--------------------	---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the Loop Protect partner capability for ge.1.1:

```
B5(rw)->clear spantree lpcapablepartner ge.1.1
```

# set spantree lpthreshold

Use this command to set the Loop Protect event threshold.

## Syntax

```
set spantree lpthreshold value
```

## Parameters

<i>value</i>	Specifies the number of events that must occur during the event window in order to lock a port/SID. The default value is 3 events. A threshold of 0 specifies that ports will never be locked.
--------------	--

## Defaults

None. The default event threshold is 3.

## Mode

Switch command, read-write.

## Usage

The LoopProtect event threshold is a global integer variable that provides protection in the case of intermittent failures. The default value is 3. If the event counter reaches the threshold within a given period (the event window), then the port, for the given SID, becomes locked (that is, held indefinitely in the blocking state). If the threshold is 0, the ports are never locked.

## Example

This example shows how to set the Loop Protect threshold value to 4:

```
B5(rw)->set spantree lpthreshold 4
```

# show spantree lpthreshold

Use this command to display the current value of the Loop Protect event threshold.

## Syntax

```
show spantree lpthreshold
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to display the current Loop Protect threshold value:

```
B5(rw)->show spantree lpthreshold  
The Loop Protect event threshold value is 4
```

# clear spantree lpthreshold

Use this command to return the Loop Protect event threshold to its default value of 3.

## Syntax

```
clear spantree lpthreshold
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the Loop Protect event threshold to the default of 3:

```
B5(rw)->clear spantree lpthreshold
```

# set spantree lpwindow

Use this command to set the Loop Protect event window value in seconds.

## Syntax

```
set spantree lpwindow value
```

## Parameters

<i>value</i>	Specifies the number of seconds that comprise the period during which Loop Protect events are counted. The default event window is 180 seconds.
--------------	---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The Loop Protect Window is a timer value, in seconds, that defines a period during which Loop Protect events are counted. The default value is 180 seconds. If the timer is set to 0, the event counter is not reset until the Loop Protect event threshold is reached. If the threshold is reached, that constitutes a loop protection event.

## Example

This example shows how to set the Loop Protect event window to 120 seconds:

```
B5(rw)->set spantree lpwindow 120
```

# show spantree lpwindow

Use this command to display the current Loop Protect event window value.

## Syntax

```
show spantree lpwindow
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to display the current Loop Protect window value:

```
B5(rw)->show spantree lpwindow  
The Loop Protect event window is set to 120 seconds
```

# clear spantree lpwindow

Use this command to reset the Loop Protect event window to the default value of 180 seconds.

## Syntax

```
clear spantree lpwindow
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the Loop Protect event window to the default of 180 seconds:

```
B5(rw)->clear spantree lpwindow
```

# set spantree lptrapenable

Use this command to enable or disable Loop Protect event notification.

## Syntax

```
set spantree lptrapenable {enable | disable}
```

## Parameters

---

<b>enable</b>   <b>disable</b>	Enables or disables the sending of Loop Protect traps. Default is disabled.
--------------------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

Loop Protect traps are sent when a Loop Protect event occurs, that is, when a port goes to listening due to not receiving BPDUs. The trap indicates port, SID and loop protection status.

## Example

This example shows how to enable sending of Loop Protect traps:

```
B5(rw)->set spantree lptrapenable enable
```

# show spantree lptrapenable

Use this command to display the current status of Loop Protect event notification.

## Syntax

```
show spantree lptrapenable
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to display the current Loop Protect event notification status:

```
B5(rw)->show spantree lptrapenable  
The Loop Protect event notification status is enable
```

# clear spantree lptrapenable

Use this command to return the Loop Protect event notification state to its default state of disabled.

## Syntax

```
clear spantree lptrapenable
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the Loop Protect event notification state to the default of disabled.

```
B5(rw)->clear spantree lptrapenable
```

# set spantree disputedbpduthreshold

Use this command to set the disputed BPDU threshold, which is the number of disputed BPDUs that must be received on a given port/SID until a disputed BPDU trap is sent.

## Syntax

```
set spantree disputedbpduthreshold value
```

## Parameters

---

<i>value</i>	Specifies the number of disputed BPDUs that must be received on a given port/SID to cause a disputed BPDU trap to be sent.  A threshold of 0 indicates that traps should not be sent. The default value is 0.
--------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

A disputed BPDU is one in which the flags field indicates a designated role and learning, and the priority vector is worse than that already held by the port. If a disputed BPDU is received the port is forced to the listening state. Refer to the 802.1Q-2005 standard, *IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks*, for a full description of the dispute mechanism, which prevents looping in cases of one-way communication.

The disputed BPDU threshold is an integer variable that represents the number of disputed BPDUs that must be received on a given port/SID until a disputed BPDU trap is sent and a syslog message is issued. For example, if the threshold is 10, then a trap is issued when 10, 20, 30, and so on, disputed BPDUs have been received.

If the value is 0, traps are not sent. The trap indicates port, SID and total Disputed BPDU count. The default is 0.

## Example

This example shows how to set the disputed BPDU threshold value to 5:

```
B5(rw)->set spantree disputedbpduthreshold 5
```

## show spantree disputedbpduthreshold

Use this command to display the current value of the disputed BPDU threshold.

### Syntax

```
show spantree disputedbpduthreshold
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

## Example

This example shows how to display the current disputed BPDU threshold:

```
B5(rw)->show spantree disputedbpduthreshold
The disputed BPDU threshold value is 0
```

## clear spantree disputedbpduthreshold

Use this command to return the disputed BPDU threshold to its default value of 0, meaning that disputed BPDU traps should not be sent.

### Syntax

```
clear spantree disputedbpduthreshold
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to reset the disputed BPDU threshold to the default of 0:

```
B5(rw)->clear spantree disputedbpduthreshold
```

## show spantree nonforwardingreason

Use this command to display the reason for placing a port in a non-forwarding state due to an exceptional condition.

### Syntax

```
show spantree nonforwardingreason port-string [sid sid]
```

### Parameters

---

<i>port-string</i>	Specifies port(s) for which to display the non-forwarding reason.
<b>sid</b> <i>sid</i>	(Optional) Specifies the specific Spanning Tree(s) for which to display the non-forwarding reason. Valid values are 0 - 4094. If not specified, SID 0 is assumed.

---

### Defaults

If no *port-string* is specified, non-forwarding reason is displayed for all ports.

If no SID is specified, SID 0 is assumed.

### Mode

Switch command, read-only.

### Usage

Exceptional conditions causing a port to be placed in listening or blocking state include a Loop Protect event, receipt of disputed BPDUs, and loopback detection.

### Example

This example shows how to display the non-forwarding reason on ge.1.1:

```
B5(rw)->show spantree nonforwardingreason port ge.1.1
The non-forwarding reason for port ge.1.1 on SID 0 is None
```



## 802.1Q VLAN Configuration

This chapter describes the Enterasys B5 system's capabilities to implement 802.1Q virtual LANs (VLANs).

For information about...	Refer to page...
<a href="#">VLAN Configuration Summary</a>	10-1
<a href="#">Viewing VLANs</a>	10-3
<a href="#">Creating and Naming Static VLANs</a>	10-5
<a href="#">Assigning Port VLAN IDs (PVIDs) and Ingress Filtering</a>	10-8
<a href="#">Configuring the VLAN Egress List</a>	10-13
<a href="#">Setting the Host VLAN</a>	10-18
<a href="#">Enabling/Disabling GVRP (GARP VLAN Registration Protocol)</a>	10-20



**Note:** An Enterasys Networks Feature Guide document containing an in-depth discussion of VLAN configuration is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads/>

### VLAN Configuration Summary

Virtual LANs allow the network administrator to partition network traffic into logical groups and control the flow of that traffic through the network. Once the traffic and, in effect, the users creating the traffic, are assigned to a VLAN, then broadcast and multicast traffic is contained within the VLAN and users can be allowed or denied access to any of the network's resources. Also, some or all of the ports on the device can be configured as GVRP ports, which enable frames received with a particular VLAN ID and protocol to be transmitted on a limited number of ports. This keeps the traffic associated with a particular VLAN and protocol isolated from the other parts of the network.



**Note:** The device can support up to 1024 802.1Q VLANs. The allowable range for VLAN IDs is 1 to 4093. As a default, all ports on the device are assigned to VLAN ID 1, untagged.

### Port String Syntax Used in the CLI

For information on how to designate VLANs and port numbers in the CLI syntax, refer to “[Port String Syntax Used in the CLI](#)” on page 7-1.

## Creating a Secure Management VLAN

By default at startup, there is one VLAN configured on the Enterasys B5 device. It is VLAN ID 1, the DEFAULT VLAN. The default community name, which determines remote access for SNMP management, is set to “public” with read-write access.

If the Enterasys B5 device is to be configured for multiple VLANs, it may be desirable to configure a management-only VLAN. This allows a station connected to the management VLAN to manage the device. It also makes management secure by preventing configuration via ports assigned to other VLANs.

To create a secure management VLAN, you must:

Step	Task	Refer to page...
1.	Create a new VLAN.	<a href="#">10-5</a>
2.	Set the PVID for the desired switch port to the VLAN created in Step 1.	<a href="#">10-9</a>
3.	Add the desired switch port to the egress list for the VLAN created in Step 1.	<a href="#">10-15</a>
4.	Assign host status to the VLAN.	<a href="#">10-18</a>
5.	Set a private community name and access policy.	<a href="#">8-14</a>

The commands used to create a secure management VLAN are listed in [Table 10-1](#). This example assumes the management station is attached to ge.1.1 and wants untagged frames.

The process described here would be repeated on every device that is connected in the network to ensure that each device has a secure management VLAN.

**Table 10-1 Command Set for Creating a Secure Management VLAN**

To do this...	Use these commands...
Create a new VLAN and confirm settings.	<b>set vlan create 2</b> (“ <a href="#">set vlan</a> ” on page 10-5) (Optional) <b>show vlan 2</b> (“ <a href="#">show vlan</a> ” on page 10-3)
Set the PVID to the new VLAN.	<b>set port vlan ge.1.1 2</b> (“ <a href="#">set port vlan</a> ” on page 10-9)
Add the port to the new VLAN’s egress list.	<b>set vlan egress 2 ge.1.1 untagged</b> (“ <a href="#">set vlan egress</a> ” on page 10-15)
Remove the port from the default VLAN’s egress list.	<b>clear vlan egress 1 ge.1.1</b> (“ <a href="#">clear vlan egress</a> ” on page 10-15)
Assign host status to the VLAN.	<b>set host vlan 2</b> (“ <a href="#">set host vlan</a> ” on page 10-18)
Set a private community name and access policy and confirm settings.	<b>set snmp community private</b> (“ <a href="#">set snmp community</a> ” on page 8-14) (Optional) <b>show snmp community</b> (“ <a href="#">show snmp community</a> ” on page 8-13)

## Viewing VLANs

### Purpose

To display a list of VLANs currently configured on the device, to determine how one or more VLANs were created, the ports allowed and disallowed to transmit traffic belonging to VLAN(s), and if those ports will transmit the traffic with a VLAN tag included.

### Command

For information about...	Refer to page...
show vlan	<a href="#">10-3</a>

## show vlan

Use this command to display all information related to one or more VLANs.

### Syntax

```
show vlan [static] [vlan-list] [portinfo [vlan vlan-list | vlan-name] [port port-string]]
```

### Parameters

<b>static</b>	(Optional) Displays information related to static VLANs. Static VLANs are manually created using the <b>set vlan</b> command (“ <a href="#">set vlan</a> ” on page 10-5), SNMP MIBs, or the WebView management application. The default VLAN, VLAN 1, is always statically configured and can’t be deleted. Only ports that use a specified VLAN as their default VLAN (PVID) will be displayed.
<i>vlan-list</i>	(Optional) Displays information for a specific VLAN or range of VLANs.
<b>portinfo</b>	(Optional) Displays VLAN attributes related to one or more ports.
<b>vlan</b> <i>vlan-list</i>   <i>vlan-name</i>	(Optional) Displays port information for one or more VLANs.
<b>port</b> <i>port-string</i>	(Optional) Displays port information for one or more ports.

### Defaults

If no options are specified, all information related to static and dynamic VLANs will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display information for VLAN 1. In this case, VLAN 1 is named “DEFAULT VLAN”. Ports allowed to transmit frames belonging to VLAN 1 are listed as egress ports. Ports that won’t include a VLAN tag in their transmitted frames are listed as untagged ports. There are no forbidden ports (prevented from transmitted frames) on VLAN 1:

```
B5(su)->show vlan 1
VLAN: 1          NAME: DEFAULT VLAN
```

```
VLAN Type: Default
Egress Ports
ge.1.1-10, ge.2.1-4, ge.3.1-7,
Forbidden Egress Ports
None.
Untagged Ports
ge.1.1-10, ge.2.1-4, ge.3.1-7,
```

[Table 10-2](#) provides an explanation of the command output.

**Table 10-2 show vlan Output Details**

Output Field	What It Displays...
VLAN	VLAN ID.
NAME	Name assigned to the VLAN.
Status	Whether it is <b>enabled</b> or <b>disabled</b> .
VLAN Type	Whether it is <b>permanent</b> (static) or <b>dynamic</b> .
Egress Ports	Ports configured to transmit frames for this VLAN.
Forbidden Egress Ports	Ports prevented from transmitting frames for this VLAN.
Untagged Ports	Ports configured to transmit untagged frames for this VLAN.

# Creating and Naming Static VLANs

## Purpose

To create a new static VLAN, or to enable or disable existing VLAN(s).

## Commands

For information about...	Refer to page...
set vlan	<a href="#">10-5</a>
set vlan name	<a href="#">10-6</a>
clear vlan	<a href="#">10-6</a>
clear vlan name	<a href="#">10-7</a>

## set vlan

Use this command to create a new static IEEE 802.1Q VLAN, or to enable or disable an existing VLAN.

### Syntax

```
set vlan {create | enable | disable} vlan-list
```

### Parameters

<b>create   enable   disable</b>	Creates, enables or disables VLAN(s).
----------------------------------	---------------------------------------

<i>vlan-list</i>	Specifies one or more VLAN IDs to be created, enabled or disabled.
------------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

Once a VLAN is created, you can assign it a name using the **set vlan name** command described in “[set vlan name](#)” on page 10-6.

Each VLAN ID must be unique. If a duplicate VLAN ID is entered, the device assumes that the Administrator intends to modify the existing VLAN.

Enter the VLAN ID using a unique number between 1 and 4093. The VLAN IDs of 0 and 4094 and higher may not be used for user-defined VLANs.

### Examples

This example shows how to create VLAN 3:

```
B5(su)->set vlan create 3
```

## set vlan name

Use this command to set or change the ASCII name for a new or existing VLAN.

### Syntax

```
set vlan name vlan-list vlan-name
```

### Parameters

<i>vlan-list</i>	Specifies the VLAN ID of the VLAN(s) to be named.
<i>vlan-name</i>	Specifies the string used as the name of the VLAN (1 to 32 characters).

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the name for VLAN 7 to green:

```
B5(su)->set vlan name 7 green
```

## clear vlan

Use this command to remove a static VLAN from the list of VLANs recognized by the device.

### Syntax

```
clear vlan vlan-list
```

### Parameters

<i>vlan-list</i>	Specifies the VLAN ID of the VLAN(s) to be removed.
------------------	---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to remove a static VLAN 9 from the device's VLAN list:

```
B5(su)->clear vlan 9
```

---

## clear vlan name

Use this command to remove the name of a VLAN from the VLAN list.

### Syntax

```
clear vlan name vlan-list
```

### Parameters

---

<i>vlan-list</i>	Specifies the VLAN ID of the VLAN(s) for which the name will be cleared.
------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the name for VLAN 9:

```
B5(su)->clear vlan name 9
```

# Assigning Port VLAN IDs (PVIDs) and Ingress Filtering

## Purpose

To assign default VLAN IDs to untagged frames on one or more ports, to configure VLAN ingress filtering and constraints, and to set the frame discard mode.

## Commands

For information about...	Refer to page...
show port vlan	<a href="#">10-8</a>
set port vlan	<a href="#">10-9</a>
clear port vlan	<a href="#">10-9</a>
show port ingress filter	<a href="#">10-10</a>
set port ingress filter	<a href="#">10-11</a>
show port discard	<a href="#">10-11</a>
set port discard	<a href="#">10-12</a>

## show port vlan

Use this command to display port VLAN identifier (PVID) information. PVID determines the VLAN to which all untagged frames received on one or more ports will be classified.

### Syntax

```
show port vlan [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays PVID information for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to " <a href="#">Port String Syntax Used in the CLI</a> " on page 7-1.
--------------------	---

### Defaults

If *port -string* is not specified, port VLAN information for all ports will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display PVIDs assigned to ge.2.1 through 6. In this case, untagged frames received on these ports will be classified to VLAN 1:

```
B5(su)->show port vlan ge.2.1-6
ge.2.1 is set to 1
ge.2.2 is set to 1
ge.2.3 is set to 1
ge.2.4 is set to 1
```



```
ge.2.5 is set to 1
ge.2.6 is set to 1
```

## set port vlan

Use this command to configure the PVID (port VLAN identifier) for one or more ports.

### Syntax

```
set port vlan port-string pvid [modify-egress | no-modify-egress]
```

### Parameters

<i>port-string</i>	Specifies the port(s) for which to configure a VLAN identifier. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
<i>pvid</i>	Specifies the VLAN ID of the VLAN to which port(s) will be added.
<b>modify-egress</b>	(Optional) Adds port(s) to VLAN's untagged egress list and removes them from other untagged egress lists.
<b>no-modify-egress</b>	(Optional) Does not prompt for or make egress list changes.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The PVID is used to classify untagged frames as they ingress into a given port.

### Example

This example shows how to add `ge.1.10` to the port VLAN list of VLAN 4 (PVID 4).

```
B5(su)->set vlan create 4
B5(su)->set port vlan ge.1.10 4 modify-egress
```

## clear port vlan

Use this command to reset a port's 802.1Q port VLAN ID (PVID) to the host VLAN ID 1.



**Note:** The following command will reset the specified port's egress status to tagged. To set the specified ports back to the default egress status of untagged, you must issue the [set port vlan](#) command as described on page 10-9.

### Syntax

```
clear port vlan port-string
```

## Parameters

---

<i>port-string</i>	Specifies the port(s) to be reset to the host VLAN ID 1. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset ports `ge.1.3` through `11` to a VLAN ID of `1` (Host VLAN):

```
B5(su)->clear port vlan ge.1.3-11
```

# show port ingress-filter

Use this command to show all ports that are enabled for port ingress filtering, which limits incoming VLAN ID frames according to a port VLAN egress list. If the VLAN ID specified in the received frame is not on the port's VLAN egress list, then that frame is dropped and not forwarded.

## Syntax

```
show port ingress-filter [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Specifies the port(s) for which to display ingress filtering status. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

---

## Defaults

If *port-string* is not specified, ingress filtering status for all ports will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display the port ingress filter status for ports `10` through `15` in slot `1`. In this case, the ports are disabled for ingress filtering:

```
B5(su)->show port ingress-filter ge.1.10-15
  Port      State
  -----  -
  ge.1.10   disabled
  ge.1.11   disabled
  ge.1.12   disabled
  ge.1.13   disabled
  ge.1.14   disabled
  ge.1.15   disabled
```

## set port ingress-filter

Use this command to discard all frames received with a VLAN ID that don't match the port's VLAN egress list.

### Syntax

```
set port ingress-filter port-string {disable | enable}
```

### Parameters

<i>port-string</i>	Specifies the port(s) on which to enable or disable ingress filtering. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
<b>disable   enable</b>	Disables or enables ingress filtering.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

When ingress filtering is enabled on a port, the VLAN IDs of incoming frames are compared to the port's egress list. If the received VLAN ID does not match a VLAN ID on the port's egress list, then the frame is dropped.

Ingress filtering is implemented according to the IEEE 802.1Q standard.

### Example

This example shows how to enable port ingress filtering on ge.1.3:

```
B5(su)->set port ingress-filter ge.1.3 enable
```

## show port discard

Use this command to display the frame discard mode for one or more ports. Ports can be set to discard frames based on whether or not the frame contains a VLAN tag. They can also be set to discard both tagged and untagged frames, or neither.

### Syntax

```
show port discard [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays the frame discard mode for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
--------------------	---

### Defaults

If *port-string* is not specified, frame discard mode will be displayed for all ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display the frame discard mode for `ge.2.7`. In this case, the port has been set to discard all tagged frames:

```
B5(su)->show port discard ge.2.7
Port          Discard Mode
-----
ge.2.7        tagged
```

# set port discard

Use this command to set the frame discard mode on one or more ports.

## Syntax

```
set port discard port-string {tagged | untagged | both | none}
```

## Parameters

---

<i>port-string</i>	Specifies the port(s) for which to set frame discard mode. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>tagged</b>   <b>untagged</b>   <b>both</b>   <b>none</b>	<ul style="list-style-type: none"><li>• Tagged - Discard all incoming (received) tagged packets on the defined port(s).</li><li>• Untagged - Discard all incoming untagged packets.</li><li>• Both - All traffic will be discarded (tagged and untagged).</li><li>• None - No packets will be discarded.</li></ul>

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The options are to discard all incoming tagged frames, all incoming untagged frames, neither (essentially allow all traffic), or both (essentially discarding all traffic).

A common practice is to discard all tagged packet on user ports. Typically an Administrator does not want the end users defining what VLAN they use for communication.

## Example

This example shows how to discard all tagged frames received on port `ge.3.3`:

```
B5(su)->set port discard ge.3.3 tagged
```

# Configuring the VLAN Egress List

## Purpose

To assign or remove ports on the egress list of a particular VLAN. This determines which ports on the switch will be eligible to transmit frames for a particular VLAN. For example, ports 1, 5, 7, 8 could be allowed to transmit frames belonging to VLAN 20 and ports 7,8, 9, 10 could be allowed to transmit frames tagged with VLAN 30 (a port can belong to multiple VLAN Egress lists). Note that the Port Egress list for ports 7 and 8 would contain both VLAN 20 and 30.

The port egress type for all ports can be set to tagged, forbidden, or untagged. In general, VLANs have no egress (except for VLAN 1) until they are configured by static administration, or through dynamic mechanisms such as GVRP.

Setting a port to forbidden prevents it from participating in the specified VLAN and ensures that any dynamic requests (either through GVRP or dynamic egress) for the port to join the VLAN will be ignored. Setting a port to untagged allows it to transmit frames without a tag header. This setting is usually used to configure a port connected to an end user device. Frames sent between VLAN aware switches are typically tagged.

The default VLAN defaults its egress to untagged for all ports.

## Commands

For information about...	Refer to page...
show port egress	<a href="#">10-13</a>
set vlan forbidden	<a href="#">10-14</a>
set vlan egress	<a href="#">10-15</a>
clear vlan egress	<a href="#">10-15</a>
show vlan dynamic egress	<a href="#">10-16</a>
set vlan dynamic egress	<a href="#">10-17</a>

## show port egress

Use this command to display the VLAN membership for one or more ports.

### Syntax

```
show port egress [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays VLAN membership for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

### Defaults

If *port-string* is not specified, VLAN membership will be displayed for all ports.

## Mode

Switch command, read-write.

## Example

This example shows you how to show VLAN egress information for `ge.1.1` through `3`. In this case, all three ports are allowed to transmit VLAN 1 frames as tagged and VLAN 10 frames as untagged. Both are static VLANs:

```
B5(su)->show port egress ge.1.1-3
Port      Vlan      Egress      Registration
Number    Id        Status      Status
-----
ge.1.1    1         tagged     static
ge.1.1    10        untagged   static
ge.1.2    1         tagged     static
ge.1.2    10        untagged   static
ge.1.3    1         tagged     static
ge.1.3    10        untagged   static
```

## set vlan forbidden

Use this command to prevent one or more ports from participating in a VLAN. This setting instructs the device to ignore dynamic requests (either through GVRP or dynamic egress) for the port to join the VLAN.

## Syntax

```
set vlan forbidden vlan-id port-string
```

## Parameters

<i>vlan-id</i>	Specifies the VLAN for which to set forbidden port(s).
<i>port-string</i>	Specifies the port(s) to set as forbidden for the specified <i>vlan-id</i> .

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows you how to set `ge.1.3` to forbidden for VLAN 6:

```
B5(su)->set vlan forbidden 6 ge.1.3
```

## set vlan egress

Use this command to add ports to the VLAN egress list for the device, or to prevent one or more ports from participating in a VLAN. This determines which ports will transmit frames for a particular VLAN.

### Syntax

```
set vlan egress vlan-list port-string [untagged | forbidden | tagged]
```

### Parameters

<i>vlan-list</i>	Specifies the VLAN where a port(s) will be added to the egress list.
<i>port-string</i>	Specifies one or more ports to add to the VLAN egress list of the specified <i>vlan-list</i> . For a detailed description of possible <i>port-string</i> values, refer to “Port String Syntax Used in the CLI” on page 7-1.
<b>untagged</b>   <b>forbidden</b>   <b>tagged</b>	(Optional) Adds the specified ports as: <ul style="list-style-type: none"> <li>• <b>untagged</b> — Causes the port(s) to transmit frames without an IEEE 802.1Q header tag.</li> <li>• <b>forbidden</b> — Instructs the device to ignore dynamic requests (either through GVRP or dynamic egress) from the port(s) to join the VLAN and disallows egress on that port.</li> <li>• <b>tagged</b> — Causes the port(s) to transmit 802.1Q tagged frames.</li> </ul>

### Defaults

If **untagged**, **forbidden** or **tagged** is not specified, the port will be added to the VLAN egress list as tagged.

### Mode

Switch command, read-write.

### Examples

This example shows how to add `ge.1.5` through `10` to the egress list of VLAN 7. Since no “tag” parameter is specified, these ports will transmit VLAN 7 frames as tagged, the default condition:

```
B5(su)->set vlan egress 7 ge.1.5-10
```

This example shows how to forbid ports 13 through 15 in slot 1 from joining VLAN 7 and disallow egress on those ports:

```
B5(su)->set vlan egress 7 ge.1.13-15 forbidden
```

This example shows how to allow port 2 in slot 1 to transmit VLAN 7 frames as untagged:

```
B5(su)->set vlan egress 7 ge.1.2 untagged
```

## clear vlan egress

Use this command to remove ports from a VLAN’s egress list.



**Note:** The following command will reset the specified port’s egress status to tagged. To set the specified ports back to the default egress status of untagged, you must issue the **set vlan egress** command as described on page 10-15.

## Syntax

```
clear vlan egress vlan-list port-string [forbidden]
```

## Parameters

<i>vlan-list</i>	Specifies the number of the VLAN from which a port(s) will be removed from the egress list.
<i>port-string</i>	Specifies one or more ports to be removed from the VLAN egress list of the specified <i>vlan-list</i> . For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
<b>forbidden</b>	(Optional) Clears the forbidden setting from the specified port(s) and resets the port(s) as able to egress frames if so configured by either static or dynamic means.

## Defaults

If **forbidden** is not specified, tagged and untagged settings will be cleared.

## Mode

Switch command, read-write.

## Examples

This example shows how to remove ge.3.14 from the egress list of VLAN 9:

```
B5(su)->clear vlan egress 9 ge.3.14
```

This example shows how to remove all Ethernet ports in slot 2 from the egress list of VLAN 4:

```
B5(su)->clear vlan egress 4 ge.2.*
```

# show vlan dynamicegress

Use this command to display the status of dynamic egress (enabled or disabled) for one or more VLANs.

## Syntax

```
show vlan dynamicegress [vlan-list]
```

## Parameters

<i>vlan-list</i>	(Optional) Displays dynamic egress status for specific VLAN(s).
------------------	---

## Defaults

If *vlan-list* is not specified, the dynamic egress status for all VLANs will be displayed.

## Mode

Switch command, read-write.



## Example

This example shows how to display the dynamic egress status for VLANs 50-55:

```
B5(rw)->show vlan dynamicegress 50-55
VLAN 50 is disabled
VLAN 51 is disabled
VLAN 52 is disabled
VLAN 53 is enabled
VLAN 54 is enabled
VLAN 55 is enabled
```

## set vlan dynamicegress

Use this command to administratively set the dynamic egress status for one or more VLANs.

### Syntax

```
set vlan dynamicegress vlan-list {enable | disable}
```

### Parameters

<i>vlan-list</i>	Specifies the VLANs by ID to enable or disable dynamic egress.
<b>enable</b>   <b>disable</b>	Enables or disables dynamic egress.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

If dynamic egress is enabled for a particular VLAN, when a port receives a frame tagged with that VLAN's ID, the switch will add the receiving port to that VLAN's egress list. Dynamic egress is disabled on the Enterasys B5 by default.

For example, assume you have 20 AppleTalk users on your network who are mobile users (that is, use different ports every day), but you want to keep the AppleTalk traffic isolated in its own VLAN. You can create an AppleTalk VLAN with a VLAN ID of 55 with a classification rule that all AppleTalk traffic gets tagged with VLAN ID 55. Then, you enable dynamic egress for VLAN 55. Now, when an AppleTalk user plugs into port ge.3.5 and sends an AppleTalk packet, the switch will tag the packet to VLAN 55 and also add port ge.3.5 to VLAN 55's egress list, which allows the AppleTalk user to receive AppleTalk traffic.

### Example

This example shows how to enable dynamic egress on VLAN 55:

```
B5(rw)->set vlan dynamicegress 55 enable
```

# Setting the Host VLAN

## Purpose

To configure a host VLAN that only select devices are allowed to access. This secures the host port for management-only tasks.



**Note:** The host port is the management entity of the device. Refer to “[Creating a Secure Management VLAN](#)” on page 10-2 for more information.

## Commands

For information about...	Refer to page...
show host vlan	<a href="#">10-18</a>
set host vlan	<a href="#">10-18</a>
clear host vlan	<a href="#">10-19</a>

## show host vlan

Use this command to display the current host VLAN.

### Syntax

```
show host vlan
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the host VLAN:

```
B5(su)->show host vlan
Host vlan is 7.
```

## set host vlan

Use this command to assign host status to a VLAN.

### Syntax

```
set host vlan vlan-id
```

## Parameters

---

<i>vlan-id</i>	Specifies the number of the VLAN to set as the host VLAN.
----------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The host VLAN should be a secure VLAN where only designated users are allowed access. For example, a host VLAN could be specifically created for device management. This would allow a management station connected to the management VLAN to manage all ports on the device and make management secure by preventing management via ports assigned to other VLANs.



**Note:** Before you can designate a VLAN as the host VLAN, you must create a VLAN using the set of commands described in [“Creating and Naming Static VLANs” on page 10-5](#).

## Example

This example shows how to set VLAN 7 as the host VLAN:

```
B5(su)->set host vlan 7
```

# clear host vlan

Use this command to reset the host VLAN to the default setting of 1.

## Syntax

```
clear host vlan
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to set the host VLAN to the default setting:

```
B5(su)->clear host vlan
```

# Enabling/Disabling GVRP (GARP VLAN Registration Protocol)

## About GARP VLAN Registration Protocol (GVRP)

The following sections describe the device operation when its ports are operating under the Generic Attribute Registration Protocol (GARP) application – GARP VLAN Registration Protocol (GVRP).

### Overview

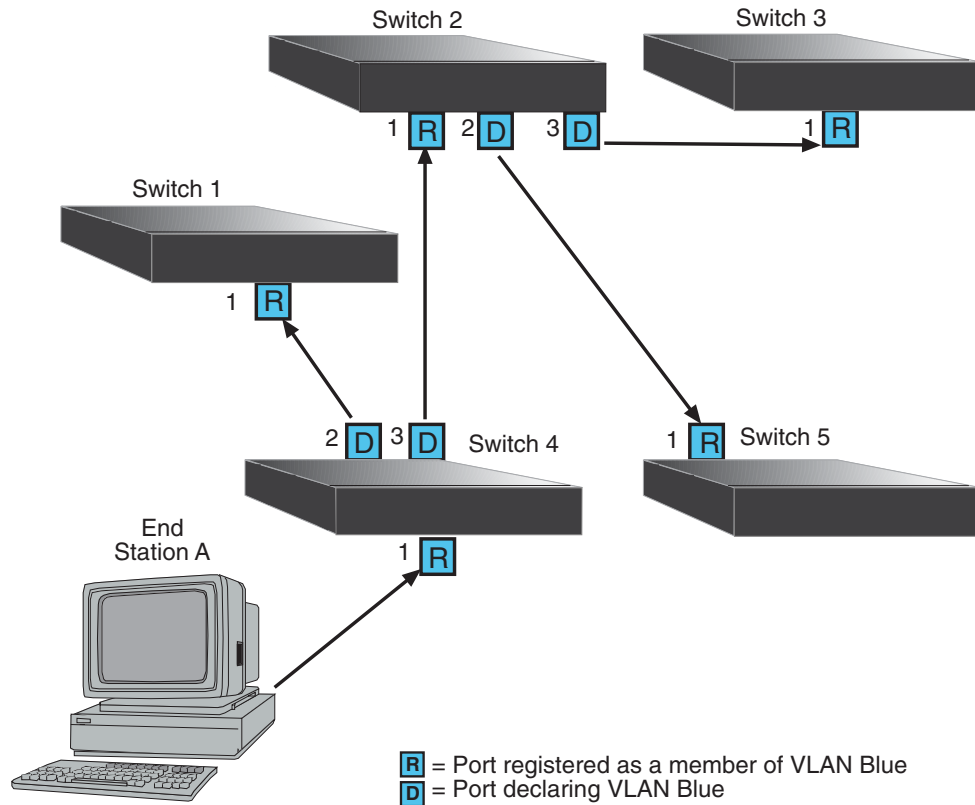
The purpose of GVRP is to dynamically create VLANs across a switched network. When a VLAN is declared, the information is transmitted out GVRP configured ports on the device in a GARP formatted frame using the GVRP multicast MAC address. A switch that receives this frame, examines the frame, and extracts the VLAN IDs. GVRP then creates the VLANs and adds the receiving port to its tagged member list for the extracted VLAN ID (s). The information is then transmitted out the other GVRP configured ports of the device. [Figure 10-1](#) shows an example of how VLAN blue from end station A would be propagated across a switch network.

### How It Works

In [Figure 10-1](#) on page 10-21, Switch 4, port 1 is registered as being a member of VLAN Blue and then declares this fact out all its ports (2 and 3) to Switch 1 and Switch 2. These two devices register this in the port egress lists of the ports (Switch 1, port 1 and Switch 2, port 1) that received the frames with the information. Switch 2, which is connected to Switch 3 and Switch 5 declares the same information to those two devices and the port egress list of each port is updated with the new information, accordingly.

Configuring a VLAN on an 802.1Q switch creates a static VLAN entry. The entry will always remain registered and will not time out. However, dynamic entries will time-out and their registrations will be removed from the member list if the end station A is removed. This ensures that, if switches are disconnected or if end stations are removed, the registered information remains accurate.

The end result is that the port egress list of a port is updated with information about VLANs that reside on that port, even if the actual station on the VLAN is several hops away.

**Figure 10-1 Example of VLAN Propagation via GVRP**

## Purpose

To dynamically create VLANs across a switched network. The GVRP command set is used to display GVRP configuration information, the current global GVRP state setting, individual port settings (enable or disable) and timer settings. By default, GVRP is disabled globally on the device and disabled on all ports.

## Commands

For information about...	Refer to page...
show gvrp	<a href="#">10-22</a>
show garp timer	<a href="#">10-22</a>
set gvrp	<a href="#">10-23</a>
clear gvrp	<a href="#">10-24</a>
set garp timer	<a href="#">10-25</a>
clear garp timer	<a href="#">10-25</a>

## show gvrp

Use this command to display GVRP configuration information.

### Syntax

```
show gvrp [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays GVRP configuration information for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

### Defaults

If *port-string* is not specified, GVRP configuration information will be displayed for all ports and the device.

### Mode

Switch command, read-only.

### Example

This example shows how to display GVRP status for the device and for fw.2.1:

```
B5(su)->show gvrp ge.2.1
Global GVRP status is enabled.
```

```
Port Number      GVRP status
-----
ge.2.1           disabled
```

## show garp timer

Use this command to display GARP timer values for one or more ports.

### Syntax

```
show garp timer [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays GARP timer information for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

### Defaults

If *port-string* is not specified, GARP timer information will be displayed for all ports.

### Mode

Switch command, read-only.

## Example

This example shows how to display GARP timer information on ports 1 through 10 in slot 1:



**Note:** For a functional description of the terms **join**, **leave**, and **leaveall timers**, refer to the standard IEEE 802.1Q documentation, which is not supplied with this device.

```
B5(su)->show garp timer ge.1.1-10
Port based GARP Configuration: (Timer units are centiseconds)
Port Number      Join          Leave         Leaveall
-----
ge.1.1           20            60            1000
ge.1.2           20            60            1000
ge.1.3           20            60            1000
ge.1.4           20            60            1000
ge.1.5           20            60            1000
ge.1.6           20            60            1000
ge.1.7           20            60            1000
ge.1.8           20            60            1000
ge.1.9           20            60            1000
ge.1.10          20            60            1000
```

Table 10-3 provides an explanation of the command output. For details on using the **set gvrp** command to enable or disable GVRP, refer to “[set gvrp](#)” on page 10-23. For details on using the **set garp timer** command to change default timer values, refer to “[set garp timer](#)” on page 10-25.

**Table 10-3 show gvrp configuration Output Details**

Output Field	What It Displays...
Port Number	Port designation. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
Join	Join timer setting.
Leave	Leave timer setting.
Leaveall	Leavall timer setting.

## set gvrp

Use this command to enable or disable GVRP globally on the device or on one or more ports.

### Syntax

```
set gvrp {enable | disable} [port-string]
```

### Parameters

<b>disable</b>   <b>enable</b>	Disables or enables GVRP on the device.
<i>port-string</i>	(Optional) Disables or enables GVRP on specific port(s). For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

### Defaults

If *port-string* is not specified, GVRP will be disabled or enabled for all ports.

The default condition on the switch is GVRP enabled globally, disabled per ports.

## Mode

Switch command, read-write.

## Examples

This example shows how to enable GVRP globally on the device:

```
B5(su)->set gvrp enable
```

This example shows how to disable GVRP globally on the device:

```
B5(su)->set gvrp disable
```

This example shows how to enable GVRP on `ge.1.3`:

```
B5(su)->set gvrp enable ge.1.3
```

## clear gvrp

Use this command to clear GVRP status on one or more ports.

## Syntax

```
clear gvrp [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Clears GVRP status on specific port(s). For a detailed description of possible <i>port-string</i> values, refer to " <a href="#">Port String Syntax Used in the CLI</a> " on page 7-1.
--------------------	---

---

## Defaults

If *port-string* is not specified, GVRP status will be cleared to the default condition for all ports.

The default condition on the switch is GVRP disabled per port.

## Mode

Switch command, read-write.

## Usage

This command does not affect the global state of GVRP. To enable or disable GVRP globally, use the `set gvrp enable | disable` command.

## Example

This example shows how to clear GVRP status on all ports on the device:

```
B5(su)->clear gvrp
```



## set garp timer

Use this command to adjust the values of the join, leave, and leaveall timers.

### Syntax

```
set garp timer {[join timer-value] [leave timer-value] [leaveall timer-value]}
port-string
```

### Parameters

<b>join</b> timer-value	Sets the GARP join timer in centiseconds (Refer to 802.1Q standard.)
<b>leave</b> timer-value	Sets the GARP leave timer in centiseconds (Refer to 802.1Q standard.)
<b>leaveall</b> timer-value	Sets the GARP leaveall timer in centiseconds (Refer to 802.1Q standard.)
<i>port-string</i>	Specifies the port(s) on which to configure GARP timer settings. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The setting of these timers is critical and should only be changed by personnel familiar with the 802.1Q standards documentation, which is not supplied with this device.

### Examples

This example shows how to set the GARP join timer value to 100 centiseconds for all ports:

```
B5(su)->set garp timer join 100 *.*.*
```

This example shows how to set the leave timer value to 300 centiseconds for all ports:

```
B5(su)->set garp timer leave 300 *.*.*
```

This example shows how to set the leaveall timer value to 20000 centiseconds for all ports:

```
B5(su)->set garp timer leaveall 20000 *.*.*
```

## clear garp timer

Use this command to reset GARP timers back to default values.

### Syntax

```
clear garp timer {[join] [leave] [leaveall]} port-string
```

## Parameters

<b>join</b>	(Optional) Resets the join timer to 20 centiseconds.
<b>leave</b>	(Optional) Resets the leave timer to 60 centiseconds.
<b>leaveall</b>	(Optional) Resets the leaveall time to 1000 centiseconds.
<i>port-string</i>	Specifies the port or ports on which to reset the GARP timer(s).

## Defaults

At least one optional parameter must be entered.

## Mode

Switch command, read-write.

## Example

The example shows how to reset the GARP leave timer to 60 centiseconds.

```
B5(su)->clear garp timer leave ge.1.1
```

## Policy Classification Configuration

This chapter describes the Policy Classification set of commands and how to use them.

For information about...	Refer to page...
<a href="#">Policy Classification Configuration Summary</a>	11-1
<a href="#">Configuring Policy Profiles</a>	11-2
<a href="#">Configuring Classification Rules</a>	11-6
<a href="#">Assigning Ports to Policy Profiles</a>	11-14
<a href="#">Configuring Policy Class of Service (CoS)</a>	11-16



**Note:** An Enterasys Networks Feature Guide document containing an in-depth discussion of Policy configuration is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads/>

### Policy Classification Configuration Summary

Enterasys B5 devices support policy profile-based provisioning of network resources by allowing IT administrators to:

- Create, change or remove policy profiles based on business-specific use of network services.
- Permit or deny access to specific services by creating and assigning classification rules which map user profiles to protocol-based frame filtering policies configured for a particular VLAN or Class of Service (CoS).
- Assign or unassign ports to policy profiles so that only ports activated for a profile will be allowed to transmit frames accordingly.



**Note:** It is recommended that you use Enterasys Networks NMS Policy Manager as an alternative to CLI for configuring policy classification on the Enterasys B5 devices.

# Configuring Policy Profiles

## Purpose

To review, create, change and remove user profiles that relate to business-driven policies for managing network resources.



**Note:** B3, B5, C3, C5, and G3 devices support profile-based CoS traffic rate limiting only. Policy rules specifying CoS will only rate limit on D2, C2 and B2 devices, including when C2 and B2 devices are configured on mixed stacks containing B3 and C3 devices.

## Commands

For information about...	Refer to page...
show policy profile	<a href="#">11-2</a>
set policy profile	<a href="#">11-4</a>
clear policy profile	<a href="#">11-5</a>

## show policy profile

Use this command to display policy profile information.

### Syntax

```
show policy profile {all | profile-index [consecutive-pids] [-verbose]}
```

### Parameters

<b>all</b>   <i>profile-index</i>	Displays policy information for all profile indexes or a specific profile index.
<i>consecutive-pids</i>	(Optional) Displays information for specified consecutive profile indexes.
<b>-verbose</b>	(Optional) Displays detailed information.

### Defaults

If optional parameters are not specified, summary information will be displayed for the specified index or all indices.

### Mode

Switch command, read-only.

### Example

This example shows how to display policy information for profile 11:

```
B5(su)->show policy profile 11
Profile Index      : 11
Profile Name      : MacAuth1
Row Status        : active
Port VID Status   : Enable
Port VID Override : 11
CoS               : 0
```

```

CoS Status           : Disable
Egress Vlans         : none
Forbidden Vlans      : none
Untagged Vlans       : none
Rule Precedence      : 1-31
                     : MACSource(1), MACDest(2), Unknown(3),
                     : Unknown(4), Unknown(5), Unknown(6),
                     : Unknown(7), Unknown(8), Unknown(9),
                     : Unknown(10), Unknown(11), IPSource(12),
                     : IPDest(13), IPFrag(14), UDPSrcPort(15),
                     : UDPDestPort(16), TCPSrcPort(17), TCPDestPort(18),
                     : ICMPType(19), Unknown(20), IPTOS(21),
                     : IPProto(22), Unknown(23), Unknown(24),
                     : Ether(25), Unknown(26), VLANTag(27),
                     : Unknown(28), Unknown(29), Unknown(30),
                     : port(31)
Admin Profile Usage   : none
Oper Profile Usage    : none
Dynamic Profile Usage : none

```

Table 11-1 provides an explanation of the command output.

**Table 11-1 show policy profile Output Details**

Output Field	What It Displays...
Profile Index	Number of the profile.
Profile Name	User-supplied name assigned to this policy profile.
Row Status	Whether or not the policy profile is enabled ( <b>active</b> ) or disabled.
Port VID Status	Whether or not PVID override is <b>enabled</b> or <b>disabled</b> for this profile. If all classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
Port VID Override	The PVID assigned to packets, if PVID override is enabled.
CoS	CoS priority value to assign to packets, if CoS override is enabled.
CoS Status	Whether or not Class of Service override is <b>enabled</b> or <b>disabled</b> for this profile. If all classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
Egress VLANs	VLAN(s) that ports to which the policy profile is assigned can use for tagged egress.
Forbidden VLANs	VLAN(s) forbidden to ports to which the policy profile is assigned.
Untagged VLANs	VLAN(s) that ports to which the policy profile is assigned can use for untagged egress.
Rule Precedence	Displays the precedence of types of rules.
Admin Profile Usage	Ports administratively assigned to use this policy profile.
Oper Profile Usage	Ports currently assigned to use this policy profile.
Dynamic Profile Usage	Port dynamically assigned to use this policy profile.

## set policy profile

Use this command to create a policy profile entry.

### Syntax

```
set policy profile profile-index [name name] [pvid-status {enable | disable}]
[pvid pvid] [cos-status {enable | disable}] [cos cos] [egress-vlans egress-
vlans][forbidden-vlans forbidden-vlans] [untagged-vlans untagged-vlans]
[precedence precedence-list] [append] [clear]
```

### Parameters

<i>profile-index</i>	Specifies an index number for the policy profile. Valid values are <b>1 - 255</b> .
<b>name</b> <i>name</i>	(Optional) Specifies a name for the policy profile. This is a string from 1 to 64 characters.
<b>pvid-status</b> <b>enable</b>   <b>disable</b>	(Optional) Enables or disables PVID override for this profile. If all classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
<b>pvid</b> <i>pvid</i>	(Optional) Specifies the PVID to packets, if PVID override is enabled and invoked as default behavior.
<b>cos-status</b> <b>enable</b>   <b>disable</b>	(Optional) Enables or disables Class of Service override for this profile. If all classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.  <b>Note:</b> A maximum of 99 rules can be supported per policy profile for policy profiles that have cos-status enabled.
<b>cos</b> <i>cos</i>	(Optional) Specifies a CoS value to assign to packets, if CoS override is enabled and invoked as default behavior. Valid values are <b>0</b> to <b>7</b> .
<b>egress-vlans</b> <i>egress-vlans</i>	(Optional) Specifies that the port to which this policy profile is applied should be added to the egress list of the VLANs defined by <i>egress-vlans</i> . Packets will be formatted as tagged.
<b>forbidden-vlans</b> <i>forbidden-vlans</i>	(Optional) Specifies that the port to which this policy profile is applied should be added as forbidden to the egress list of the VLANs defined by <i>forbidden-vlans</i> . Packets from this port will not be allowed to participate in the listed VLANs.
<b>untagged-vlans</b> <i>untagged-vlans</i>	(Optional) Specifies that the port to which this policy profile is applied should be added to the egress list of the VLANs defined by <i>untagged-vlans</i> . Packets will be formatted as untagged.
<b>append</b>	(Optional) Appends this policy profile setting to settings previously specified for this policy profile by the <b>egress-vlans</b> , <b>forbidden-vlans</b> , or <b>untagged-vlans</b> parameters.  If <b>append</b> is not used, previous VLAN settings are replaced.
<b>clear</b>	(Optional) Appends this policy profile setting from settings previously specified for this policy profile by the <b>egress-vlans</b> , <b>forbidden-vlans</b> , or <b>untagged-vlans</b> parameters.
<b>precedence</b> <i>precedence-list</i>	(Optional) Assigns a rule precedence to this profile. Lower values will be given higher precedence. For a list of values, refer to the <b>show policy profile</b> command output.

## Defaults

If optional parameters are not specified, none will be applied.

## Mode

Switch command, read-write.

## Example

This example shows how to create a policy profile 1 named "netadmin" with PVID override enabled for PVID 10, and Class-of-Service override enabled for CoS 5. This profile can use VLAN 10 for untagged egress:

```
B5(su)->set policy profile 1 name netadmin pvid-status enable pvid 10 cos-status enable cos 5 untagged-vlans 10
```

# clear policy profile

Use this command to delete a policy profile entry.

## Syntax

```
clear policy profile profile-index
```

## Parameters

---

<i>profile-index</i>	Specifies the index number of the profile entry to be deleted. Valid values are 1 to 255.
----------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to delete policy profile 8:

```
B5(su)->clear policy profile 8
```

# Configuring Classification Rules

## Purpose

To review, create, assign, and unassign classification rules to policy profiles. This maps user profiles to protocol-based frame filtering policies.



**Note:** B3, B5, C3, C5, and G3 devices support profile-based CoS traffic rate limiting only. Policy rules specifying CoS will only rate limit on D2, C2 and B2 devices, including when C2 and B2 devices are configured on mixed stacks containing B3 and C3 devices.

## Commands

For information about...	Refer to page...
show policy rule	<a href="#">11-6</a>
show policy capability	<a href="#">11-8</a>
set policy rule	<a href="#">11-10</a>
clear policy rule	<a href="#">11-12</a>
clear policy all-rules	<a href="#">11-13</a>

## show policy rule

Use this command to display policy classification rule information.

### Syntax

```
show policy rule [all | admin-profile | profile-index] [ether | ipproto |
ipdestsocket | ipsourcesocket | iptos | macdest | macsource | tcpdestport |
tcpsourceport | udpdestport | udpsourceport] [data] [mask mask] [port-string port-
string] [rule-status {active | not-in-service | not-ready}] [storage-type {non-
volatile | volatile}] | [drop | forward] [dynamic-pid dynamic-pid] [cos cos]
[admin-pid admin-pid] [-verbose] [usage-list] [display-if-used]
```

### Parameters

<b>all</b>   <b>admin-profile</b>   <i>profile-index</i>	Displays policy classification rules for <b>all</b> profiles, the <b>admin-profile</b> , or for a specific profile index number. Valid values are <b>1 - 1023</b> .
<b>ether</b>	Displays Ethernet type II rules.
<b>ipproto</b>	Displays IP protocol field in IP packet rules.
<b>ipdestsocket</b>	Displays IP destination address rules.
<b>ipsourcesocket</b>	Displays IP source address rules.
<b>iptos</b>	Displays Type of Service rules.
<b>macdest</b>	Displays MAC destination address rules.
<b>macsource</b>	Displays MAC source address rules.
<b>tcpdestport</b>	Displays TCP destination port rules.



<b>tcpsourceport</b>	Displays TCP source port rules.
<b>udpdestport</b>	Displays UDP destination port rules.
<b>udpsourceport</b>	Displays UDP source port rules.
<i>data</i>	Displays rules for a predefined classifier. This value is dependent on the classification type entered. Refer to <a href="#">Table 11-3</a> for valid values for each classification type.
<b>mask</b> <i>mask</i>	(Optional) Displays rules for a specific data mask. Refer to <a href="#">Table 11-3</a> for valid values for each classification type and data value.
<b>port-string</b> <i>port-string</i>	(Optional) Displays rules related to a specific ingress port.
<b>rule-status</b> <i>active</i>   <i>not-in-service</i>   <i>not-ready</i>	(Optional) Displays rules related to a specific rules status.
<b>storage-type</b> <i>non-volatile</i>   <i>volatile</i>	(Optional) Displays rules configured for either non-volatile or volatile storage.
<b>drop</b>   <b>forward</b>	Displays rules based on whether matching packets will be dropped or forwarded.
<b>dynamic-pid</b> <i>dynamic-pid</i>	Displays rules associated with a specific dynamic policy ID.
<b>cos</b> <i>cos</i>	(Optional) Displays rules for a Class-of-Service value.
<b>admin-pid</b> <i>admin-pid</i>	Displays rules associated with a specific administrative policy ID [1..1023].
<b>-verbose</b>	(Optional) Displays detailed information.
<b>usage-list</b>	(Optional) If selected, each rule's usage-list shall be checked and shall display only those ports which have applied this rule.
<b>display-if-used</b>	(Optional) Displays rule(s) only if they are applied to at least one port.

## Defaults

If **verbose** is not specified, summary information will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display policy classification information for Ethernet type 2 rules

```
B5(su)->show policy rule ether
|PID|Rule Type|Rule Data|Mk|PortStr|RS|ST|VLAN|CoS|U|
|02|Ether|2048 (0x0800)|16|All|A|NV|fwr|?|
|02|Ether|2049 (0x0801)|16|All|A|NV|drp|?|
|02|Ether|2989 (0x0bad)|16|All|A|NV|drp|?|
|02|Ether|33079 (0x8137)|16|All|A|NV|drp|?|
```

This example shows how to display policy classification information for administrative rule 1

```
B5(su)->show policy rule admin-pid 1
|Admin|Rule Type|Rule Data|Mk|PortStr|RS|ST|dPID|aPID|U|
|admin|Port|ge.1.1|16|ge.1.1|A|NV||1|?|
|admin|Port|ge.1.2|16|ge.1.2|A|NV||1|?|
|admin|Port|ge.1.3|16|ge.1.3|A|NV||1|?|
```

admin Port	ge.1.4	16 ge.1.4	A NV	1 ?
admin Port	ge.1.5	16 ge.1.5	A NV	1 ?
admin Port	ge.1.6	16 ge.1.6	A NV	1 ?
admin Port	ge.1.7	16 ge.1.7	A NV	1 ?
admin Port	ge.1.8	16 ge.1.8	A NV	1 ?
admin Port	ge.1.9	16 ge.1.9	A NV	1 ?
admin Port	ge.1.10	16 ge.1.10	A NV	1 ?
admin Port	ge.1.11	16 ge.1.11	A NV	1 ?
admin Port	ge.1.12	16 ge.1.12	A NV	1 ?

Table 11-2 provides an explanation of the command output.

**Table 11-2 show policy rule Output Details**

Output Field	What It Displays...
PID	Profile index number. Assigned to this classification rule with the <b>set policy profile</b> command (“ <a href="#">set policy profile</a> ” on page 11-4).
Rule Type	Type of classification rule. Refer to <a href="#">Table 11-3</a> for valid types.
Rule Data	Rule data value. Refer to <a href="#">Table 11-3</a> for valid values for each classification type.
Mk	Rule data mask. Refer to <a href="#">Table 11-3</a> for valid values for each classification data value.
PortStr	Ingress port(s) to which this rule applies.
RS	Whether or not the status of this rule is active (A), not in service or not ready.
ST	Whether or not this rule's storage type is non-volatile (NV) or volatile (V).
VLAN	VLAN ID to which this rule applies and whether or not matching packets will be dropped or forwarded.
CoS	If applicable, Class of Service value to which this rule applies.
U	Whether or not this rule has been used.
dPID	Whether or not this is a dynamic profile ID.
aPID	Whether or not this is an administrative profile ID.

## show policy capability

Use this command to display detailed policy classification capabilities supported by your Enterasys B5 device.

### Syntax

```
show policy capability
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

## Usage

Use this command to display detailed policy classification capabilities supported by your Enterasys B5 device. The output of this command shows a table listing classifiable traffic attributes and the type of actions, by rule type, that can be executed relative to each attribute. Above the table is a list of all the actions possible on this device.

The left-most column of the table lists all possible classifiable traffic attributes. The next two columns from the left indicate how policy profiles may be assigned, either administratively or dynamically. The next four columns from the left indicate the actions that may be performed. The last three columns indicate auditing options.

An x in an action column for a traffic attribute row indicates that your system has the capability to perform that action for traffic classified by that attribute.

## Example

This example shows how to display the device's policy classification capabilities. Refer to [“set policy rule”](#) on page 11-10 for a description of the parameters displayed:

```
B5(su)->show policy capability
```

The following supports related to policy are supported in this device:

VLAN Forwarding	Priority	Permit							
Deny	Precedence Reordering	Rules Table							
Longest Prefix Rules									
SUPPORTED RULE TYPES	C	N	N	S	P	D	G	P	E
MAC source address				X	X	X			
MAC destination address				X	X	X			
IPX source address									
IPX destination address									
IPX source socket									
IPX destination socket									
IPX transmission control									
IPX type field									
IPv6 source address									
IPv6 destination address									
IPv6 flow label									
IP source address				X	X	X			
IP destination address				X	X	X			
IP fragmentation									
UDP port source				X	X	X			
UDP port destination				X	X	X			
TCP port source				X	X	X			
TCP port destination				X	X	X			
ICMP packet type				X	X	X			
TTL									
IP type of service				X	X	X			
IP proto				X	X	X			
Ether II packet type			X	X	X	X			
LLC DSAP/SSAP/CTRL									
VLAN tag									
Replace tci									
Port string	X	X	X	X	X	X			

=====

## set policy rule

Use this command to assign incoming untagged frames to a specific policy profile and to VLAN or Class-of-Service classification rules.

### Syntax

```
set policy rule profile-index {ether | ipproto | ipdestsocket | ipsourcesocket |
iptos | macdest | macsource | tcpdestport | tcpsourceport | udpdestport |
udpsourceport} data [mask mask] {[vlan vlan] [cos cos] | [drop | forward]}
```



**Note:** Classification rules are automatically enabled when created.

### Parameters

The following parameters apply to creating a traffic classification rule.

<i>profile-index</i>	Specifies a policy profile number to which this rule will be assigned. Policy profiles are configured with the <b>set policy profile</b> command as described in “ <a href="#">set policy profile</a> ” on page 11-4. Valid <i>profile-index</i> values are 1- 255.
<b>ether</b>	Specifies that the rule should apply to traffic with the specified type field in Ethernet II packet.
<b>ipproto</b>	Specifies that the rule should apply to traffic with the specified Protocol field in IP packet.
<b>ipdestsocket</b>	Specifies that the rule should apply to traffic with the specified destination IP address with optional post-fixed TCP or UDP port.
<b>ipsourcesocket</b>	Specifies that the rule should apply to traffic with the specified source IP address, with optional post-fixed TCP or UDP port.
<b>iptos</b>	Specifies that the rule should apply to traffic with the specified Type of Service field in IP packet.
<b>macdest</b>	Specifies that the rule should apply to traffic with the specified MAC destination address.
<b>macsource</b>	Specifies that the rule should apply to traffic with the specified MAC source address.
<b>tcpdestport</b>	Specifies that the rule should apply to traffic with the specified TCP destination port.
<b>tcpsourceport</b>	Specifies that the rule should apply to traffic with the specified TCP source port.
<b>udpdestport</b>	Specifies that the rule should apply to traffic with the specified UDP destination port.
<b>udpsourceport</b>	Specifies that the rule should apply to traffic with the specified UDP source port.
<i>data</i>	Specifies the code for the specified traffic classifier (listed above). This value is dependent on the classification type entered. Refer to <a href="#">Table 11-3</a> for valid values for each classification type.

<b>mask</b> <i>mask</i>	(Optional) Specifies the number of significant bits to match, dependent on the <i>data</i> value entered. Refer to <a href="#">Table 11-3</a> for valid values for each classification type and data value.
<b>vlan</b> <i>vlan</i>	Specifies the action of the rule is to classify to a VLAN ID.
<b>cos</b> <i>cos</i>	Specifies the action of the rule is to classify to a Class-of-Service ID. Valid values are <b>0 - 4095</b> . A value of -1 indicates that no CoS forwarding behavior modification is desired. (Not supported on B3, B5, C3, C5, and G3.)
<b>drop   forward</b>	Specifies that packets within this classification will be dropped or forwarded.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

A policy classification rule has two main parts: Traffic Description and Actions. The Traffic Description identifies the type of traffic to which the rule will pertain. Actions specify whether that traffic will be assigned class of service, assigned to a VLAN, or both.

[Table 11-3](#) provides the **set policy rule** *data* values that can be entered for a particular parameter, and the *mask* bits that can be entered for each classifier associated with that parameter.

**Table 11-3 Valid Values for Policy Classification Rules**

Classification Rule Parameter	<i>data</i> value	<i>mask</i> bits
ether	Type field in Ethernet II packet: <b>1536 - 65535</b> or <b>0x600 - 0xFFFF</b>	Not applicable.
ipproto	Protocol field in IP packet: <b>0 - 255</b> or <b>0 - 0xFF</b>	Not applicable.
Destination or Source IP Address: ipdestsocket ipsourcesocket	IP Address in dotted decimal format: <b>000.000.000.000</b> and (Optional) post-fixed port: <b>0 - 65535</b>	<b>1 - 48</b>
iptos	Type of Service field in IP packet: <b>0 - 252</b> or <b>0 - 0xFC</b>	Not applicable.
Destination or Source MAC: macdest macsource	MAC Address: <b>00-00-00-00-00-00</b>	<b>1 - 48</b>
Destination or Source TCP port: tcpdestport tcpsourceport	TCP Port Number: <b>0 - 65535</b> or <b>0 - 0xFFFF</b>	<b>1 - 16</b>
Destination or Source UDP port: udpsourceport udpdestport	UDP Port Number: <b>0 - 65535</b> or <b>0 - 0xFFFF</b>	<b>1 - 16</b>

## Examples

This example shows how to use [Table 11-3](#) to assign a rule to policy profile 3 that will filter Ethernet II Type 1526 frames to VLAN 7:

```
B5(su)->set policy rule 3 ether 1526 vlan 7
```

This example shows how to use [Table 11-3](#) to assign a rule to policy profile 5 that will forward UDP packets from source port 45:

```
B5(su)->set policy rule 5 udpportsource 45 forward
```

This example shows how to use [Table 11-3](#) to assign a rule to policy profile 1 that will drop IP source traffic from IP address 1.2.3.4. If mask 32 is not specified as shown, a default mask of 48 bits (IP address + port) would be applied:

```
B5(su)->set policy rule 1 ipsourcesocket 1.2.3.4 mask 32 drop
```

## clear policy rule

Use this command to delete policy classification rule entries.

### Syntax

```
clear policy rule profile-index {all-pid-entries | {ether | iproto | ipdestsocket | ipsourcesocket | iptos | macdest | macsource | tcpdestport | tcpsourceport | udpdestport | udpsourceport}}
```

### Parameters

The following parameters apply to deleting a classification rule.

<i>profile-index</i>	Specifies a policy profile for which to delete classification rules. Valid <i>profile-index</i> values are <b>1 - 255</b> .
<b>all-pid-entries</b>	Deletes all entries associated with the specified policy profile.
<b>ether</b>	Deletes associated Ethernet II classification rule.
<b>iproto</b>	Deletes associated IP protocol classification rule.
<b>ipdestsocket</b>	Deletes associated IP destination classification rule.
<b>ipsourcesocket</b>	Deletes associated IP source classification rule.
<b>iptos</b>	Deletes associated IP Type of Service classification rule.
<b>macdest</b>	Deletes associated MAC destination address classification rule.
<b>macsource</b>	Deletes associated MAC source address classification rule.
<b>tcpdestport</b>	Deletes associated TCP destination port classification rule.
<b>tcpsourceport</b>	Deletes associated TCP source port classification rule.
<b>udpdestport</b>	Deletes associated UDP destination port classification rule.
<b>udpsourceport</b>	Deletes associated UDP source port classification rule.

### Defaults

When applicable, *data* and *mask* must be specified for individual rules to be cleared.

### Mode

Switch command, read-write.

## Examples

This example shows how to delete Ethernet II Type 1526 classification rule entries associated with policy profile 1 from all ports.

```
B5(su)->clear policy rule 1 ether 1526
```

This example shows how to remove a rule from policy profile 5 that will forward UDP frames from source port 45.

```
B5(su)->clear policy rule 5 udpsourceport 45
```

## clear policy all-rules

Use this command to remove all policy classification rules.

### Syntax

```
clear policy all-rules
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to remove all administrative and policy index rules:

```
B5(su)->clear policy all-rules
```

# Assigning Ports to Policy Profiles



**Note:** Refer to [Appendix A, Policy and Authentication Capacities](#) for information about policy limits for this platform.

## Purpose

To assign and unassign ports to policy profiles.

## Commands

For information about...	Refer to page...
set policy port	<a href="#">11-14</a>
clear policy port	<a href="#">11-15</a>

## set policy port

Use this command to assign ports to a policy profile.

### Syntax

```
set policy port port-string profile-index
```

### Parameters

<i>port-string</i>	Specifies the port(s) to add to the policy profile. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
<i>profile-index</i>	Specifies the ID of the policy profile (role) to which the port(s) will be added. This value must match the <i>profile-index</i> value assigned using the <b>set policy profile</b> command (“ <a href="#">set policy profile</a> ” on page 11-4) in order for a policy profile to be active on the specified port.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to allow Gigabit Ethernet ports 5 through 15 in slot 1 to transmit frames according to policy profile 1:

```
B5(su)->set policy port ge.1.5-15 1
```



## clear policy port

Use this command to remove a policy profile from one or more ports.

### Syntax

```
clear policy port port-string profile-index
```

### Parameters

<i>port-string</i>	Specifies the port(s) from which to remove the policy profile. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<i>profile-index</i>	Specifies the ID of the policy profile (role) to which the port(s) will be added. This value must match the <i>profile-index</i> value assigned using the <b>set policy profile</b> command ( <a href="#">“set policy profile”</a> on page 11-4) in order for a policy profile to be active on the specified port.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to remove policy profile 10 from port 21 in slot 1:

```
B5(rw)->clear policy port ge.1.21 10
```

## Configuring Policy Class of Service (CoS)



**Note:** It is recommended that you use Enterasys Networks NMS Policy Manager as an alternative to CLI for configuring policy-based CoS on the switches.

The Enterasys B5 supports Class of Service (CoS), which allows you to assign mission-critical data to a higher priority through the device by delaying less critical traffic during periods of congestion. The higher priority traffic going through the device is serviced first (before lower priority traffic). The Class of Service capability of the device is implemented by a priority queueing mechanism. Class of Service is based on the IEEE 802.1D (802.1p) standard specification, and allows you to define eight priorities (0-7, with 7 granted highest priority) and up to 8 transmit queues (0-7) for each port.

By default, policy-based CoS is disabled on the device, and default or user-assigned port-based 802.1D (802.1p) settings are used to determine traffic prioritization. When policy-based CoS is enabled, the default and user-assigned policy-based settings will override port-based settings described in [Chapter 12](#).

Class of Service functionality can also be used to control broadcast, unknown unicast, and/or multicast flooding. This feature prevents configured ports from being disrupted by a traffic storm by rate-limiting specific types of packets through those ports. Refer to “[About CoS-Based Flood Control](#)” on page 11-18 for more information.

### About Policy-Based CoS Configurations

Once enabled using the `set cos state` command, you can add to the policy-based CoS function by defining new port groupings, and assigning inbound rate limiters. The process for user-defined CoS configuration involves the following steps and associated commands listed in [Procedure 11-1](#). An example follows the procedure.

#### Procedure 11-1 User-Defined CoS Configuration

Step	Task	Command(s)
1.	Enable CoS	<code>set cos state enable</code>
2.	Create CoS IRL port groups	<code>set cos port-config irl</code>
3.	Define physical rate limiters for groups	<code>set cos port-resource irl</code>
4.	Create virtual reference for the IRL resource (physical reference) for each port group	<code>set cos reference</code>
5.	Add IRL reference to CoS settings table	<code>set cos settings</code>

#### Example

This example creates different inbound rate limiters for two port groups and then assigns them to traffic with a CoS setting of 0.

1. Configure two port groups, one for user ports and one for uplink ports and assign ports to the groups. Port group 1.0 will represent user ports, group 2.0 will represent uplink ports.

```
B5(su)->set cos port-config irl 1.0 name Users ports ge.1.1-46
B5(su)->set cos port-config irl 2.0 name Uplink ports ge.1.47-48
```

```
B5(su)->show cos port-config
Inbound Rate Limiting Port Configuration Entries
```

```

-----
Port Group Name :Default
Port Group      :0
Port Type       :0
Assigned Ports  :none
-----

```

```

-----
Port Group Name :Users
Port Group      :1
Port Type       :0
Assigned Ports  :ge.1.1-46
-----

```

```

-----
Port Group Name :Uplink
Port Group      :2
Port Type       :0
Assigned Ports  :ge.1.47-48
-----

```

2. Configure physical inbound rate limiters for each port group. For the user port group (1.0), create an IRL (irl-index of 1) for 512 kbps. For the uplink port group (2.0), create an IRL (irl-index of 1) for 10 megabits per second (10,000 kbps).

```

B5(su)->set cos port-resource irl 1.0 1 unit kbps rate 512
B5(su)->set cos port-resource irl 2.0 1 unit kbps rate 10000

```

```

B5(su)->show cos port-resource irl 1.0 1
Group Index Resource Type Unit      Rate      Rate Limit Type Action
-----
1.0          1          irl kbps 512          drop          none

```

```

B5(su)->show cos port-resource irl 2.0 1
Group Index Resource Type Unit      Rate      Rate Limit Type Action
-----
2.0          1          irl kbps 10000       drop          none

```

3. In the CoS IRL reference mapping table for each port group, create a reference for each IRL resource created in the previous step. We will use reference number 1.

```

B5(su)->set cos reference irl 1.0 1 rate-limit 1
B5(su)->set cos reference irl 2.0 1 rate-limit 1

```

```

B5(su)->show cos reference irl 1.0

```

```

Group Index Reference Type Rate Limiter
-----
1.0          0          irl none
1.0          1          irl 1
1.0          2          irl none
1.0          3          irl none
...
1.0          97         irl none
1.0          98         irl none
1.0          99         irl none

```

```

B5(su)->show cos reference irl 2.0

```

```

Group Index Reference Type Rate Limiter
-----
2.0          0          irl none
2.0          1          irl 1
2.0          2          irl none
2.0          3          irl none
...

```

```

2.0      97      irl  none
2.0      98      irl  none
2.0      99      irl  none

```

- In the CoS settings table, configure a CoS setting for CoS index 1, which has a priority of 0. We enter the IRL reference, created in the previous step.

```
B5(su)->set cos settings 0 irl-reference 1
```

```
B5(su)->show cos settings
```

CoS Index	Priority	ToS	IRL
0	0	*	1
1	1	*	*
2	2	*	*
3	3	*	*
4	4	*	*
5	5	*	*
6	6	*	*
7	7	*	*

## About CoS-Based Flood Control

CoS-based flood control prevents configured ports from being disrupted by a traffic storm by rate-limiting specific types of packets through those ports. When flood control is enabled on a port, incoming traffic is monitored over one second intervals. During an interval, the incoming traffic rate for each configured traffic type (unicast, broadcast, multicast) is compared with the configured traffic flood control rate, specified in packets per second.

If, during a one second interval, the incoming traffic of a configured type reaches the traffic flood control rate configured on the port, CoS-based flood control drops the traffic until the interval ends. Packets are then allowed to flow again until the limit is again reached.

The following procedure describes the steps and commands required to configure CoS-based flood control.

### Procedure 11-2

Step	Task	Command(s)
1.	Enable CoS.	<code>set cos state enable</code>
2.	Create a CoS flood control port resource, which specifies flood control rate limiters that can be mapped to specific ports.	<code>set cos port-resource flood-ctrl</code>
3.	Assign the flood control resource to specific ports.	<code>set cos port-config flood-ctrl</code>

### Example

This example creates a broadcast rate limiter (index 1.0) of 5 packets per second and assigns it to ports ge.1.2 and ge.2.2.

```
B5(su)->set cos state enable
```

```
B5(su)->set cos port-resource flood-ctrl 1.0 broadcast rate 5
```

```
B5(su)->set cos port-config flood-ctrl 1.0 ports ge.1.2;ge.2.2 append
```

## Commands

For information about...	Refer to page...
set cos state	<a href="#">11-19</a>
show cos state	<a href="#">11-20</a>
clear cos state	<a href="#">11-20</a>
set cos settings	<a href="#">11-21</a>
clear cos settings	<a href="#">11-22</a>
show cos settings	<a href="#">11-22</a>
set cos port-config	<a href="#">11-23</a>
show cos port-config	<a href="#">11-24</a>
clear cos port-config	<a href="#">11-25</a>
set cos port-resource irl	<a href="#">11-26</a>
set cos port-resource flood-ctrl	<a href="#">11-27</a>
show cos port-resource	<a href="#">11-28</a>
clear cos port-resource irl	<a href="#">11-29</a>
clear cos port-resource flood-ctrl	<a href="#">11-30</a>
set cos reference	<a href="#">11-30</a>
show cos reference	<a href="#">11-31</a>
clear cos reference	<a href="#">11-32</a>
show cos unit	<a href="#">11-33</a>
clear cos all-entries	<a href="#">11-33</a>
show cos port-type	<a href="#">11-34</a>

## set cos state

Use this command to enable or disable Class of Service.

### Syntax

```
set cos state {enable | disable}
```

### Parameters

<b>enable   disable</b>	Enables or disables Class of Service on the switch. Default state is disabled.
-------------------------	--

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to enable Class of Service:

```
B5(rw)->set cos state enable
```

## show cos state

Use this command to display the Class of Service enable state.

### Syntax

```
show cos state
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to show the Class of Service enable state:

```
B5(rw)->show cos state  
Class-of-Service application is enabled
```

## clear cos state

Use this command to set CoS state back to its default setting of disabled.

### Syntax

```
clear cos state
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the CoS state back to its default setting of disabled:

```
B5(su)->clear cos state
```

## set cos settings

Use this command to configure a Class of Service entry in the CoS settings table.

### Syntax

```
set cos settings cos-index priority priority [tos-value tos-value] [irl-reference
irl-reference]
```

### Parameters

<i>cos-index</i>	Specifies a Class of Service entry. Valid values are <b>0</b> to <b>255</b> .
<b>priority</b> <i>priority</i>	Specifies an 802.1d priority value. Valid values are <b>0</b> to <b>7</b> , with 0 being the lowest priority. See Usage section below for more information.
<b>tos-value</b> <i>tos-value</i>	(Optional) Specifies a Type of Service value. Valid values are <b>0</b> to <b>255</b> . See Usage section below for more information.
<b>irl-reference</b> <i>irl-reference</i>	(Optional) Set the inbound rate limiter associated with this entry. Valid values are 0 to 99. See Usage section below for more information.

### Defaults

If no optional parameters are specified, none will be applied.

### Mode

Switch command, read-write.

### Usage

The CoS settings table takes individual class of service features and displays them as belonging to a CoS entry. Essentially, it is used for CoS feature assignment. Each class of service entry consists of an index, 802.1p priority, an optional ToS value, and an IRL reference.

- **CoS Index**

Indexes are unique identifiers for each CoS setting. CoS indexes 0 through 7 are created by default and mapped directly to 802.1p priority for backwards compatibility. These entries cannot be removed, and 802.1p priority values cannot be changed. When CoS is enabled, indexes are assigned. Up to 256 CoS indexes or entries can be configured.

- **Priority**

802.1p priority can be applied per CoS index. For each new CoS index created, the user has the option to assign an 802.1p priority value 0 to 7 for the class of service. CoS indexes 0 through 7 map directly to 802.1p priorities and cannot be changed as they exist for backward compatibility.

- **ToS**

This value can be set per class of service, but is not required. When a frame is assigned to a class of service for which this value is configured, the ToS field of the incoming IP packet will be overwritten to the user-defined value. All but the last two bits of the ToS field are rewritable. ToS can be set for CoS indexes 0 through 7.

- **IRL Reference**

The CoS IRL reference field is optional, as rate limits are not required. The IRL reference does not assign an inbound rate limit but points to the CoS IRL Reference Mapping Table. This reference may be thought of as the virtual rate limiter that will assign the physical rate limiter defined by the IRL Reference Mapping Table.

## Example

This example shows how to create CoS entry 8 with a priority value of 3:

```
B5(rw)->set cos settings 8 priority 3
```

## clear cos settings

Use this command to clear Class of Service entry settings.

### Syntax

```
clear cos settings cos-list {[all] | [priority] [tos-value] [irl-reference]}
```

### Parameters

<i>cos-list</i>	Specifies a Class of Service entry to clear.
<b>all</b>	Clears all settings associated with this entry.
<b>priority</b>	Clears the priority value associated with this entry.
<b>tos-value</b>	Clears the Type of Service value associated with this entry.
<b>irl-reference</b>	Clear the IRL reference associated with this entry.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the priority for CoS entry 8:

```
B5(rw)->clear cos settings 8 priority
```

## show cos settings

Use this command to display Class of Service parameters.

### Syntax

```
show cos settings [cos-list]
```

### Parameters

<i>cos-list</i>	(Optional) Specifies a Class of Service entry to display.
-----------------	---

### Defaults

If not specified, all CoS entries will be displayed.

### Mode

Switch command, read-only.



## Example

This example shows how to show all CoS settings:

```
B5(su)->show cos settings
CoS Index Priority  ToS      IRL      flood-ctrl
-----
0             0           48       *        enabled
1             1           *        *        enabled
2             2           *        *        enabled
3             3           *        *        enabled
4             4           *        *        enabled
5             5           *        *        enabled
6             6           *        *        enabled
7             7           *        *        enabled
```

## set cos port-config

Use this command to create a port group for inbound rate limiting or flood control and add or remove ports from the group.

### Syntax

```
set cos port-config {irl|flood-ctrl} group-type-index [name name] [ports port-
list] [append] | [clear]
```

### Parameters

<b>irl</b>	Specifies that this is an inbound rate limiting (IRL) port group.
<b>flood-ctrl</b>	Specifies that this is a flood control port group.
<i>group-type-index</i>	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .
<b>name name</b>	(Optional) User defined name for the <b>group</b> .
<b>ports port-list</b>	(Optional) Ports assigned to the <b>group</b> . All ports must be of the same port <b>type</b> (Fast Ethernet, Gigabit Ethernet).
<b>append</b>	(Optional) Append (add) the ports to the ports that are already in the <b>group</b> .
<b>clear</b>	(Optional) Clear the given ports from those assigned to the <b>group</b> .

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

CoS port groups are identified by group number and the type of ports in the group, in the form of **group#.port-type**. The port group 0.0 exists by default. This default port group cannot be removed and all physical ports in the system are assigned to it. Up to seven additional port groups (1

through 7) can be configured. Currently, only one port type (type 0) is supported. This port type supports 100 limiters.

Additional port groups may be created for flexibility. Ports assigned to a new port group must be mutually exclusive from the other port group entries—ports are automatically removed from the default port group—and must be comprised of the same port type as defined by the port group.

The creation of additional port groups could be used to combine similar ports by their function for flexibility. For instance, ports associated to users can be added to a port group called “Users” and ports associated to uplink ports can be added to a port group called “Uplink.” Using these port groups, a single class of service can assign different rate limits to each port group. “User” ports can be assigned one rate limit, while “Uplink” ports can be assigned another.

The command `show cos port-config` displays each port group configured by group and type, with the group name and associated (assigned) ports. The command `show cos port-type` displays the available inbound rate limiting resources for the port type.

## Example

This example configures two port groups, one for user ports and one for uplink ports and assign ports to the groups. Port group 1.0 will represent user ports, group 2.0 will represent uplink ports.

```
B5(su)->set cos port-config irl 1.0 name Users ports ge.1.1-46
B5(su)->set cos port-config irl 2.0 name Uplink ports ge.1.47-48
```

## show cos port-config

Use this command to show CoS port groups and the assigned ports.

### Syntax

```
show cos port-config [irl|flood-ctrl [group-type-index]]
```

### Parameters

<b>irl</b>	(Optional) Specifies that inbound rate limiting configuration information should be displayed.
<b>flood-ctrl</b>	(Optional) Specifies that flood control rate configuration information should be displayed.
<i>group-type-index</i>	(Optional) Show assigned ports for a specific port group. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .

### Defaults

The `show cos port-config` command by itself will show all Port Groups.

### Mode

Switch command, read-only.

## Example

This example shows all inbound rate limiting port groups. Note that ports ge.1.1 through ge.1.48 were removed from the default port group 0.0 when they were added to port groups 1.0 and 2.0.

```
B5(su)->show cos port-config irl
```

```
Inbound Rate Limiting Port Configuration Entries
```

```
-----
Port Group Name  :Default
Port Group      :0
Port Type       :0
Assigned Ports  :none
-----
```

```
Port Group Name  :Users
Port Group      :1
Port Type       :0
Assigned Ports  :ge.1.1-46
-----
```

```
Port Group Name  :Uplink
Port Group      :2
Port Type       :0
Assigned Ports  :ge.1.47-48
-----
```

## clear cos port-config

Use this command to clear CoS port groups or assigned ports.

### Syntax

```
clear cos port-config {irl|flood-ctrl} {all | group-type-index [entry] | [name]
[ports]}
```

### Parameters

<b>irl</b>	Clear an IRL port group configuration.
<b>flood-ctrl</b>	Clear a flood control port group configuration.
<b>all</b>	Clear all inbound rate limiting port-config non-default entries.
<i>group-type-index</i>	Delete a specific port group or group name, or clear the ports from that group. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .
<b>entry</b>	Delete this non-default inbound rate limiter entry.
<b>name</b>	Clear the administratively assigned textual description of this port group entry to its default.
<b>ports</b>	Clear the ports assigned to this group to its default.

### Defaults

None.

## Mode

Switch command, read-write.

## Usage

The default port group 0.0 cannot be deleted.

## Example

This example deletes all IRL Port Groups except for the Default group 0.0:

```
B5(su)->clear cos port-config irl all
```

# set cos port-resource irl

Use this command to set the inbound rate limit parameters for a specific IRL resource for a specific port group.

## Syntax

```
set cos port-resource irl group-type-index irl-index {[unit {kbps}] [rate rate]
[type {drop}]}[syslog enable | disable] [trap enable|disable]
```

## Parameters

<i>group-type-index</i>	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .
<i>irl-index</i>	Index number of the inbound rate limiter resource associated with this entry. Valid values range from 0 to 99.
<b>unit</b>	Unit of measure for the inbound rate limiter (only option is Kbps).
<b>kbps</b>	Kilobits per second.
<b>rate rate</b>	Data rate for this inbound rate limiter. This is the actual rate limit. Valid values range from 512 to 1,000,000 Kbps for a Gigabit port.
<b>type drop</b>	Action for the rate limiter. The only action option is drop the frame if all limiters are exceeded.
<b>syslog enable disable</b>	Enable or disable reporting a syslog entry if limiters are exceeded.
<b>trap enable disable</b>	Enable or disable sending a trap if limiters are exceeded.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

CoS port resources are where actual physical rate limiters are configured. Resources map directly to the number of rate limiters supported by the port type. (Port type 0 supports 100 IRL resources.) Resources exist for each port group and are indexed as **group#.port-type.irl-index**. Port resources are not initially configured as rate limiting.

Inbound rate limiting, or rate policing, simply drops or clips traffic inbound if a configured rate is exceeded. CoS inbound rate limiting allows the user to configure rate limits based on kilobits per second.

The `show cos port-resource` command displays the resources available for each port group. By default, no IRL resources are configured. The default Rate Limiting algorithm is drop and cannot be configured otherwise.

## Example

This example sets the inbound rate limit resource index number 1 for port group 2.0 to 10000 Kbps or 1 MB:

```
B5(su)->set cos port-resource irl 2.0 1 unit kbps rate 10000 type drop
```

## set cos port-resource flood-ctrl

Use this command to create a CoS-based flood control port resource. This resource specifies flood control rate limiters that can be mapped to specific ports.

## Syntax

```
set cos port-resource flood-ctrl group-type-index {unicast | multicast | broadcast | all} rate rate
```

## Parameters

<i>group-type-index</i>	Specifies a port group/type index. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .
<b>unicast</b>	Specifies rate limiting will be applied to unknown unicast traffic.
<b>multicast</b>	Specifies rate limiting will be applied to multicast traffic.
<b>broadcast</b>	Specifies rate limiting will be applied to broadcast traffic.
<b>all</b>	Specifies rate limiting will be applied to unknown unicast, multicast, and broadcast traffic.
<b>rate rate</b>	Specifies a rate limit in packets per second.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

CoS port resources are where actual physical rate limiters are configured. This command can be used to create up to three different flood control limit resources for the port-type index of 0. The resources are assigned to specific ports with the **set cos port-config** command.

## Example

This example creates a port resource broadcast rate limiter of 5 packets per second for the port group type index of 1.0 (group # 1 of port-type index 0).

```
B5(su)->set cos port-resource flood-ctrl 1.0 broadcast rate 5
```

## show cos port-resource

Use this command to display the configured port resources.

## Syntax

```
show cos port-resource [irl [group-type-index [irl-index]]] | [flood-ctrl [group-type-index]]
```

## Parameters

<b>irl</b>	(Optional) Specifies that inbound rate limiting port resources should be displayed.
<b>flood-ctrl</b>	(Optional) Specifies that flood control port resources should be displayed.
<i>group-type-index</i>	(Optional) Specifies a port group/type index. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .
<i>irl-index</i>	(Optional) Inbound rate limiter resource index configured for the specified port group. Valid values range from 0 to 99.

## Defaults

If **irl** or **flood-ctrl** are not specified, all port resources are shown.

If a port group and IRL index are not specified, the IRL configuration for all resources (0-99) for all configured port groups will be shown.

If a port group is not specified with the **flood-ctrl** parameter, flood control resources for all configured port groups will be shown.

## Mode

Switch command, read-only.

## Examples

This example displays the IRL resource index number 1 configuration for group 2.0.

```
B5(su)->show cos port-resource irl 2.0 1
```

'?' after the rate value indicates an invalid rate value

```
Group Index Resource Type Unit Rate Rate Limit Type Action
```

```

-----
2.0          1          irl  kbps 10000          drop          none
-----

```

This example displays the flood control resources configured for group 1.0.

```
B5(su)->show cos port-resource flood-ctrl 1.0
```

'?' after the rate value indicates an invalid rate value

Group Index	Resource	Type	Unit	Rate	Rate Limit type	Action
1.0	ucast	flood-ctrl	pps	20	drop	none
1.0	mcast	flood-ctrl	pps	10	drop	none
1.0	bcast	flood-ctrl	pps	5	drop	none

## clear cos port-resource irl

Use this command to clear inbound rate limit resources to default values.

### Syntax

```
clear cos port-resource irl {all | group-type-index [irl-index [unit] [rate]
[type]]}
```

### Parameters

<b>all</b>	Clear all IRL resources for all port groups.
<i>group-type-index</i>	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .
<i>irl-index</i>	(Optional) Inbound rate limiter resource index associated with the specified port group. Valid values range from 0 to 99.
<b>unit</b>	Clear the unit of measure for the inbound rate limiter.
<b>rate</b>	Clear the data rate for this inbound rate limiter.
<b>type</b>	Clear the action for the rate limiter.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example clears the data rate to 0 for IRL resource index 1 for group 2.0.

```
B5(su)->clear cos port-resource irl 2.0 1 rate
```

## clear cos port-resource flood-ctrl

Use this command to clear flood control port resources to default values.

### Syntax

```
clear cos port-resource flood-ctrl {all | group-type-index {unicast | multicast | broadcast | all [rate]}}
```

### Parameters

<b>all</b>	Clear all flood control resources for all port groups.
<i>group-type-index</i>	Specifies a port group/type index. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .
<b>unicast</b>	Clear unicast port resources for the specified port group.
<b>multicast</b>	Clear multicast port resources for the specified port group.
<b>broadcast</b>	Clear broadcast port resources for the specified port group.
<b>all</b>	Clear all flood control port resources for the specified port group.
<b>rate</b>	(Optional) Clear the data rate limiter of the specified type of port resource to the default (none or disabled).

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example clears the unicast port resource for port group 1.0 to default values.

```
B5(su)->clear cos port-resource flood-ctrl 1.0 unicast
```

## set cos reference

Use this command to set the Class of Service inbound rate limiting reference configuration.

### Syntax

```
set cos reference irl group-type-index reference rate-limit irl-index
```

### Parameters

<b>irl</b>	Specifies that an IRL reference is being configured.
<i>group-type-index</i>	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .



<i>reference</i>	IRL reference number associated with this entry.
<b>rate-limit</b> <i>irl-index</i>	Rate limiter (IRL resource index) to bind this reference to. Valid values range from 0 to 99.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The CoS reference table maps the user-defined IRL references found in the CoS settings table (see “[set cos settings](#)” on page 11-21) to rate limiters created in the port resource table (see “[set cos port-resource irl](#)” on page 11-26). The CoS reference table indexes can be thought of as virtual rate limiters. The table accounts for the maximum number of rate limiters supported by the device. The virtual limiters then map to the physical rate limiters. The CoS IRL Reference Table is not configured by default.

The CoS IRL reference table uses 100 indexes or virtual rate limiters, and maps each virtual limiter to a physical limiter or resource. An IRL reference table exists for each port group configured, and is indexed similarly to port resources, as `port group#, port-type, reference`. IRL references are not populated with limiters (resources), but can be configured by the user. The IRL reference table can be displayed using the [show cos reference](#) command.

## Example

In the CoS IRL reference mapping table for port groups 1.0 and 2.0, create a reference for the IRL resource number 1 created for each group. The reference number 1 is used.

```
B5(su)->set cos reference irl 1.0 1 rate-limit 1
B5(su)->set cos reference irl 2.0 1 rate-limit 1
```

# show cos reference

Use this command to show the Class of Service inbound rate limiting reference configuration.

## Syntax

```
show cos reference [irl [group-type-index]]
```

## Parameters

<b>irl</b>	(Optional) Specifies that inbound rate limiting reference information should be displayed.
<i>group-type-index</i>	(Optional) Specifies an inbound rate limiting port group/type index. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for <code>group#</code> can range from 0 to 7. Valid values for <code>port-type</code> can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .

## Defaults

If **irl** is not specified, all CoS reference information is displayed.

If a specific port group is not specified, information for all port groups is displayed.

## Mode

Switch command, read-only.

## Example

This example shows the Class of Service IRL references for port group 1.0. Note that not all of the 100 possible references are displayed in this output example.

```
B5(su)->show cos reference irl 1.0
```

Group	Index	Reference	Type	Rate Limiter
1.0	0		irl	none
1.0	1		irl	1
1.0	2		irl	none
1.0	3		irl	none
...				
1.0	97		irl	none
1.0	98		irl	none
1.0	99		irl	none

## clear cos reference

Use this command to clear the Class of Service inbound rate limiting reference configuration.

## Syntax

```
clear cos reference irl {all / group-type-index reference}
```

## Parameters

<b>irl</b>	Specifies that IRL references are being cleared.
<b>all</b>	Clear all groups indexes and references.
<i>group-type-index</i>	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of <b>group#.port-type</b> .  Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as <b>3.0</b> .
<i>reference</i>	Clear a specific reference for the specified port group.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear the CoS inbound rate limiting reference configuration for all groups:

```
B5(su)->clear cos reference irl all
```

## show cos unit

Use this command to show possible CoS unit entries.

### Syntax

```
show cos unit [irl [port-type index] [kbps]] [flood-ctrl [port-type index] [pps]]
```

### Parameters

<b>irl</b>	(Optional) Display only IRL unit information.
<b>port-type index</b>	(Optional) Display information about the specified port type. (Only port-type index 0 is supported.)
<b>kbps</b>	(Optional) Display kbps information.
<b>flood-ctrl</b>	(Optional) Display only flood control unit information.
<b>pps</b>	(Optional) Display pps information.

### Defaults

If no parameters are entered, all Cos unit information is displayed.

### Mode

Switch command, read-only.

### Examples

This example shows possible unit entries for inbound rate limiting:

```
B5(su)->show cos unit irl
```

```
Type:                               Unit:
irl = inbound rate limiting          Kbps = Kilobits per second
```

Port Type	Type	Unit	Maximum Rate	Minimum Rate	Granularity
0	irl	Kbps	1000000	64	1

This examples shows flood control unit information.

```
B5(su)->show cos unit flood-ctrl
```

```
Type:                               Unit:
flood-ctrl = flood control type      pps = packets per second
```

Port Type	Type	Unit	Maximum Rate	Minimum Rate	Granularity
0	flood-ctrl	pps	148810	0	1

## clear cos all-entries

Use this command to clear all Class of Service entries except entries 0-7.

### Syntax

```
clear cos all-entries
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear the CoS configuration for all entries except entries 0-7:

```
B5(su)->clear cos all-entries
```

# show cos port-type

Use this command to display Class of Service port type configurations.

## Syntax

```
show cos port-type [irl [port-type]] [flood-ctrl [port-type]]
```

## Parameters

<b>irl</b>	(Optional) Displays inbound rate limiting information.
<b>flood-ctrl</b>	(Optional) Displays flood control information.
<i>port-type</i>	(Optional) Displays information for a specific port type. (Only port type 0 is supported.)

## Defaults

If no parameters are specified, inbound rate limiting and flood control information for all port types is displayed.

## Mode

Switch command, read-only.

## Usage

The B5 implementation provides one default port type (0) for designating available inbound rate limiting or flood control resources. Port type 0 includes all ports.

The port type 0 IRL description is "B5 100 IRL," which indicates that this port type provides a maximum of 100 inbound rate limiting resources per port group. The port type 0 flood control description is "B5 3 flood-ctrl" which indicates that this port type provides a maximum of 3 flood control resources per port group.

## Examples

This example shows inbound rate limiting information for port type 0.

```
B5(su)->show cos port-type irl 0
```

Number of resources: Supported rate types:  
 irl = inbound rate limiter(s) Kbps = kilobits per second

Index	Port type description	Number of limiters	Supported rate type	Eligible ports	Unselected ports
0	B5 100 IRL	100	kbps	ge.1.1-48	ge.1.1-4

This example shows flood control information for port type 0.

B5(su)->show cos port-type flood-ctrl 0

Number of resources: Supported rate types:  
 flood-ctrl = flood control type Pps = Packets per second

Index	Port type description	Number of limiters	Supported rate type	Eligible ports	Unselected ports
0	B5 3 flood-ctrl	3	pps	ge.1.1-24	ge.1.1-24



## Port Priority Configuration

This chapter describes the Port Priority set of commands and how to use them. Refer to the “Configuring QoS” Feature Guide for detailed information about configuring quality of service on the Enterasys B5. The Enterasys Networks firmware Feature Guides are available at:

<https://extranet.enterasys.com/downloads/>

For information about...	Refer to page...
<a href="#">Port Priority Configuration Summary</a>	12-1
<a href="#">Configuring Port Priority</a>	12-2
<a href="#">Configuring Priority to Transmit Queue Mapping</a>	12-4
<a href="#">Configuring Quality of Service (QoS)</a>	12-7

### Port Priority Configuration Summary

The Enterasys B5 device supports Class of Service (CoS), which allows you to assign mission-critical data to higher priority through the device by delaying less critical traffic during periods of congestion. The higher priority traffic through the device is serviced first before lower priority traffic. The Class of Service capability of the device is implemented by a priority queueing mechanism. Class of Service is based on the IEEE 802.1D (802.1p) standard specification, and allows you to define eight priorities (0 through 7) and assign them to transmit queues for each port.

A priority 0 through 7 can be set on each port, with 0 being the lowest priority. A port receiving a frame without priority information in its tag header is assigned a priority according to the default priority setting on the port. For example, if the priority of a port is set to 4, the frames received through that port without a priority indicated in their tag header are classified as a priority 4 and transmitted according to that priority.



**Note:** When CoS override is enabled using the **set policy profile** command as described in “[set policy profile](#)” on page 11-4, CoS-based classification rules will take precedence over priority settings configured with the **set port priority** command described in this section.

# Configuring Port Priority

## Purpose

To view or configure port priority characteristics as follows:

- Display or change the port default Class-of Service (CoS) transmit priority (0 through 7) of each port for frames that are received (ingress) without priority information in their tag header.
- Display the current traffic class mapping-to-priority of each port.
- Set each port to transmit frames according to 802.1D (802.1p) priority set in the frame header.

## Commands

For information about...	Refer to page...
show port priority	<a href="#">12-4</a>
set port priority	<a href="#">12-3</a>
clear port priority	<a href="#">12-3</a>

## show port priority

Use this command to display the 802.1D priority for one or more ports.

### Syntax

```
show port priority [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays priority information for a specific port. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

### Defaults

If *port-string* is not specified, priority for all ports will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display the port priority for the ge.2.1 through 5.

```
B5(su)->show port priority ge.2.1-5
ge.2.1 is set to 0
ge.2.2 is set to 0
ge.2.3 is set to 0
ge.2.4 is set to 0
ge.2.5 is set to 0
```



## set port priority

Use this command to set the 802.1D (802.1p) Class-of-Service transmit priority (0 through 7) on each port. A port receiving a frame without priority information in its tag header is assigned a priority according to the priority setting on the port. For example, if the priority of a port is set to 5, the frames received through that port without a priority indicated in their tag header are classified as a priority 5.

A frame with priority information in its tag header is transmitted according to that priority.

### Syntax

```
set port priority port-string priority
```

### Parameters

<i>port-string</i>	Specifies the port for which to set priority. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<i>priority</i>	Specifies a value of <b>0 to 7</b> to set the CoS priority for the port entered in the <i>port-string</i> . Priority value of 0 is the lowest priority.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The **set port priority** command will not change the 802.1p priority tag on tagged traffic with a default priority tag. The command only has an effect on how untagged traffic will be prioritized as it passes internally through the device.

### Example

This example shows how to set a default priority of 6 on ge.1.3. Frames received by this port without priority information in their frame header are set to the default setting of 6:

```
B5(su)->set port priority ge.1.3 6
```

## clear port priority

Use this command to reset the current CoS port priority setting to 0. This will cause all frames received without a priority value in its header to be set to priority 0.

### Syntax

```
clear port priority port-string
```

### Parameters

<i>port-string</i>	Specifies the port for which to clear priority. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset ge.1.11 to the default priority:

```
B5(rw)->clear port priority ge.1.11
```

# Configuring Priority to Transmit Queue Mapping

## Purpose

To perform the following:

- View the current priority to transmit queue mapping of each physical port.
- Configure each port to either transmit frames according to the port priority, set using the **set port priority** command described in “[set port priority](#)” on page 12-3, or according to a priority based on a percentage of port transmission capacity, assigned to transmit queues using the **set port txq** command described in “[set port txq](#)” on page 12-8.
- Clear current port priority queue settings for one or more ports.

## Commands

For information about...	Refer to page...
show port priority-queue	<a href="#">12-4</a>
set port priority-queue	<a href="#">12-5</a>
clear port priority-queue	<a href="#">12-6</a>

## show port priority-queue

Use this command to display the port priority levels (0 through 7, with 0 as the lowest level) associated with the current transmit queues (0 being the lowest priority) for each selected port. A frame with a certain port priority is transmitted according to the settings entered using the **set port priority-queue** command described in “[set port priority-queue](#)” on page 12-5.

## Syntax

```
show port priority-queue [port-string]
```

## Parameters

<i>port-string</i>	(Optional) Displays the mapping of priorities to transmit queues for one or more ports.
--------------------	---

## Defaults

If *port-string* is not specified, priority queue information for all ports will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display priority queue information for ge.1.1. In this case, frames with a priority of 0 are associated with transmit queue 1; frames with 1 or 2 priority, are associated with transmit queue 0; and so forth:

```
B5(su)->show port priority-queue ge.1.1
  Port      P0 P1 P2 P3 P4 P5 P6 P7
  -----
ge.1.1     1  0  0  2  3  4  5  5
```

# set port priority-queue

Use this command to map 802.1D (802.1p) priorities to transmit queues.

## Syntax

```
set port priority-queue port-string priority queue
```

## Parameters

<i>port-string</i>	Specifies the port(s) for which to set priority-to-queue mappings. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">"Port String Syntax Used in the CLI"</a> on page 7-1.
<i>priority</i>	Specifies a value of 0 through 7 (0 is the lowest level) that determines what priority frames will be transmitted on the transmit queue entered in this command.
<i>queue</i>	Specifies a value of 0 through 5 (0 is the lowest level) that determines the queue on which to transmit the frames with the port priority entered in this command.  <b>Note:</b> Although there are 8 queues, only queues 0 through 5 may be configured. Queues 6 and 7 are reserved for management traffic.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command enables you to change the transmit queue (0 to 5, with 0 being the lowest priority queue) for each port priority of the selected port. You can apply the new settings to one or more ports.

## Example

This example shows how to set priority 5 frames received on ge.2.12 to transmit on queue 0.

```
B5(su)->set port priority-queue ge.2.12 5 0
```

## clear port priority-queue

Use this command to reset port priority queue settings back to defaults for one or more ports.

### Syntax

```
clear port priority-queue port-string
```

### Parameters

---

<i>port-string</i>	Specifies the port for which to clear priority-to-queue mappings. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the priority queue settings on ge.2.12:

```
B5(su)->clear port priority-queue ge.2.12
```

# Configuring Quality of Service (QoS)

Refer to the “Configuring QoS” Feature Guide for detailed information about configuring quality of service on the Enterasys B5. The Enterasys Networks firmware Feature Guides are available at:

<https://extranet.enterasys.com/downloads/>

## Purpose

Eight transmit queues are implemented in the switch hardware for each port. The commands in this section allow you to set the priority mode and weight for each of the available queues (0 through 7) for each physical port on the switch. Priority mode and weight cannot be configured on LAGs, only on the physical ports that make up the LAG.

## Commands

For information about...	Refer to page...
show port txq	<a href="#">12-7</a>
set port txq	<a href="#">12-8</a>
clear port txq	<a href="#">12-8</a>

## show port txq

Use this command to display QoS transmit queue information for one or more physical ports.

### Syntax

```
show port txq [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Specifies port(s) for which to display QoS settings. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.  Only physical ports will be displayed. LAG ports have no transmit queue information.
--------------------	--

### Defaults

If the *port-string* is not specified, the QoS setting of all physical ports will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display the current algorithm and transmit queue weights configured on port ge.1.10:

```
B5(su)->show port txq ge.1.10
Port   Alg  Q0  Q1  Q2  Q3  Q4  Q5  Q6  Q7
-----
```

```
ge.1.10 WRR 10 10 15 20 25 20 0 0
```

## set port txq

Use this command to set QoS transmit queue arbitration values for physical ports.

### Syntax

```
set port txq port-string value0 value1 value2 value3 value4 value5 value6 value7
```

### Parameters

<i>port-string</i>	Specifies port(s) on which to set queue arbitration values. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.  Only physical ports can be configured with this command. LAG ports cannot be configured.
<i>value0 - value7</i>	Specifies percentage to allocate to a specific transmit queue. The values must total 100 percent.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

Queues can be set for strict priority (SP) or weighted round-robin (WRR). If set for WRR mode, weights may be assigned to those queues with this command. Weights are specified in the range of 0 to 100 percent. Weights specified for queues 0 through 7 on any port must total 100 percent.

### Examples

This example shows how to change the arbitration values for the eight transmit queues belonging to ge.1.1:

```
B5(su)->set port txq ge.1.1 10 10 10 10 10 10 10 30
```

This example shows how to change the algorithm to strict priority for the eight transmit queues belonging to ge.1.1:

```
B5(su)->set port txq ge.1.1 0 0 0 0 0 0 0 100
B5(su)->show port txq ge.1.1
Port      Alg  Q0  Q1  Q2  Q3  Q4  Q5  Q6  Q7
-----  -
ge.1.1   STR SP  SP  SP  SP  SP  SP  SP  SP
```

## clear port txq

Use this command to clear port transmit queue values back to their default values.

### Syntax

```
clear port txq port-string
```

## Parameters

---

<i>port-string</i>	<p>Clears transmit queue values on specific port(s) back to their default values. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.</p> <p>Only physical ports can be configured with this command. LAG ports cannot be configured.</p>
--------------------	--

---

## Defaults

By default, transmit queues are defined as follows:

Queue	Mode	Weight	Queue	Mode	Weight
0	WRR	1	4	WRR	5
1	WRR	2	5	WRR	6
2	WRR	3	6	WRR	7
3	WRR	4	7	WRR	8

## Mode

Switch command, read-write.

## Example

This example shows how to clear transmit queue values on ge.1.1:

```
B5(su)->clear port txq ge.1.1
```





## IGMP Configuration

This chapter describes the IGMP Configuration set of commands and how to use them.

For information about...	Refer to page...
<a href="#">IGMP Overview</a>	13-1
<a href="#">Configuring IGMP at Layer 2</a>	13-2
<a href="#">Configuring IGMP on Routing Interfaces</a>	13-10

### IGMP Overview

#### About IP Multicast Group Management

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast device. The protocol's mechanisms allow a host to inform its local device that it wants to receive transmissions addressed to a specific multicast group.

A multicast-enabled device can periodically ask its hosts if they want to receive multicast traffic. If there is more than one device on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the responsibility of querying the LAN for group members.

Based on the group membership information learned from IGMP, a device can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer-3, multicast devices use this information, along with a multicast routing protocol, to support IP multicasting across an IP network.

IGMP provides the final step in an IP multicast packet delivery service, since it is only concerned with forwarding multicast traffic from the local device to group members on a directly attached subnetwork or LAN segment.

This device supports IP multicast group management by passively snooping on the IGMP query and IGMP report packets transferred between IP multicast devices and IP multicast host groups to learn IP multicast group members.

The purpose of IP multicast group management is to optimize a switched network's performance so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast devices instead of flooding to all ports in the subnet (VLAN).

In addition to passively monitoring IGMP query and report messages, the Enterasys B5 can also actively send L3 IGMP query messages to learn locations of multicast devices and member hosts in multicast groups within each VLAN.

However, note that IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across subnetworks, multicast routing is needed if IP multicast packets have to be routed across different subnetworks.

## About Multicasting

Multicasting is used to support real-time applications such as video conferences or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed to the hosts that subscribed to this service.

## Configuring IGMP at Layer 2

The Enterasys B5 switch device uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The device looks up the IP Multicast Group used for this service and adds it to the egress list of the Level 3 interface. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.



**Note:** An Enterasys Networks Feature Guide document containing an in-depth discussion of multicast configuration is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads/>

## Purpose

To configure IGMP snooping from the switch CLI.

## Commands

For information about...	Refer to page...
show igmpsnooping	13-3
set igmpsnooping adminmode	13-3
set igmpsnooping interfacemode	13-4
set igmpsnooping groupmembershipinterval	13-4
set igmpsnooping maxresponse	13-5
set igmpsnooping mcrtexpiretime	13-6
set igmpsnooping add-static	13-6
set igmpsnooping remove-static	13-7
show igmpsnooping static	13-7
show igmpsnooping mfdb	13-8
clear igmpsnooping	13-9

## show igmpsnooping

Use this command to display IGMP snooping information.

### Syntax

```
show igmpsnooping
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Usage

Configured information is displayed whether or not IGMP snooping is enabled. Status information is displayed only when the function is enabled. For information on enabling IGMP on the system, refer to “[set igmpsnooping adminmode](#)” on page 13-3. For information on enabling IGMP on one or more ports, refer to “[set igmpsnooping interfacemode](#)” on page 13-4.

### Example

This example shows how to display IGMP snooping information:

```
B5(su)->show igmpsnooping
Admin Mode..... Enable
Group Membership Interval..... 260
Max Response Time..... 100
Multicast Router Present Expiration Time..... 0
Interfaces Enabled for IGMP Snooping..... ge.1.1.1,ge.1.2,ge.1.3
Multicast Control Frame Count..... 0
Data Frames Forwarded by the CPU..... 0 set
```

## set igmpsnooping adminmode

Use this command to enable or disable IGMP on the system.

### Syntax

```
set igmpsnooping adminmode {enable | disable}
```

### Parameters

---

<b>enable   disable</b>	Enables or disables IGMP snooping on the system.
-------------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

## Usage

In order for IGMP snooping to be enabled on one or all ports, it must be globally enabled on the device with this command, and then enabled on a port(s) using the **set igmpsnooping interface mode** command as described in “[set igmpsnooping interfacemode](#)” on page 13-4.



**Note:** IGMP snooping cannot be controlled via WebView.

## Example

This example shows how to enable IGMP on the system:

```
B5(su)->set igmpsnooping adminmode enable
```

# set igmpsnooping interfacemode

Use this command to enable or disable IGMP on one or all ports.

## Syntax

```
set igmpsnooping interfacemode port-string {enable | disable}
```

## Parameters

<i>port-string</i>	Specifies one or more ports on which to enable or disable IGMP.
<b>enable   disable</b>	Enables or disables IGMP.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

In order for IGMP snooping to be enabled on one or all ports, it must be globally enabled on the device using the **set igmpsnooping adminmode** command as described in “[set igmpsnooping adminmode](#)” on page 13-3, and then enabled on a port(s) using this command.

## Example

This example shows how to enable IGMP on port ge.1.10:

```
B5(su)->set igmpsnooping interfacemode ge.1.10 enable
```

# set igmpsnooping groupmembershipinterval

Use this command to configure the IGMP group membership interval time for the system.

## Syntax

```
set igmpsnooping groupmembershipinterval time
```

## Parameters

---

<i>time</i>	<p>Specifies the IGMP group membership interval. Valid values are <b>2 - 3600</b> seconds.</p> <p>This value works together with the <b>set igmpsnooping maxresponsetime</b> command to remove ports from an IGMP group and must be greater than the max response time value.</p>
-------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The IGMP group membership interval time sets the frequency of host-query frame transmissions and must be greater than the IGMP maximum response time as described in “[set igmpsnooping maxresponse](#)” on page 13-5.

## Example

This example shows how to set the IGMP group membership interval to 250 seconds:

```
B5(su)->set igmpsnooping groupmembershipinterval 250
```

# set igmpsnooping maxresponse

Use this command to configure the IGMP query maximum response time for the system.

## Syntax

```
set igmpsnooping maxresponse time
```

## Parameters

---

<i>time</i>	<p>Specifies the IGMP maximum query response time. Valid values are <b>100 - 255</b> seconds. The default value is 100 seconds.</p> <p>This value works together with the <b>set igmpsnooping groupmembershipinterval</b> command to remove ports from an IGMP group and must be lesser than the group membership interval value.</p>
-------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This value must be less than the IGMP maximum response time described in “[set igmpsnooping groupmembershipinterval](#)” on page 13-4.

## Example

This example shows how to set the IGMP maximum response time to 100 seconds:

```
B5(su)->set igmpsnooping maxresponse 100
```

## set igmpsnooping mcrtreptime

Use this command to configure the IGMP multicast router expiration time for the system.

### Syntax

```
set igmpsnooping mcrtreptime time
```

### Parameters

---

<i>time</i>	Specifies the IGMP multicast router expiration time. Valid values are 0 - 3600 seconds. A value of 0 will configure the system with an infinite expiration time. The default value is 0.
-------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

This timer is for expiring the switch from the multicast database. If the timer expires, and the only address left is the multicast switch, then the entry will be removed.

### Example

This example shows how to set the IGMP multicast router expiration time to infinity:

```
B5(su)->set igmpsnooping mcrtreptime 0
```

## set igmpsnooping add-static

This command creates a new static IGMP entry or adds one or more new ports to an existing entry.

### Syntax

```
set igmpsnooping add-static group vlan-list [modify] [port-string]
```

### Parameters

---

<i>group</i>	Specifies the multicast group IP address for the entry.
<i>vlan-list</i>	Specifies the VLANs on which to configure the entry.
<b>modify</b>	(Optional) Adds the specified port or ports to an existing entry.
<i>port-string</i>	(Optional) Specifies the port or ports to add to the entry.

---

### Defaults

If no ports are specified, all ports are added to the entry.

If **modify** is not specified, a new entry is created.

## Mode

Switch command, read-write.

## Usage

Use this command to create and configure static Layer 2 IGMP entries. Currently, up to 100 static groups can be configured. A total of 256 dynamic and static IGMP groups are supported.

## Example

This example creates an IGMP entry for the multicast group with IP address of 233.11.22.33 configured on VLAN 20 configured with the port ge.1.1.

```
B5(su)->set igmpsnooping add-static 233.11.22.33 20 ge.1.1
```

# set igmpsnooping remove-static

This command deletes a static IGMP entry or removes one or more new ports from an existing entry.

## Syntax

```
set igmpsnooping remove-static group vlan-list [modify] [port-string]
```

## Parameters

<i>group</i>	Specifies the multicast group IP address of the entry.
<i>vlan-list</i>	Specifies the VLANs on which the entry is configured.
<b>modify</b>	(Optional) Removes the specified port or ports from an existing entry.
<i>port-string</i>	(Optional) Specifies the port or ports to remove from the entry.

## Defaults

If no ports are specified, all ports are removed from the entry.

## Mode

Switch command, read-write.

## Example

This example removes port ge.1.1 from the entry for the multicast group with IP address of 233.11.22.33 configured on VLAN 20.

```
B5(su)->set igmpsnooping remove-static 233.11.22.33 20 ge.1.1
```

# show igmpsnooping static

This command displays static IGMP ports for one or more VLANs or IGMP groups.

## Syntax

```
show igmpsnooping static vlan-list [group group]
```

## Parameters

<i>vlan-list</i>	Specifies the VLAN for which to display static IGMP ports.
<b>group</b> <i>group</i>	(Optional) Specifies the IGMP group for which to display static IGMP ports.

## Defaults

If no group is specified, information for all groups is displayed.

## Mode

Switch command, read-only.

## Example

This example displays the static IGMP ports for VLAN 20.

```
B5(su)->show igmpsnooping static 20
-----
Vlan Id      = 20      Static Multicast Group Address = 233.11.22.33      Type = IGMP
IGMP Port List = ge.1.1
```

# show igmpsnooping mfdb

Use this command to display multicast forwarding database (MFDB) information.

## Syntax

```
show igmpsnooping mfdb [stats]
```

## Parameters

<b>stats</b>	(Optional) Displays MFDB statistics.
--------------	--------------------------------------

## Defaults

If **stats** is not specified, all MFDB table entries will be displayed.

## Mode

Switch command, read-only.

## Examples

This example shows how to display multicast forwarding database entries:

```
B5(su)->show igmpsnooping mfdb
MAC Address      Type      Description      Interfaces
-----
00:14:01:00:5E:02:CD:B0  Dynamic  Network Assist  Fwd: ge.1.1,ge.3.1,ge.4.1
00:32:01:00:5E:37:96:D0  Dynamic  Network Assist  Fwd: ge.4.7
00:32:01:00:5E:7F:FF:FA  Dynamic  Network Assist  Fwd: ge.4.7
```

This example shows how to display multicast forwarding database statistics:

```
B5(su)->show igmpsnooping mfdb stats
Max MFDB Table Entries..... 256
Most MFDB Entries Since Last Reset..... 1
Current Entries..... 0
```



---

## clear igmpsnooping

Use this command to clear all IGMP snooping entries.

### Syntax

```
clear igmpsnooping
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear all IGMP snooping entries:

```
B5(su)->clear igmpsnooping
Are you sure you want to clear all IGMP snooping entries? (y/n) y

IGMP Snooping Entries Cleared.
```

# Configuring IGMP on Routing Interfaces



**Router:** The commands covered in this section can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to [“Enabling Router Configuration Modes”](#) on page 18-2.

## Purpose

To configure IGMP on routing interfaces.

## Commands

For information about...	Refer to page...
ip igmp	<a href="#">13-10</a>
ip igmp enable	<a href="#">13-11</a>
ip igmp version	<a href="#">13-11</a>
show ip igmp interface	<a href="#">13-12</a>
show ip igmp groups	<a href="#">13-13</a>
ip igmp query-interval	<a href="#">13-13</a>
ip igmp query-max-response-time	<a href="#">13-14</a>
ip igmp startup-query-interval	<a href="#">13-14</a>
ip igmp startup-query-count	<a href="#">13-15</a>
ip igmp last-member-query-interval	<a href="#">13-15</a>
ip igmp last-member-query-count	<a href="#">13-16</a>
ip igmp robustness	<a href="#">13-16</a>

## ip igmp

Use this command to enable the L3 IGMP Querier functionality on the switch. The **no** form of this command disables IGMP Querier functionality.

### Syntax

```
ip igmp
no ip igmp
```

### Parameters

None.

### Defaults

None.

### Mode

Global configuration: B5(su)->router(Config)#

## Usage

Enabling IGMP on a routing interface requires both the `ip igmp` command (page 13-10), which enables it on the router, and the `ip igmp enable` command (page 13-11), which enables it on an interface. Once these commands are executed, the device will start sending and processing IGMP multicast traffic. IGMP is disabled by default, both globally and on a per interface basis.

## Example

This example shows how to enable IGMP on the router:

```
B5(su)->router(Config)#ip igmp
```

## ip igmp enable

Use this command to enable IGMP on an interface. The **no** form of this command disables IGMP on an interface.

### Syntax

```
ip igmp enable  
no ip igmp enable
```

### Parameters

None.

### Defaults

None.

### Usage

Enabling IGMP on a routing interface requires both the `ip igmp` command (page 13-10), which enables it on the router, and the `ip igmp enable` command (page 13-11), which enables it on an interface. Once these commands are executed, the device will start sending and processing IGMP multicast traffic. IGMP is disabled by default, both globally and on a per interface basis.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Example

This example shows how to enable IGMP on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1  
B5(su)->router(Config-if(Vlan 1))#ip igmp enable
```

## ip igmp version

Use this command to set the version of IGMP running on the router. The **no** form of this command resets IGMP to the default version of 2 (IGMPv2).

### Syntax

```
ip igmp version version  
no ip igmp
```

## Parameters

<i>version</i>	Specifies the IGMP version number to run on the router. Valid values are 1, 2, or 3.
----------------	--

## Defaults

None.

## Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Example

This example shows how to set the IGMP version to version 1 on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip igmp version 1
```

# show ip igmp interface

Use this command to display information about one or more IGMP routing interfaces.

## Syntax

```
show ip igmp interface [vlan vlan-id]
```

## Parameters

<b>vlan</b> <i>vlan-id</i>	(Optional) Displays information for one or more VLANs.
----------------------------	--

## Defaults

If not specified, information will be displayed for all VLANs configured for IGMP routing.

## Mode

Any router mode.

## Example

This example shows how to display IGMP routing information for VLAN 1:

```
B5(su)->router#show ip igmp interface vlan 1
Vlan 1 is Admin UP
Vlan 1 is Oper UP
IGMP is configured via the Switch
IGMP ACL currently not supported
Multicast TTL currently defaults to 1
IGMP Version is 2
Query Interval is 125 (secs)
Query Max Response Time is 100 (1/10 of a second)
Robustness is 2
Startup Query Interval is 31 (secs)
Startup Query Count is 2
Last Member Query Interval is 10 (1/10 of a second)
Last Member Query Count is 2
```

## show ip igmp groups

Use this command to display a list of IGMP streams and client connection ports.

### Syntax

```
show ip igmp groups
```

### Parameters

None.

### Defaults

None.

### Mode

Any router mode.

### Example

This example shows how to display information about IGMP groups:

```
B5(su)->router#show ip igmp groups
REGISTERED MULTICAST GROUP DETAILS
Multicast
IP Address          Last Reporter    Up Time Expiry Time  Host Timer          Version1
-----
228.1.1.1          12.12.12.2      27
```

## ip igmp query-interval

Use this command to set the IGMP query interval on a routing interface. The **no** form of this command resets the IGMP query interval to the default value of 125 seconds.

### Syntax

```
ip igmp query-interval time
no ip igmp query-interval
```

### Parameters

<i>time</i>	Specifies the IGMP query interval. Valid values are from <b>1</b> to <b>3600</b> seconds. Default is 125 seconds.
-------------	---

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Example

This example shows how to set the IGMP query interval to 1800 seconds on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip igmp query-interval 1800
```

## ip igmp query-max-response-time

Use this command to set the maximum response time interval advertised in IGMPv2 queries. The **no** form of this command resets the IGMP maximum response time to the default value of 100 (one tenth of a second).

### Syntax

```
ip igmp query-max-response-time time
no ip igmp query-max-response-time
```

### Parameters

---

<i>time</i>	Specifies the IGMP maximum response time interval. Valid values are from 0 to 255 tenths of a second. The default value is 100 (one tenth of a second).
-------------	---

---

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Example

This example shows how to set the IGMP query maximum response time interval to 200 (2 tenths of a second) on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip igmp query-max-response-time 200
```

## ip igmp startup-query-interval

Use this command to set the interval between general IGMP queries sent on startup. The **no** form of this command resets the IGMP startup query interval to the default value of 31 seconds.

### Syntax

```
ip igmp startup-query-interval time
no ip igmp startup-query-interval
```

### Parameters

---

<i>time</i>	Specifies the IGMP startup query interval. Valid values are from 1 to 300 seconds. The default value is 31 seconds.
-------------	---

---

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Example

This example shows how to set the IGMP startup query interval to 100 seconds on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip igmp startup-query-interval 100
```

## ip igmp startup-query-count

Use this command to set the number of IGMP queries sent out on startup, separated by the **startup-query-interval** as described in [ip igmp startup-query-interval](#) (page 13-14). The **no** form of this command resets the IGMP startup query count to the default value of 2.

### Syntax

```
ip igmp startup-query-count count
no ip igmp startup-query-count
```

### Parameters

<i>count</i>	Specifies the number of IGMP startup queries. Valid values are from 1 to 20. The default value is 2.
--------------	--

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Example

This example shows how to set the IGMP startup query count to 10 on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip igmp startup-query-count 10
```

## ip igmp last-member-query-interval

Use this command to set the maximum response time being inserted into group-specific queries sent in response to leave group messages. The **no** form of this command resets the IGMP last member query interval to the default value of 1 second.

### Syntax

```
ip igmp last-member-query-interval time
no ip igmp last-member-query-interval
```

### Parameters

<i>time</i>	Specifies the IGMP last member query interval. Valid values are from 0 to 255 seconds. The default value is 1 second.
-------------	---

### Defaults

None.

## Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Example

This example shows how to set the IGMP last member query interval to 10 seconds on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip igmp last-member-query-interval 10
```

# ip igmp last-member-query-count

Use this command to set the number of group-specific queries sent before assuming there are no local members. The **no** form of this command resets the IGMP last member query count to the default value of 2.

## Syntax

```
ip igmp last-member-query-count count
no ip igmp last-member-query-count
```

## Parameters

<i>count</i>	Specifies the number of IGMP startup queries. Valid values are from 1 to 20. The default value is 2.
--------------	--

## Defaults

None.

## Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Example

This example shows how to set the IGMP last member query count to 10 on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip igmp last-member-query-count 10
```

# ip igmp robustness

Use this command to configure the robustness tuning for expected packet loss on an IGMP routing interface. The **no** form of this command resets the IGMP robustness value to the default of 2.

## Syntax

```
ip igmp robustness robustness
no ip igmp robustness
```

## Parameters

<i>robustness</i>	Specifies the IGMP robustness value. Valid values are from 1 to 255. The default value is 2.
-------------------	--



## Defaults

None.

## Mode

Interface configuration: B5 (su)->router(Config-if(Vlan 1))#

## Usage

This value determines how many times IGMP messages will be sent. A higher number will mean that end stations will be more likely to see the packet. After the robustness value is reached, IGMP will assume there is no response to queries.

## Example

This example shows how to set the IGMP robustness value to 5 on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip igmp robustness 5
```



## Logging and Network Management

This chapter describes switch-related logging and network management commands and how to use them.



**Note:** The commands in this chapter pertain to network management of the Enterasys B5 device from the **switch CLI** only. For information on router-related network management tasks, including reviewing router ARP tables and IP traffic, refer to [Chapter 19](#).

For information about...	Refer to page...
<a href="#">Configuring System Logging</a>	<a href="#">14-1</a>
<a href="#">Monitoring Network Events and Status</a>	<a href="#">14-14</a>
<a href="#">Managing Switch Network Addresses and Routes</a>	<a href="#">14-19</a>
<a href="#">Configuring Simple Network Time Protocol (SNTP)</a>	<a href="#">14-29</a>
<a href="#">Configuring Node Aliases</a>	<a href="#">14-39</a>

### Configuring System Logging



**Note:** An Enterasys Networks Feature Guide document containing an in-depth discussion of Syslog configuration is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads/>

#### Purpose

To display and configure system logging, including Syslog server settings, Syslog default settings, and the logging buffer.

#### Commands

For information about...	Refer to page...
show logging server	<a href="#">14-2</a>
set logging server	<a href="#">14-3</a>
clear logging server	<a href="#">14-4</a>
show logging default	<a href="#">14-4</a>
set logging default	<a href="#">14-5</a>

For information about...	Refer to page...
clear logging default	<a href="#">14-6</a>
show logging application	<a href="#">14-6</a>
set logging application	<a href="#">14-7</a>
clear logging application	<a href="#">14-9</a>
show logging local	<a href="#">14-9</a>
set logging local	<a href="#">14-10</a>
clear logging local	<a href="#">14-10</a>
show logging buffer	<a href="#">14-11</a>
show logging interface	<a href="#">14-11</a>
set logging interface	<a href="#">14-12</a>
clear logging interface	<a href="#">14-13</a>

## show logging server

Use this command to display the Syslog configuration for a particular server.

### Syntax

```
show logging server [index]
```

### Parameters

<i>index</i>	(Optional) Displays Syslog information pertaining to a specific server table entry. Valid values are <b>1-8</b> .
--------------	---

### Defaults

If *index* is not specified, all Syslog server information will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display Syslog server configuration information:

```
B5(ro)->show logging server
```

IP Address	Facility	Severity	Description	Port	Status
1 132.140.82.111	local4	warning(5)	default	514	enabled
2 132.140.90.84	local4	warning(5)	default	514	enabled

[Table 14-1](#) provides an explanation of the command output.

**Table 14-1 show logging server Output Details**

Output Field	What It Displays...
IP Address	Syslog server's IP address. For details on setting this using the <b>set logging server</b> command, refer to "set logging server" on page 14-3.
Facility	Syslog facility that will be encoded in messages sent to this server. Valid values are: <b>local0</b> to <b>local7</b> .
Severity	Severity level at which the server is logging messages.
Description	Text string description of this facility/server.
Port	UDP port the client uses to send to the server.
Status	Whether or not this Syslog configuration is currently enabled or disabled.

## set logging server

Use this command to configure a Syslog server.

### Syntax

```
set logging server index [ip-addr ip-addr] [facility facility] [severity severity]
[descr descr] [port port] [state {enable | disable}]
```

### Parameters

<i>index</i>	Specifies the server table index number for this server. Valid values are <b>1 - 8</b> .
<b>ip-addr</b> <i>ip-addr</i>	(Optional) Specifies the Syslog message server's IP address.
<b>facility</b> <i>facility</i>	(Optional) Specifies the server's facility name. Valid values are: <b>local0</b> to <b>local7</b> .
<b>severity</b> <i>severity</i>	(Optional) Specifies the severity level at which the server will log messages. Valid values and corresponding levels are: <b>1</b> — emergencies (system is unusable) <b>2</b> — alerts (immediate action required) <b>3</b> — critical conditions <b>4</b> — error conditions <b>5</b> — warning conditions <b>6</b> — notifications (significant conditions) <b>7</b> — informational messages <b>8</b> — debugging messages
<b>descr</b> <i>descr</i>	(Optional) Specifies a textual string description of this facility/server.
<b>port</b> <i>port</i>	(Optional) Specifies the default UDP port the client uses to send to the server.
<b>state</b> <b>enable</b>   <b>disable</b>	(Optional) Enables or disables this facility/server configuration.

## Defaults

If **ip-addr** is not specified, an entry in the Syslog server table will be created with the specified *index* number and a message will display indicating that no IP address has been assigned.

If not specified, **facility**, severity and port will be set to defaults configured with the **set logging default** command (“[set logging default](#)” on page 14-5).

If **state** is not specified, the server will not be enabled or disabled.

## Mode

Switch command, read-write.

## Example

This command shows how to enable a Syslog server configuration for index 1, IP address 134.141.89.113, facility local4, severity level 3 on port 514:

```
B5(su)->set logging server 1 ip-addr 134.141.89.113 facility local4 severity 3
port 514 state enable
```

# clear logging server

Use this command to remove a server from the Syslog server table.

## Syntax

```
clear logging server index
```

## Parameters

---

<i>index</i>	Specifies the server table index number for the server to be removed. Valid values are 1 - 8.
--------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This command shows how to remove the Syslog server with index 1 from the server table:

```
B5(su)->clear logging server 1
```

# show logging default

Use this command to display the Syslog server default values.

## Syntax

```
show logging default
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This command shows how to display the Syslog server default values. For an explanation of the command output, refer back to [Table 14-1](#) on page 14-3.

```
B5(su)->show logging default
```

```

                Facility      Severity      Port
-----
Defaults:      local4        warning(5)   514

```

# set logging default

Use this command to set logging default values.

## Syntax

```
set logging default {[facility facility] [severity severity] port port}
```

## Parameters

<b>facility</b> <i>facility</i>	Specifies the default facility name. Valid values are: <b>local0</b> to <b>local7</b> .
<b>severity</b> <i>severity</i>	Specifies the default logging severity level. Valid values and corresponding levels are: <b>1</b> — emergencies (system is unusable) <b>2</b> — alerts (immediate action required) <b>3</b> — critical conditions <b>4</b> — error conditions <b>5</b> — warning conditions <b>6</b> — notifications (significant conditions) <b>7</b> — informational messages <b>8</b> — debugging messages
<b>port</b> <i>port</i>	Specifies the default UDP port the client uses to send to the server.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to set the Syslog default facility name to local2 and the severity level to 4 (error logging):

```
B5(su)->set logging default facility local2 severity 4
```

## clear logging default

Use this command to reset logging default values.

### Syntax

```
clear logging default {[facility] [severity] [port]}
```

### Parameters

<b>facility</b>	(Optional) Resets the default facility name to <b>local4</b> .
<b>severity</b>	(Optional) Resets the default logging severity level to <b>6</b> (notifications of significant conditions).
<b>port</b>	(Optional) Resets the default UDP port the client uses to send to the server to <b>514</b> .

### Defaults

At least one optional parameter must be entered.

All three optional keywords must be entered to reset all logging values to defaults.

### Mode

Switch command, read-write.

### Example

This example shows how to reset the Syslog default severity level to 6:

```
B5(su)->clear logging default severity
```

## show logging application

Use this command to display the severity level of Syslog messages for one or all applications configured for logging on your system.

### Syntax

```
show logging application [mnemonic | all]
```



## Parameters

<i>mnemonic</i>	(Optional) Displays severity level for one application configured for logging. Mnemonics will vary depending on the number and types of applications running on your system. Sample mnemonics and their corresponding applications are listed in <a href="#">Table 14-3</a> on page 14-8.  <b>Note:</b> Mnemonic values are case sensitive and must be typed as they appear in <a href="#">Table 14-3</a> .
<b>all</b>	(Optional) Displays severity level for all applications configured for logging.

## Defaults

If no parameter is specified, information for all applications will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display system logging information pertaining to the SNMP application.

```
B5(ro)->show logging application SNMP
```

```
Application      Current Severity Level
-----
 90      SNMP                      6

1(emergencies)  2(alerts)          3(critical)
4(errors)       5(warnings)       6(notifications)
7(information)  8(debugging)
```

[Table 14-2](#) provides an explanation of the command output.

**Table 14-2** show logging application Output Details

Output Field	What it displays...
Application	A mnemonic abbreviation of the textual description for applications being logged.
Current Severity Level	Severity level at which the server is logging messages for the listed application. This range (from 1 to 8) and its associated severity list is shown in the CLI output. For a description of these entries, which are set using the <b>set logging application</b> command, refer to “ <a href="#">set logging application</a> ” on page 14-7.

## set logging application

Use this command to set the severity level of log messages for one or all applications.

### Syntax

```
set logging application {[mnemonic | all]} [level level]
```

## Parameters

<i>mnemonic</i>	Specifies a case sensitive mnemonic abbreviation of an application to be logged. This parameter will vary depending on the number and types of applications running on your system. To display a complete list, use the <b>show logging application</b> command as described in “ <a href="#">show logging application</a> ” on page 14-6. Sample mnemonics and their corresponding applications are listed in <a href="#">Table 14-3</a> on page 14-8.  <b>Note:</b> Mnemonic values are case sensitive and must be typed as they appear in <a href="#">Table 14-3</a> .
<b>all</b>	Sets the logging severity level for all applications.
<b>level</b> <i>level</i>	(Optional) Specifies the severity level at which the server will log messages for applications. Valid values and corresponding levels are:  <ul style="list-style-type: none"> <li>1 – emergencies (system is unusable)</li> <li>2 – alerts (immediate action required)</li> <li>3 – critical conditions</li> <li>4 – error conditions</li> <li>5 – warning conditions</li> <li>6 – notifications (significant conditions)</li> <li>7 – informational messages</li> <li>8 – debugging messages</li> </ul>

**Table 14-3 Mnemonic Values for Logging Applications**

Mnemonic	Application
CLIWEB	Command Line Interface and Webview management
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
Driver	Hardware drivers
System	Non-application items such as general chassis management
Stacking	Stacking management (if applicable)
UPN	User Personalized Networking
Router	Router

## Defaults

If **level** is not specified, none will be applied.

## Mode

Switch command, read-write.

## Example

This example shows how to set the severity level for SNMP to 4 so that error conditions will be logged for that application.

```
B5(rw)->set logging application SNMP level 4
```

## clear logging application

Use this command to reset the logging severity level for one or all applications to the default value of 6 (notifications of significant conditions).

### Syntax

```
clear logging application {mnemonic | all}
```

### Parameters

<i>mnemonic</i>	Resets the severity level for a specific application to 6. Valid mnemonic values and their corresponding applications are listed in <a href="#">Table 14-3</a> on page 14-8.
<b>all</b>	Resets the severity level for all applications to 6.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to reset the logging severity level to 6 for SNMP.

```
B5(rw)->clear logging application SNMP
```

## show logging local

Use this command to display the state of message logging to the console and a persistent file.

### Syntax

```
show logging local
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

## Example

This example shows how to display the state of message logging. In this case, logging to the console is enabled and logging to a persistent file is disabled.

```
B5(su)->show logging local
Syslog Console Logging enabled
Syslog File Logging disabled
```

## set logging local

Use this command to configure log messages to the console and a persistent file.

### Syntax

```
set logging local console {enable | disable} file {enable | disable}
```

### Parameters

<b>console enable   disable</b>	Enables or disables logging to the console.
<b>file enable   disable</b>	Enables or disables logging to a persistent file.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This command shows how to enable logging to the console and disable logging to a persistent file:

```
B5(su)->set logging local console enable file disable
```

## clear logging local

Use this command to clear the console and persistent store logging for the local session.

### Syntax

```
clear logging local
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to clear local logging:

```
B5(su)->clear logging local
```

## show logging buffer

Use this command to display the last 256 messages logged. By default, critical failures and user login and logout timestamps are displayed.

### Syntax

```
show logging buffer
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

## Example

This example shows a portion of the information displayed with the **show logging buffer** command:

```
B5(su)->show logging buffer
<165>Sep  4 07:43:09 10.42.71.13 CLI[5]User:rw logged in from 10.2.1.122 (telnet)
<165>Sep  4 07:43:24 10.42.71.13 CLI[5]User: debug failed login from 10.4.1.100
(telnet)
```

## show logging interface

Use this command to display the interface used for the source IP address of the system logging.

### Syntax

```
show logging interface
```

### Parameters

None.

### Defaults

None.

### Mode

Switch mode, read-only.

## Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the system logging.

```
B5(rw)->show logging interface
loopback 1 192.168.10.1
```

## set logging interface

Use this command to specify the interface used for the source IP address of the system logging.

### Syntax

```
set logging interface {loopback loop-ID | vlan vlan-ID}
```

### Parameters

<b>loopback</b> <i>loop-ID</i>	Specifies the loopback interface to be used. The value of <i>loop-ID</i> can range from 0 to 7.
<b>vlan</b> <i>vlan-ID</i>	Specifies the VLAN interface to be used. The value of <i>vlan-ID</i> can range from 1 to 4093.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

This command allows you to configure the source IP address used by the system logging application when generating packets for management purposes. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the system logging.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface will be used.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

## Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the system logging source IP address.

```
B5(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
B5(rw)->router(Config-if(Vlan 100))#exit
```

```
B5(rw)->router(Config)#exit
B5(rw)->router#exit
B5(rw)->router>exit
B5(rw)->set logging interface vlan 100
```

```
B5(rw)->show logging interface
vlan 100 192.168.10.1
```

## clear logging interface

Use this command to clear the interface used for the source IP address of the system logging back to the default of the Host interface.

### Syntax

```
clear logging interface
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This command returns the interface used for the source IP address of the system logging back to the default of the Host interface.

```
B5(rw)->show logging interface
vlan 100 192.168.10.1
B5(rw)->clear logging interface
B5(rw)->
```

# Monitoring Network Events and Status

## Purpose

To display switch events and command history, to set the size of the history buffer, and to display and disconnect current user sessions.

## Commands

For information about...	Refer to page...
history	<a href="#">14-14</a>
show history	<a href="#">14-15</a>
set history	<a href="#">14-15</a>
ping	<a href="#">14-16</a>
show users	<a href="#">14-16</a>
disconnect	<a href="#">14-17</a>
show netstat	<a href="#">14-17</a>

## history

Use this command to display the contents of the command history buffer. The command history buffer includes all the switch commands entered up to a maximum of 100, as specified in the **set history** command (“[set history](#)” on page 14-15).

### Syntax

```
history
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the contents of the command history buffer. It shows there are five commands in the buffer:

```
B5(su)->history
 1 hist
 2 show gvrp
 3 show vlan
 4 show igmp
 5 show ip address
```



## show history

Use this command to display the size (in lines) of the history buffer.

### Syntax

```
show history
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the size of the history buffer:

```
B5(su)->show history
History buffer size: 20
```

## set history

Use this command to set the size of the history buffer.

### Syntax

```
set history size [default]
```

### Parameters

<i>size</i>	Specifies the size of the history buffer in lines. Valid values are <b>1</b> to <b>100</b> .
<b>default</b>	(Optional) Makes this setting persistent for all future sessions.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the size of the command history buffer to 30 lines:

```
B5(su)->set history 30
```

## ping

Use this command to send ICMP echo-request packets to another node on the network from the switch CLI.

### Syntax

```
ping host
```

### Parameters

---

<i>host</i>	Specifies the IP address of the device to which the <b>ping</b> will be sent.
-------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Examples

This example shows how to ping IP address 134.141.89.29. In this case, this host is alive:

```
B5(su)->ping 134.141.89.29
134.141.89.29 is alive
```

In this example, the host at IP address is not responding:

```
B5(su)->ping 134.141.89.255
no answer from 134.141.89.255
```

## show users

Use this command to display information about the active console port or Telnet session(s) logged in to the switch.

### Syntax

```
show users
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to use the **show users** command. In this output, there are two Telnet users logged in with Read-Write access privileges from IP addresses 134.141.192.119 and 134.141.192.18:

```
B5(su)->show users
  Session  User  Location
  -----
* telnet   rw    134.141.192.119
telnet     rw    134.141.192.18
```

## disconnect

Use this command to close an active console port or Telnet session from the switch CLI.

### Syntax

```
disconnect {ip-addr | console}
```

### Parameters

<i>ip-addr</i>	Specifies the IP address of the Telnet session to be disconnected. This address is displayed in the output shown in “ <a href="#">show users</a> ” on page 12-15.
<b>console</b>	Closes an active console port.

### Defaults

None.

### Mode

Switch command, read-write.

### Examples

This example shows how to close a Telnet session to host 134.141.192.119:

```
B5(su)->disconnect 134.141.192.119
```

This example shows how to close the current console session:

```
B5(su)->disconnect console
```

## show netstat

Use this command to display network layer statistics.

### Syntax

```
show netstat [icmp | ip | routes | stats | tcp | udp]
```

### Parameters

<b>icmp</b>	(Optional) Shows Internet Control Message Protocol (ICMP) statistics.
<b>ip</b>	(Optional) Shows Internet Protocol (IP) statistics.
<b>routes</b>	(Optional) Shows the IP routing table.
<b>stats</b>	(Optional) Shows all statistics for TCP, UDP, IP, and ICMP.
<b>tcp</b>	(Optional) Shows Transmission Control Protocol (TCP) statistics.
<b>udp</b>	(Optional) Shows User Datagram Protocol (UDP) statistics.

## Defaults

If no parameters are specified, **show netstat** will be executed as shown in the example below.

## Mode

Switch command, read-only.

## Example

The following example shows how to display statistics for all the current active network connections.

```
B5(su)->show netstat
Prot Local Address                Foreign Address                State
-----
TCP  127.0.0.1.2222                0.0.0.0.*                     LISTEN
TCP  0.0.0.0.80                    0.0.0.0.*                     LISTEN
TCP  0.0.0.0.23                    0.0.0.0.*                     LISTEN
TCP  10.1.56.17.23                 134.141.99.104.47718         ESTABLISHED
UDP  0.0.0.0.17185                 0.0.0.0.*                     LISTEN
UDP  127.0.0.1.49152               127.0.0.1.17185              ESTABLISHED
UDP  0.0.0.0.161                   0.0.0.0.*                     LISTEN
UDP  0.0.0.0.*                     0.0.0.0.*                     LISTEN
UDP  0.0.0.0.514                   0.0.0.0.*                     LISTEN
```

The following table describes the output of this command.

**Table 14-4 show netstat Output Details**

Output Field	What it displays...
Prot	Type of protocol running on the connection.
Local Address	IP address of the connection's local host.
Foreign Address	IP address of the connection's foreign host.
State	Communications mode of the connection.

# Managing Switch Network Addresses and Routes

## Purpose

To display or delete switch ARP table entries, and to display MAC address information.

## Commands

For information about...	Refer to page...
show arp	<a href="#">14-19</a>
set arp	<a href="#">14-20</a>
clear arp	<a href="#">14-21</a>
tracert	<a href="#">14-21</a>
show mac	<a href="#">14-22</a>
show mac agetime	<a href="#">14-23</a>
set mac agetime	<a href="#">14-24</a>
clear mac agetime	<a href="#">14-24</a>
set mac algorithm	<a href="#">14-25</a>
show mac algorithm	<a href="#">14-25</a>
clear mac algorithm	<a href="#">14-26</a>
set mac multicast	<a href="#">14-26</a>
clear mac address	<a href="#">14-27</a>
show mac unreserved-flood	<a href="#">14-28</a>
set mac unreserved-flood	<a href="#">14-28</a>

## show arp

Use this command to display the switch's ARP table.

### Syntax

```
show arp
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

## Example

This example shows how to display the ARP table:

```
B5(su)->show arp
```

```
LINK LEVEL ARP TABLE
IP Address          Phys Address      Flags  Interface
-----
10.20.1.1           00-00-5e-00-01-1  S      host
134.142.21.194     00-00-5e-00-01-1  S      host
134.142.191.192    00-00-5e-00-01-1  S      host
134.142.192.18     00-00-5e-00-01-1  S      host
134.142.192.119    00-00-5e-00-01-1  S      host
-----
```

[Table 14-5](#) provides an explanation of the command output.

**Table 14-5 show arp Output Details**

Output Field	What It Displays...
IP Address	IP address mapped to MAC address.
Phys Address	MAC address mapped to IP address.
Flags	Route status. Possible values and their definitions include: <b>S</b> - manually configured entry (static) <b>P</b> - respond to ARP requests for this entry

## set arp

Use this command to add mapping entries to the switch's ARP table.

### Syntax

```
set arp ip-address mac-address
```

### Parameters

<i>ip-address</i>	Specifies the IP address to map to the MAC address and add to the ARP table.
<i>mac-address</i>	Specifies the MAC address to map to the IP address and add to the ARP table. The MAC address can be formatted as xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to map IP address 192.168.219.232 to MAC address 00-00-0c-40-0f-bc:

```
B5(su)->set arp 192.168.219.232 00-00-0c-40-0f-bc
```

## clear arp

Use this command to delete a specific entry or all entries from the switch's ARP table.

### Syntax

```
clear arp {ip-address | all}
```

### Parameters

---

<i>ip-address</i>   <b>all</b>	Specifies the IP address in the ARP table to be cleared, or clears all ARP entries.
--------------------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to delete entry 10.1.10.10 from the ARP table:

```
B5(su)->clear arp 10.1.10.10
```

## traceroute

Use this command to display a hop-by-hop path through an IP network from the device to a specific destination host. Three UDP or ICMP probes will be transmitted for each hop between the source and the traceroute destination.

### Syntax

```
traceroute [-w waittime] [-f first-ttl] [-m max-ttl] [-p port] [-q nqueries] [-r]
[-d] [-n] [-v] host
```

### Parameters

---

<b>-w</b> <i>waittime</i>	(Optional) Specifies time in seconds to wait for a response to a probe.
<b>-f</b> <i>first-ttl</i>	(Optional) Specifies the time to live (TTL) of the first outgoing probe packet.
<b>-m</b> <i>max-ttl</i>	(Optional) Specifies the maximum time to live (TTL) used in outgoing probe packets.
<b>-p</b> <i>port</i>	(Optional) Specifies the base UDP port number used in probes.
<b>-q</b> <i>nqueries</i>	(Optional) Specifies the number of probe inquiries.
<b>-r</b>	(Optional) Bypasses the normal host routing tables.
<b>-d</b>	(Optional) Sets the debug socket option.
<b>-n</b>	(Optional) Displays hop addresses numerically. (Supported in a future release.)

---

<b>-v</b>	(Optional) Displays verbose output, including the size and destination of each response.
<i>host</i>	Specifies the host to which the route of an IP packet will be traced.

## Defaults

If not specified, *waittime* will be set to **5** seconds.

If not specified, *first-ttl* will be set to **1** second.

If not specified, *max-ttl* will be set to **30** seconds.

If not specified, *port* will be set to **33434**.

If not specified, *nqueries* will be set to **3**.

If **-r** is not specified, normal host routing tables will be used.

If **-d** is not specified, the debug socket option will not be used.

If **-v** is not specified, summary output will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to use traceroute to display a round trip path to host 192.167.252.17. In this case, hop 1 is the Enterasys B5 switch, hop 2 is 14.1.0.45, and hop 3 is back to the host IP address. Round trip times for each of the three UDP probes are displayed next to each hop:

```
B5(su)->traceroute 192.167.252.17
traceroute to 192.167.252.17 (192.167.252.17), 30 hops max, 40 byte packets
 1 matrix.enterasys.com (192.167.201.40)  20.000 ms  20.000 ms  20.000 ms
 2  14.1.0.45 (14.1.0.45)  40.000 ms  10.000 ms  20.000 ms
 3  192.167.252.17 (192.167.252.17)  50.000 ms  0.000 ms  20.000 ms
```

## show mac

Use this command to display MAC addresses in the switch's filtering database. These are addresses learned on a port through the switching process.

## Syntax

```
show mac [address mac-address] [fid fid] [port port-string] [type {other | learned
| self | mgmt | mcast}]
```

## Parameters

<b>address</b> <i>mac-address</i>	(Optional) Displays a specific MAC address (if it is known by the device).
<b>fid</b> <i>fid</i>	(Optional) Displays MAC addresses for a specific filter database identifier.
<b>port</b> <i>port-string</i>	(Optional) Displays MAC addresses for specific port(s).
<b>type</b> <b>other</b>   <b>learned</b>   <b>self</b>   <b>mgmt</b>   <b>mcast</b>	(Optional) Displays information related to <b>other</b> , <b>learned</b> , <b>self</b> , <b>mgmt</b> (management), or static multicast ( <b>mcast</b> ) address type.



## Defaults

If no parameters are specified, all MAC addresses for the device will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display MAC address information for ge.3.1:

```
B5(su)->show mac port ge.3.1
```

```

MAC Address      FID  Port          Type
-----
00-09-6B-0F-13-E6 15   ge.3.1        Learned

MAC Address      VLAN Port          Type   Status  Egress Ports
-----
01-01-23-34-45-56 20   any           mcast  perm    ge.3.1

```

[Table 14-6](#) provides an explanation of the command output.

**Table 14-6 show mac Output Details**

Output Field	What It Displays...
MAC Address	MAC addresses mapped to the port(s) shown.
FID	Filter database identifier.
Port	Port designation.
Type	Address type. Valid types are: <ul style="list-style-type: none"> <li>• Learned</li> <li>• Self</li> <li>• Management</li> <li>• Other (this will include any static MAC locked addresses as described in <a href="#">“Configuring MAC Locking”</a> on page 15-42).</li> <li>• mcast (multicast)</li> </ul>
VLAN	The VLAN ID configured for the multicast MAC address.
Status	The status of the multicast address.
Egress Ports	The ports which have been added to the egress ports list.

## show mac agetime

Use this command to display the timeout period for aging learned MAC entries.

### Syntax

```
show mac agetime
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the MAC timeout period:

```
B5(su)->show mac agetime
Aging time: 300 seconds
```

## set mac agetime

Use This command to set the timeout period for aging learned MAC entries.

### Syntax

```
set mac agetime time
```

### Parameters

---

<i>time</i>	Specifies the timeout period in seconds for aging learned MAC addresses. Valid values are 10 to 1,000,000 seconds. Default value is 300 seconds.
-------------	--

---

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to set the MAC timeout period:

```
B5(su)->set mac agetime 250
```

## clear mac agetime

Use this command to reset the timeout period for aging learned MAC entries to the default value of 300 seconds.

### Syntax

```
clear mac agetime
```

### Parameters

None.

### Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to reset the MAC timeout period to the default value of 300 seconds.

```
B5(su)->clear mac agetime
```

# set mac algorithm

Use this command to set the MAC algorithm mode, which determines the hash mechanism used by the device when performing Layer 2 lookups on received frames.

## Syntax

```
set mac algorithm {mac-crc16-lowerbits | mac-crc16-upperbits |  
mac-crc32-lowerbits | mac-crc32-upperbits}
```

## Parameters

<b>mac-crc16-lowerbits</b>	Select the MAC CRC 16 lower bits algorithm for hashing.
<b>mac-crc16-upperbits</b>	Select the MAC CRC 16 upper bits algorithm for hashing.
<b>mac-crc32-lowerbits</b>	Select the MAC CRC 32 lower bits algorithm for hashing.
<b>mac-crc32-upperbits</b>	Select the MAC CRC 32 upper bits algorithm for hashing.

## Defaults

The default MAC algorithm is **mac-crc16-upperbits**.

## Mode

Switch command, read-write.

## Usage

Each algorithm is optimized for a different spread of MAC addresses. When changing this mode, the switch will display a warning message and prompt you to restart the device.

The default MAC algorithm is mac-crc16-upperbits.

## Example

This example sets the hashing algorithm to mac-crc32-upperbits.

```
B5(rw)->set mac algorithm mac-crc32-upperbits
```

# show mac algorithm

This command displays the currently selected MAC algorithm mode.

## Syntax

```
show mac algorithm
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows the output of this command.

```
B5(su)->show mac algorithm
Mac hashing algorithm is mac-crc16-upperbits.
```

# clear mac algorithm

Use this command to return the MAC hashing algorithm to the default value of **mac-crc16-upperbits**.

## Syntax

```
clear mac algorithm
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example resets the MAC hashing algorithm to the default value.

```
B5(su)->clear mac algorithm
```

# set mac multicast

Use this command to define on what ports within a VLAN a multicast address can be dynamically learned on, or on what ports a frame with the specified MAC address can be flooded. Also, use this command to append ports to or clear ports from the egress ports list.

## Syntax

```
set mac multicast mac-address vlan-id [port-string] [{append | clear} port-string]
```

## Parameters

<i>mac-address</i>	Specifies the multicast MAC address. The MAC address can be formatted as xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.
<i>vlan-id</i>	Specifies the VLAN ID containing the ports.
<i>port-string</i>	Specifies the port or range of ports the multicast MAC address can be learned on or flooded to.
<b>append</b>   <b>clear</b>	Appends or clears the port or range of ports from the egress port list.

## Defaults

If no *port-string* is defined, the command will apply to all ports.

## Mode

Switch command, read-write.

## Example

This example configures multicast MAC address 01-01-22-33-44-55 for VLAN 24.

```
B5(su)->set mac multicast 01-01-22-33-44-55 24
```

## clear mac address

Use this command to remove a multicast MAC address.

## Syntax

```
clear mac address mac-address [vlan-id]
```

## Parameters

<i>mac-address</i>	Specifies the multicast MAC address to be cleared. The MAC address can be formatted as xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.
<i>vlan-id</i>	(Optional) Specifies the VLAN ID from which to clear the static multicast MAC address.

## Defaults

If no *vlan-id* is specified, the multicast MAC address is cleared from all VLANs.

## Mode

Switch command, read-write.

## Example

This example clears multicast MAC address 01-01-22-33-44-55 from VLAN 24.

```
B5(su)->clear mac multicast 01-01-22-33-44-55 24
```

## show mac unreserved-flood

Use this command to display the state of multicast flood protection.

### Syntax

```
show mac unreserved-flood
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example displays the status of multicast flood protection.

```
B5(su)->show mac unreserved-flood  
mac unreserved flood is disabled.
```

## set mac unreserved-flood

Use this command to enable or disable multicast flood protection. When enabled, this prevents policy profiles requiring a full 10 masks from being loaded.

### Syntax

```
set mac unreserved-flood {disable | enable}
```

### Parameters

---

<b>disable   enable</b>	Disables or enables multicast flood protection.
-------------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The following addresses will be forwarded when this function is enabled:

01:80:C2:00:00:11

01:80:C2:00:00:14

01:80:C2:00:00:15

The default state is disabled, and these addresses will not be forwarded.

## Example

This example enables multicast flood protection.

```
B5(su)->set mac unreserved-flood enable
```

# Configuring Simple Network Time Protocol (SNTP)

## Purpose

To configure the Simple Network Time Protocol (SNTP), which synchronizes device clocks in a network.



**Note:** A management IP (host, routing interface, or loopback) address must be configured for SNTP to work..

## Commands

For information about...	Refer to page...
show sntp	<a href="#">14-29</a>
set sntp client	<a href="#">14-31</a>
clear sntp client	<a href="#">14-31</a>
set sntp server	<a href="#">14-32</a>
clear sntp server	<a href="#">14-32</a>
set sntp poll-interval	<a href="#">14-33</a>
clear sntp poll-interval	<a href="#">14-33</a>
set sntp poll-retry	<a href="#">14-34</a>
clear sntp poll-retry	<a href="#">14-34</a>
set sntp poll-timeout	<a href="#">14-35</a>
clear sntp poll-timeout	<a href="#">14-35</a>
set timezone	<a href="#">14-36</a>
show sntp interface	<a href="#">14-37</a>
set sntp interface	<a href="#">14-37</a>
clear sntp interface	<a href="#">14-38</a>

## show sntp

Use this command to display SNTP client settings.

### Syntax

```
show sntp
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example shows how to display SNTP client settings:

```
B5(su)->show sntp
SNTP Version: 3
Current Time: TUE SEP 09 16:13:33 2003
Timezone: 'EST', offset from UTC is -4 hours and 0 minutes
Client Mode: unicast
Broadcast Count: 0
Poll Interval: 512 seconds
Poll Retry: 1
Poll Timeout: 5 seconds
SNTP Poll Requests: 1175
Last SNTP Update: TUE SEP 09 16:05:24 2003
Last SNTP Request: TUE SEP 09 16:05:24 2003
Last SNTP Status: Success
```

SNTP-Server	Precedence	Status
10.2.8.6	2	Active
144.111.29.19	1	Active

[Table 14-7](#) provides an explanation of the command output.

**Table 14-7 show sntp Output Details**

Output Field	What It Displays...
SNTP Version	SNTP version number.
Current Time	Current time on the system clock.
Timezone	Time zone name and amount it is offset from UTC (Universal Time). Set using the <b>set timezone</b> command (“ <a href="#">set timezone</a> ” on page 14-36).
Client Mode	Whether SNTP client is operating in unicast or broadcast mode. Set using <b>set sntp client</b> command (“ <a href="#">set sntp client</a> ” on page 14-31).
Broadcast Count	Number of SNTP broadcast frames received.
Poll Interval	Interval between SNTP unicast requests. Default of 512 seconds can be reset using the <b>set sntp poll-interval</b> command (“ <a href="#">set sntp poll-interval</a> ” on page 14-33).
Poll Retry	Number of poll retries to a unicast SNTP server. Default of 1 can be reset using the <b>set sntp poll-retry</b> command (“ <a href="#">set sntp poll-retry</a> ” on page 14-34).
Poll Timeout	Timeout for a response to a unicast SNTP request. Default of 5 seconds can be reset using <b>set sntp poll-timeout</b> command (“ <a href="#">set sntp poll-timeout</a> ” on page 14-35).
SNTP Poll Requests	Total number of SNTP poll requests.



**Table 14-7 show sntp Output Details (Continued)**

Output Field	What It Displays...
Last SNTP Update	Date and time of most recent SNTP update.
Last SNTP Request	Date and time of most recent SNTP request.
Last SNTP Status	Whether or not broadcast reception or unicast transmission and reception was successful.
SNTP-Server	IP address(es) of SNTP server(s).
Precedence	Precedence level of SNTP server in relation to its peers. Highest precedence is 1 and lowest is 10. Default of 1 can be reset using the <b>set sntp server</b> command (“ <a href="#">set sntp server</a> ” on page 14-32).
Status	Whether or not the SNTP server is active.

## set sntp client

Use this command to set the SNTP operation mode.

### Syntax

```
set sntp client {broadcast | unicast | disable}
```

### Parameters

<b>broadcast</b>	Enables SNTP in broadcast client mode.
<b>unicast</b>	Enables SNTP in unicast (point-to-point) client mode. In this mode, the client must supply the IP address from which to retrieve the current time.
<b>disable</b>	Disables SNTP.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to enable SNTP in broadcast mode:

```
B5(su)->set sntp client broadcast
```

## clear sntp client

Use this command to clear the SNTP client’s operational mode.

### Syntax

```
clear sntp client
```

### Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear the SNTP client's operational mode:

```
B5(su)->clear sntp client
```

# set sntp server

Use this command to add a server from which the SNTP client will retrieve the current time when operating in unicast mode. Up to 10 servers can be set as SNTP servers.

## Syntax

```
set sntp server ip-address [precedence]
```

## Parameters

<i>ip-address</i>	Specifies the SNTP server's IP address.
<i>precedence</i>	(Optional) Specifies this SNTP server's precedence in relation to its peers. Valid values are 1 (highest) to 10 (lowest).

## Defaults

If *precedence* is not specified, 1 will be applied.

## Mode

Switch command, read-write.

## Example

This example shows how to set the server at IP address 10.21.1.100 as an SNTP server:

```
B5(su)->set sntp server 10.21.1.100
```

# clear sntp server

Use this command to remove one or all servers from the SNTP server list.

## Syntax

```
clear sntp server {ip-address | all}
```

## Parameters

<i>ip-address</i>	Specifies the IP address of a server to remove from the SNTP server list.
<b>all</b>	Removes all servers from the SNTP server list.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to remove the server at IP address 10.21.1.100 from the SNTP server list:

```
B5(su)->clear sntp server 10.21.1.100
```

# set sntp poll-interval

Use this command to set the poll interval between SNTP unicast requests.

## Syntax

```
set sntp poll-interval value
```

## Parameters

<i>value</i>	The poll interval is 2 to the power of <i>value</i> in seconds, where <i>value</i> can range from 6 to 10.
--------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to set the SNTP poll interval to 64 seconds:

```
B5(su)->set sntp poll-interval 6
```

# clear sntp poll-interval

Use this command to clear the poll interval between unicast SNTP requests.

## Syntax

```
clear sntp poll-interval
```

## Parameters

None.

## Defaults

None.

**Mode**

Switch command, read-write.

**Example**

This example shows how to clear the SNTP poll interval:

```
B5(su)->clear sntp poll-interval
```

## set sntp poll-retry

Use this command to set the number of poll retries to a unicast SNTP server.

**Syntax**

```
set sntp poll-retry retry
```

**Parameters**

---

<i>retry</i>	Specifies the number of retries. Valid values are <b>0</b> to <b>10</b> .
--------------	---

---

**Defaults**

None.

**Mode**

Switch command, read-write.

**Example**

This example shows how to set the number of SNTP poll retries to 5:

```
B5(su)->set sntp poll-retry 5
```

## clear sntp poll-retry

Use this command to clear the number of poll retries to a unicast SNTP server.

**Syntax**

```
clear sntp poll-retry
```

**Parameters**

None.

**Defaults**

None.

**Mode**

Switch command, read-write.

## Example

This example shows how to clear the number of SNTP poll retries:

```
B5(su)->clear sntp poll-retry
```

## set sntp poll-timeout

Use this command to set the poll timeout (in seconds) for a response to a unicast SNTP request.

### Syntax

```
set sntp poll-timeout timeout
```

### Parameters

---

<i>timeout</i>	Specifies the poll timeout in seconds. Valid values are <b>1</b> to <b>30</b> .
----------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the SNTP poll timeout to 10 seconds:

```
B5(su)->set sntp poll-timeout 10
```

## clear sntp poll-timeout

Use this command to clear the SNTP poll timeout.

### Syntax

```
clear sntp poll-timeout
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the SNTP poll timeout:

```
B5(su)->clear sntp poll-timeout
```

## set timezone

Use this command to configure the current timezone as an offset from UTC.

### Syntax

```
set timezone name [hours] [minutes]
```

### Parameters

<i>name</i>	The name of the timezone. Typically, this name is a standard abbreviation such as EST (Eastern Standard Time) or EDT (Eastern Daylight Time).
<i>hours</i>	(Optional) Specifies the offset in hours from UTC. The value can range from -13 to 13. The default is 0 hours.
<i>minutes</i>	(Optional) Specifies additional offset in minutes from UTC. The value can range from 0 to 59. The default is 0 minutes.

### Defaults

If you enter a timezone name without specifying an offset in hours and minutes, the default is an offset from UTC of 0 hours and 0 minutes.

### Mode

Switch command, read-write.

### Usage

Typically, this command is used to configure the local timezone offset from UTC (Universal Time) when SNTP is used to synchronize the time used by devices on the network.

To display the current timezone setting used by SNTP, use the **show sntp** command. To clear an existing offset to zero, enter the command without specifying any hours or minutes.

Standard timezone names and offsets can be found at the following URL, among others:

<http://www.timeanddate.com/library/abbreviations/timezones/>

### Example

The following example sets the timezone name to EST and the offset to North American Eastern Standard Time offset of -5 hours from UTC, then displays the timezone used with SNTP.

```
B5(su)->set timezone EST -5

B5(su)->show sntp
SNTP Version: 3
Current Time: WED JUL 16 11:35:52 2008
Timezone: 'EST' offset from UTC is -5 hours and 0 minutes
Client Mode: unicast
Broadcast Count: 0
Poll Interval: 6 (64 seconds)
Poll Retry: 1
Poll Timeout: 5 seconds
SNTP Poll Requests: 2681
Last SNTP Update: WED JUL 16 16:35:23 2008
Last SNTP Request: WED JUL 16 16:35:23 2008
Last SNTP Status: Success
```

SNTP-Server	Precedence	Status
192.255.255.254	2	Active

## show sntp interface

Use this command to display the interface used for the source IP address of the SNTP client.

### Syntax

```
show sntp interface
```

### Parameters

None.

### Defaults

None.

### Mode

Switch mode, read-only.

### Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the SNTP client.

```
B5(rw)->show sntp interface
loopback 1 192.168.10.1
```

## set sntp interface

Use this command to specify the interface used for the source IP address of the SNTP client.

### Syntax

```
set sntp interface {loopback loop-ID | vlan vlan-ID}
```

### Parameters

<b>loopback</b> <i>loop-ID</i>	Specifies the loopback interface to be used. The value of <i>loop-ID</i> can range from 0 to 7.
<b>vlan</b> <i>vlan-ID</i>	Specifies the VLAN interface to be used. The value of <i>vlan-ID</i> can range from 1 to 4093.

### Defaults

None.

### Mode

Switch command, read-write.

## Usage

This command allows you to configure the source IP address used by the SNTP application when generating packets for management purposes. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the SNTP client.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface will be used.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

## Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the SNTP client source IP address.

```
B5(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
B5(rw)->router(Config-if(Vlan 100))#exit
B5(rw)->router(Config)#exit
B5(rw)->router#exit
B5(rw)->router>exit
B5(rw)->set sntp interface vlan 100

B5(rw)->show sntp interface
vlan 100 192.168.10.1
```

## clear sntp interface

Use this command to clear the interface used for the source IP address of the SNTP client back to the default of the Host interface.

### Syntax

```
clear sntp interface
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.



## Example

This command returns the interface used for the source IP address of the SNTP client back to the default of the Host interface.

```
B5(rw)->show sntp interface
vlan 100 192.168.10.1
B5(rw)->clear sntp interface
B5(rw)->
```

## Configuring Node Aliases

The node alias feature enables administrators to determine the MAC address and location of a given end-station (or node) using the node's Layer 3 alias information (IP address) as a key. With this method, it is possible to determine that, for instance, IP address 123.145.2.23 is located on switch 5 port 3.

The passive accumulation of a network's node/alias information is accomplished by "snooping" on the contents of network traffic as it passes through the switch fabric.

In the B5, node data is automatically accumulated into the ct-alias mib, and by default this feature is enabled. The NetSight Console Compass utility and Automated Security Manager (ASM) use the information in the node/alias MIB table.

It's important to make sure that inter-switch links are not learning node/alias information, as it would slow down searches by the NetSight Compass and ASM tools and give inaccurate results.

## Purpose

To review, disable, and re-enable node (port) alias functionality on the switch.

## Commands

For information about...	Refer to page...
show nodealias config	<a href="#">14-39</a>
set nodealias	<a href="#">14-40</a>
clear nodealias config	<a href="#">14-41</a>

## show nodealias config

Use this command to display node alias configuration settings on one or more ports.

### Syntax

```
show nodealias config [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays node alias configuration settings for specific port(s).
--------------------	---

## Defaults

If *port-string* is not specified, node alias configurations will be displayed for all ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display node alias configuration settings for ports ge.2.1 through 9:

```
B5(rw)->show nodealias config ge.2.1-9
Port Number          Max Entries          Used Entries          Status
-----
ge.2.1               16                   0                    Enable
ge.2.2               47                   0                    Enable
ge.2.3               47                   2                    Enable
ge.2.4               47                   0                    Enable
ge.2.5               47                   0                    Enable
ge.2.6               47                   2                    Enable
ge.2.7               47                   0                    Enable
ge.2.8               47                   0                    Enable
ge.2.9               4000                 1                    Enable
```

[Table 14-8](#) provides an explanation of the command output.

**Table 14-8 show nodealias config Output Details**

Output Field	What It Displays...
Port Number	Port designation.
Max Entries	Maximum number of alias entries configured for this port.
Used Entries	Number of alias entries (out of the maximum amount configured) already used by this port.
Status	Whether or not a node alias agent is enabled (default) or disabled on this port.

## set nodealias

Use this command to enable or disable a node alias agent on one or more ports, or set the maximum number of alias entries stored per port.

### Syntax

```
set nodealias {enable | disable | maxentries maxentries} port-string
```

### Parameters

<b>enable</b>   <b>disable</b>	Enables or disables a node alias agent.
<b>maxentries</b> <i>maxentries</i>	Set the maximum number of alias entries stored per port. Valid range is 0 to 4096. The default value is 32.
<i>port-string</i>	Specifies the port(s) on which to enable/disable node alias agent or set a maximum number of stored entries.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

Upon packet reception, node aliases are dynamically assigned to ports enabled with an alias agent, which is the default setting on Enterasys B5 devices. Node aliases cannot be statically created, but can be deleted using the command "[clear nodealias config](#)" (page 14-41).

It's important to make sure that inter-switch links are not learning node/alias information, as it would slow down searches by the NetSight Compass and ASM tools and give inaccurate results.

## Example

This example shows how to disable the node alias agent on ge.1.3:

```
B5(su)->set nodealias disable ge.1.3
```

# clear nodealias config

Use this command to reset node alias state to enabled and clear the maximum entries value.

## Syntax

```
clear nodealias config port-string
```

## Parameters

---

<i>port-string</i>	Specifies the port(s) on which to reset the node alias configuration.
--------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the node alias configuration on ge.1.3:

```
B5(su)->clear nodealias config ge.1.3
```



## RMON Configuration

This chapter describes the commands used to configure RMON on a Enterasys B5 switch.

For information about...	Refer to page...
<a href="#">RMON Monitoring Group Functions</a>	15-1
<a href="#">Design Considerations</a>	15-2
<a href="#">Statistics Group Commands</a>	15-3
<a href="#">History Group Commands</a>	15-6
<a href="#">Alarm Group Commands</a>	15-9
<a href="#">Event Group Commands</a>	15-13
<a href="#">Filter Group Commands</a>	15-17
<a href="#">Packet Capture Commands</a>	15-22

### RMON Monitoring Group Functions

RMON (Remote Network Monitoring) provides comprehensive network fault diagnosis, planning, and performance tuning information and allows for interoperability between SNMP management stations and monitoring agents. RMON extends the SNMP MIB capability by defining additional MIBs that generate a much richer set of data about network usage. These MIB “groups” each gather specific sets of data to meet common network monitoring requirements.

[Table 15-1](#) lists the RMON monitoring groups supported on Enterasys B5 devices, each group’s function and the elements it monitors, and the associated configuration commands needed.

**Table 15-1 RMON Monitoring Group Functions and Commands**

RMON Group	What It Does...	What It Monitors...	CLI Command(s)
Statistics	Records statistics measured by the RMON probe for each monitored interface on the device.	Packets dropped, packets sent, bytes sent (octets), broadcast and multicast packets, CRC errors, oversized and undersized packets, fragments, jabbers, and counters for packets.	<p>“<a href="#">show rmon stats</a>” on page 15-4</p> <p>“<a href="#">set rmon stats</a>” on page 15-4</p> <p>“<a href="#">clear rmon stats</a>” on page 15-5</p>

**Table 15-1 RMON Monitoring Group Functions and Commands (Continued)**

RMON Group	What It Does...	What It Monitors...	CLI Command(s)
History	Records periodic statistical samples from a network.	Sample period, number of samples and item(s) sampled.	<a href="#">“show rmon history”</a> on page 15-6 <a href="#">“set rmon history”</a> on page 15-7 <a href="#">“clear rmon history”</a> on page 15-7
Alarm	Periodically gathers statistical samples from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.	Alarm type, interval, starting threshold, stop threshold.	<a href="#">“show rmon alarm”</a> on page 15-9 <a href="#">“set rmon alarm properties”</a> on page 15-10 <a href="#">“set rmon alarm status”</a> on page 15-11 <a href="#">“clear rmon alarm”</a> on page 15-12
Event	Controls the generation and notification of events from the device.	Event type, description, last time event was sent.	<a href="#">“show rmon event”</a> on page 15-13 <a href="#">“set rmon event properties”</a> on page 15-14 <a href="#">“set rmon event status”</a> on page 15-15 <a href="#">“clear rmon event”</a> on page 15-15
Filter	Allows packets to be matched by a filter equation. These matched packets form a data stream or “channel” that may be captured.	Packets matching the filter configuration.	<a href="#">“show rmon channel”</a> on page 15-17 <a href="#">“set rmon channel”</a> on page 15-18 <a href="#">“clear rmon channel”</a> on page 15-19 <a href="#">“show rmon filter”</a> on page 15-19 <a href="#">“set rmon filter”</a> on page 15-20 <a href="#">“clear rmon filter”</a> on page 15-21
Packet Capture	Allows packets to be captured upon a filter match.	Packets matching the filter configuration.	<a href="#">“show rmon capture”</a> on page 15-22 <a href="#">“set rmon capture”</a> on page 15-23 <a href="#">“clear rmon capture”</a> on page 15-24

## Design Considerations

The B5 supports RMON Packet Capture/Filter Sampling through both the CLI and MIBs, but with the following constraints:

- RMON Packet Capture/Filter Sampling and Port Mirroring cannot be enabled on the same interface concurrently.
- You can capture a total of 100 packets on an interface, no more and no less.
  - The captured frames will be as close to sequential as the hardware will allow.
  - Only one interface can be configured for capturing at a time.
  - Once 100 frames have been captured by the hardware, the application will stop without manual intervention.
- As described in the MIB, the filter is only applied after the frame is captured, thus only a subset of the frames captured will be available for display.
- There is only one Buffer Control Entry supported.
- Due to the limitations of the hardware, the Buffer Control Entry table will have limits on a few of its elements:
  - MaxOctetsRequested can only be set to the value -1 which indicates the application will capture as many packets as possible given its restrictions.
  - CaptureSliceSize can only be set to 1518.
  - The Full Action element can only be set to “lock” since the device does not support wrapping the capture buffer.
- Due to hardware limitations, the only frame error counted is oversized frames.
- The application does not support Events. Therefore, the following elements of the Channel Entry Table are not supported: TurnOnEventIndex, TurnOffEventIndex, EventIndex, and EventStatus.
- There is only one Channel Entry available at a time.
  - There are only three Filter Entries available, and a user can associate all three Filter Entries with the Channel Entry.
- Configured channel, filter, and buffer information will be saved across resets, but not frames within the capture buffer.

## Statistics Group Commands

### Purpose

To display, configure, and clear RMON statistics.



**Note:** Due to hardware limitations, the only frame error counted is oversized frames.

### Commands

For information about...	Refer to page...
show rmon stats	<a href="#">15-4</a>
set rmon stats	<a href="#">15-4</a>
clear rmon stats	<a href="#">15-5</a>

## show rmon stats

Use this command to display RMON statistics measured for one or more ports.

### Syntax

```
show rmon stats [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays RMON statistics for specific port(s).
--------------------	---

---

### Defaults

If *port-string* is not specified, RMON stats will be displayed for all ports.

### Mode

Switch command, read-only.

### Example

This example shows how to display RMON statistics for Gigabit Ethernet port 1 in switch 1.

```
B5(su)->show rmon stats ge.1.1
```

```
Port: ge.1.1
```

```
-----
Index          = 1
Owner          = monitor
Data Source    = ifIndex.1

Drop Events    = 0          Packets          = 0
Collisions    = 0          Octets          = 0
Jabbers       = 0          0 - 64 Octets = 0
Broadcast Pkts = 0          65 - 127 Octets = 0
Multicast Pkts = 0          128 - 255 Octets = 0
CRC Errors     = 0          256 - 511 Octets = 0
Undersize Pkts = 0          512 - 1023 Octets = 0
Oversize Pkts = 0          1024 - 1518 Octets = 0
Fragments     = 0
```

[Table 15-2](#) provides an explanation of the command output.

## set rmon stats

Use this command to configure an RMON statistics entry.

### Syntax

```
set rmon stats index port-string [owner]
```

### Parameters

---

<i>index</i>	Specifies an index for this statistics entry.
<i>port-string</i>	Specifies port(s) to which this entry will be assigned.
<i>owner</i>	(Optional) Assigns an owner for this entry.

---



## Defaults

If *owner* is not specified, **monitor** will be applied.

## Mode

Switch command, read-write.

## Example

This example shows how to configure RMON statistics entry 2 for ge.1.20:

```
B5(rw)->set rmon stats 2 ge.1.20
```

# clear rmon stats

Use this command to delete one or more RMON statistics entries.

## Syntax

```
clear rmon stats {index-list / to-defaults}
```

## Parameters

<i>index-list</i>	Specifies one or more stats entries to be deleted, causing them to disappear from any future RMON queries.
<b>to-defaults</b>	Resets all history entries to default values. This will cause entries to reappear in RMON queries.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to delete RMON statistics entry 2:

```
B5(rw)->clear rmon stats 2
```

# History Group Commands

## Purpose

To display, configure, and clear RMON history properties and statistics.

## Commands

For information about...	Refer to page...
show rmon history	<a href="#">15-6</a>
set rmon history	<a href="#">15-7</a>
clear rmon history	<a href="#">15-7</a>

## show rmon history

Use this command to display RMON history properties and statistics. The RMON history group records periodic statistical samples from a network.

### Syntax

```
show rmon history [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays RMON history entries for specific port(s).
--------------------	--

### Defaults

If *port-string* is not specified, information about all RMON history entries will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display RMON history entries for Gigabit Ethernet port 1 in switch 1. A control entry displays first, followed by actual entries corresponding to the control entry. In this case, the default settings for entry owner, sampling interval, and maximum number of entries (buckets) have not been changed from their default values. For a description of the types of statistics shown, refer to [Table 15-2](#).

```
B5(su)->show rmon history ge.1.1
```

```
Port: ge.1.1
```

```
-----
Index 1
Owner           = monitor
Status          = valid
Data Source     = ifIndex.1
Interval        = 30
Buckets Requested = 50
Buckets Granted  = 10
```

```

Sample 2779          Interval Start: 1 days 0 hours 2 minutes 22 seconds
Drop Events         = 0          Undersize Pkts         = 0
Octets              = 0          Oversize Pkts         = 0
Packets            = 0          Fragments             = 0
Broadcast Pkts     = 0          Jabbers               = 0
Multicast Pkts     = 0          Collisions            = 0
CRC Align Errors   = 0          Utilization(%)       = 0

```

## set rmon history

Use this command to configure an RMON history entry.

### Syntax

```
set rmon history index [port-string] [buckets buckets] [interval interval] [owner owner]
```

### Parameters

<i>index-list</i>	Specifies an index number for this entry.
<i>port-string</i>	(Optional) Assigns this entry to a specific port.
<b>buckets</b> <i>buckets</i>	(Optional) Specifies the maximum number of entries to maintain.
<b>interval</b> <i>interval</i>	(Optional) Specifies the sampling interval in seconds.
<b>owner</b> <i>owner</i>	(Optional) Specifies an owner for this entry.

### Defaults

If *buckets* is not specified, the maximum number of entries maintained will be 50.

If not specified, *interval* will be set to 30 seconds.

If *owner* is not specified, **monitor** will be applied.

### Mode

Switch command, read-write.

### Example

This example shows how configure RMON history entry 1 on port ge.2.1 to sample every 20 seconds:

```
B5(rw)->set rmon history 1 ge.2.1 interval 20
```

## clear rmon history

Use this command to delete one or more RMON history entries or reset one or more entries to default values. For specific values, refer to “[set rmon history](#)” on page 15-7.

### Syntax

```
clear rmon history {index-list | to-defaults}
```

## Parameters

---

<i>index-list</i>	Specifies one or more history entries to be deleted, causing them to disappear from any future RMON queries.
<b>to-defaults</b>	Resets all history entries to default values. This will cause entries to reappear in RMON queries.

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to delete RMON history entry 1:

```
B5(rw)->clear rmon history 1
```

# Alarm Group Commands

## Purpose

To display, configure, and clear RMON alarm entries and properties.

## Commands

For information about...	Refer to page...
show rmon alarm	<a href="#">15-9</a>
set rmon alarm properties	<a href="#">15-10</a>
set rmon alarm status	<a href="#">15-11</a>
clear rmon alarm	<a href="#">15-12</a>

## show rmon alarm

Use this command to display RMON alarm entries. The RMON alarm group periodically takes statistical samples from RMON variables and compares them with previously configured thresholds. If the monitored variable crosses a threshold an RMON event is generated.

### Syntax

```
show rmon alarm [index]
```

### Parameters

<i>index</i>	(Optional) Displays RMON alarm entries for a specific entry index ID.
--------------	---

### Defaults

If *index* is not specified, information about all RMON alarm entries will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display RMON alarm entry 3:

```
B5(rw)->show rmon alarm 3
Index 3
-----
Owner           = Manager
Status          = valid
Variable        = 1.3.6.1.4.1.5624.1.2.29.1.2.1.0
Sample Type     = delta           Startup Alarm     = rising
Interval       = 30              Value           = 0
Rising Threshold = 1              Falling Threshold = 0
Rising Event Index = 2          Falling Event Index = 0
```

[Table 15-2](#) provides an explanation of the command output.

**Table 15-2 show rmon alarm Output Details**

Output Field	What It Displays...
Index	Index number for this alarm entry.
Owner	Text string identifying who configured this entry.
Status	Whether this event entry is enabled (valid) or disabled.
Variable	MIB object to be monitored.
Sample Type	Whether the monitoring method is an absolute or a delta sampling.
Startup Alarm	Whether alarm generated when this entry is first enabled is rising, falling, or either.
Interval	Interval in seconds at which RMON will conduct sample monitoring.
Rising Threshold	Minimum threshold for causing a rising alarm.
Falling Threshold	Maximum threshold for causing a falling alarm.
Rising Event Index	Index number of the RMON event to be triggered when the rising threshold is crossed.
Falling Event Index	Index number of the RMON event to be triggered when the falling threshold is crossed.


## set rmon alarm properties

Use this command to configure an RMON alarm entry, or to create a new alarm entry with an unused alarm index number.

### Syntax

```
set rmon alarm properties index [interval interval] [object object] [type
{absolute | delta}] [startup {rising | falling | either}] [rthresh rthresh]
[fthresh fthresh] [revent revent] [fevent fevent] [owner owner]
```

### Parameters

<i>index</i>	Specifies an index number for this entry. Maximum number of entries is 50. Maximum value is 65535.
<b>interval</b> <i>interval</i>	(Optional) Specifies an interval (in seconds) for RMON to conduct sample monitoring.
<b>object</b> <i>object</i>	(Optional) Specifies a MIB object to be monitored.
	 <b>Note:</b> This parameter is not mandatory for executing the command, but must be specified in order to enable the alarm entry configuration.
<b>type</b> <b>absolute</b>   <b>delta</b>	(Optional) Specifies the monitoring method as: sampling the absolute value of the object, or the difference (delta) between object samples.

<b>startup</b> <i>rising</i>   <b>falling</b>   <b>either</b>	(Optional) Specifies the type of alarm generated when this event is first enabled as: <ul style="list-style-type: none"> <li>• Rising - Sends alarm when an RMON event reaches a maximum threshold condition is reached, for example, more than 30 collisions per second.</li> <li>• Falling - Sends alarm when RMON event falls below a minimum threshold condition, for example when the network is behaving normally again.</li> <li>• Either - Sends alarm when either a rising or falling threshold is reached.</li> </ul>
<b>rthresh</b> <i>rthresh</i>	(Optional) Specifies a minimum threshold for causing a rising alarm.
<b>fthresh</b> <i>fthresh</i>	Specifies a maximum threshold for causing a falling alarm.
<b>revent</b> <i>revent</i>	Specifies the index number of the RMON event to be triggered when the rising threshold is crossed.
<b>fevent</b> <i>fevent</i>	Specifies the index number of the RMON event to be triggered when the falling threshold is crossed.
<b>owner</b> <i>owner</i>	(Optional) Specifies the name of the entity that configured this alarm entry.

## Defaults

interval - **3600** seconds

type - **absolute**

startup - **rising**

rthresh - **0**

fthresh - **0**

revent - **0**

fevent - **0**

owner - **monitor**

## Mode

Switch command, read-write.

## Example

This example shows how to configure a rising RMON alarm. This entry will conduct monitoring of the delta between samples every 30 seconds:

```
B5(rw)->set rmon alarm properties 3 interval 30 object
1.3.6.1.4.1.5624.1.2.29.1.2.1.0 type delta rthresh 1 revent 2 owner Manager
```

## set rmon alarm status

Use this command to enable an RMON alarm entry. An alarm is a notification that a statistical sample of a monitored variable has crossed a configured threshold.

## Syntax

```
set rmon alarm status index enable
```

## Parameters

---

<i>index</i>	Specifies an index number for this entry. Maximum number of entries is 50. Maximum value is <b>65535</b> .
<b>enable</b>	Enables this alarm entry.

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

An RMON alarm entry can be created using this command, configured using the **set rmon alarm properties** command ([“set rmon alarm properties” on page 15-10](#)), then enabled using this command. An RMON alarm entry can be created and configured at the same time by specifying an unused index with the **set rmon alarm properties** command.

## Example

This example shows how to enable RMON alarm entry 3:

```
B5(rw)->set rmon alarm status 3 enable
```

# clear rmon alarm

Use this command to delete an RMON alarm entry.

## Syntax

```
clear rmon alarm index
```

## Parameters

---

<i>index</i>	Specifies the index number of entry to be cleared.
--------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear RMON alarm entry 1:

```
B5(rw)->clear rmon alarm 1
```



# Event Group Commands

## Purpose

To display and clear RMON events, and to configure RMON event properties.

## Commands

For information about...	Refer to page...
show rmon event	<a href="#">15-13</a>
set rmon event properties	<a href="#">15-14</a>
set rmon event status	<a href="#">15-15</a>
clear rmon event	<a href="#">15-15</a>

## show rmon event

Use this command to display RMON event entry properties.

### Syntax

```
show rmon event [index]
```

### Parameters

<i>index</i>	(Optional) Displays RMON properties and log entries for a specific entry index ID.
--------------	--

### Defaults

If *index* is not specified, information about all RMON entries will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display RMON event entry 3:

```
B5(rw)->show rmon event 3
Index 3
-----
Owner          = Manager
Status         = valid
Description    = STP Topology change
Type           = log-and-trap
Community      = public
Last Time Sent = 0 days 0 hours 0 minutes 37 seconds
```

[Table 15-3](#) provides an explanation of the command output.

**Table 15-3 show rmon event Output Details**

Output Field	What It Displays...
Index	Index number for this event entry.
Owner	Text string identifying who configured this entry.
Status	Whether this event entry is enabled (valid) or disabled.
Description	Text string description of this event.
Type	Whether the event notification will be a log entry, and SNMP trap, both, or none.
Community	SNMP community name if message type is set to trap.
Last Time Sent	When an event notification matching this entry was sent.

## set rmon event properties

Use this command to configure an RMON event entry, or to create a new event entry with an unused event index number.

### Syntax

```
set rmon event properties index [description description] [type {none | log | trap | both}] [community community] [owner owner]
```

### Parameters

<i>index</i>	Specifies an index number for this entry. Maximum number of entries is 100. Maximum value is <b>65535</b> .
<b>description</b> <i>description</i>	(Optional) Specifies a text string description of this event.
<b>type</b> <i>none</i>   <i>log</i>   <i>trap</i>   <i>both</i>	(Optional) Specifies the type of RMON event notification as: none, a log table entry, an SNMP trap, or both a log entry and a trap message.
<b>community</b> <i>community</i>	(Optional) Specifies an SNMP community name to use if the message type is set to <b>trap</b> . For details on setting SNMP traps and community names, refer to “ <a href="#">Creating a Basic SNMP Trap Configuration</a> ” on page 8-36.
<b>owner</b> <i>owner</i>	(Optional) Specifies the name of the entity that configured this entry.

### Defaults

If **description** is not specified, none will be applied.

If not specified, **type none** will be applied.

If *owner* is not specified, **monitor** will be applied.

### Mode

Switch command, read-write.

## Example

This example shows how to create and enable an RMON event entry called “STP topology change” that will send both a log entry and an SNMP trap message to the “public” community:

```
B5(rw)->set rmon event properties 2 description "STP topology change" type both
community public owner Manager
```

## set rmon event status

Use this command to enable an RMON event entry. An event entry describes the parameters of an RMON event that can be triggered. Events can be fired by RMON alarms and can be configured to create a log entry, generate a trap, or both.

### Syntax

```
set rmon event status index enable
```

### Parameters

<i>index</i>	Specifies an index number for this entry. Maximum number of entries is 100. Maximum value is <b>65535</b> .
<b>enable</b>	Enables this event entry.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

An RMON event entry can be created using this command, configured using the **set rmon event properties** command (“[set rmon event properties](#)” on page 15-14), then enabled using this command. An RMON event entry can be created and configured at the same time by specifying an unused index with the **set rmon event properties** command.

### Example

This example shows how to enable RMON event entry 1:

```
B5(rw)->set rmon event status 1 enable
```

## clear rmon event

Use this command to delete an RMON event entry and any associated log entries.

### Syntax

```
clear rmon event index
```

### Parameters

<i>index</i>	Specifies the index number of the entry to be cleared.
--------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear RMON event 1:

```
B5(rw)->clear rmon event 1
```

## Filter Group Commands

The packet capture and filter function is disabled by default. Only one interface can be configured for capturing and filtering at a time.

When packet capture is enabled on an interface, the Enterasys B5 switch will capture 100 frames as close to sequentially as possible. These 100 frames will be placed into a buffer for inspection. If there is data in the buffer when the function is started, the buffer will be overwritten. Once 100 frames have been captured, the capture will stop. Filtering will be performed on the frames captured in the buffer. Therefore, only a subset of the frames captured will be available for display.



**Note:** Packet capture is sampling only and does not guarantee receipt of back to back packets.

One channel at a time can be supported, with up to three filters. Configured channel, filter, and buffer control information will be saved across resets, but captured frames within the buffer will not be saved.

This function cannot be used concurrently with port mirroring. The system will check to prevent concurrently enabling both functions, and a warning will be generated in the CLI if attempted.

## Commands

For information about...	Refer to page...
show rmon channel	<a href="#">15-17</a>
set rmon channel	<a href="#">15-18</a>
clear rmon channel	<a href="#">15-19</a>
show rmon filter	<a href="#">15-19</a>
set rmon filter	<a href="#">15-20</a>
clear rmon filter	<a href="#">15-21</a>

## show rmon channel

Use this command to display RMON channel entries for one or more ports.

### Syntax

```
show rmon channel [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays RMON channel entries for a specific port(s).
--------------------	--

### Defaults

If *port-string* is not specified, information about all channels will be displayed.

### Mode

Switch command, read-only.

## Example

This example shows how to display RMON channel information for ge.2.12:

```
B5(rw)->show rmon channel ge.2.12
Port ge.2.12      Channel index= 628      EntryStatus= valid
-----
Control           off           AcceptType       matched
OnEventIndex     0            OffEventIndex    0
EventIndex       0            Status           ready
Matches          4498
Description      Thu Dec 16 12:57:32 EST 2004
Owner            NetSight smith
```

## set rmon channel

Use this command to configure an RMON channel entry.

### Syntax

```
set rmon channel index port-string [accept {matched | failed}] [control {on | off}]
[description description] [owner owner]
```

### Parameters

<i>index</i>	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 2. Maximum value is <b>65535</b> .
<i>port-string</i>	Specifies the port on which traffic will be monitored.
<b>accept matched</b>   <b>failed</b>	(Optional) Specifies the action of the filters on this channel as: <ul style="list-style-type: none"> <li><b>matched</b> - Packets will be accepted on filter matches</li> <li><b>failed</b> - Packets will be accepted if they fail a match</li> </ul>
<b>control on</b>   <b>off</b>	(Optional) Enables or disables control of the flow of data through the channel.
<b>description</b> <i>description</i>	(Optional) Specifies a description for this channel.
<i>owner</i> <i>owner</i>	(Optional) Specifies the name of the entity that configured this entry.

### Defaults

If an action is not specified, packets will be accepted on filter matches.

If not specified, **control** will be set to **off**.

If a **description** is not specified, none will be applied.

If *owner* is not specified, it will be set to **monitor**.

### Mode

Switch command, read-write.

## Example

This example shows how to create an RMON channel entry:

```
B5(rw)->set rmon channel 54313 ge.2.12 accept failed control on description
"capture all"
```

## clear rmon channel

Use this command to clear an RMON channel entry.

### Syntax

```
clear rmon channel index
```

### Parameters

<i>index</i>	Specifies the channel entry to be cleared.
--------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear RMON channel entry 2:

```
B5(rw)->clear rmon channel 2
```

## show rmon filter

Use this command to display one or more RMON filter entries.

### Syntax

```
show rmon filter [index index | channel channel]
```

### Parameters

<i>index index</i>   <i>channel channel</i>	(Optional) Displays information about a specific filter entry, or about all filters which belong to a specific channel.
--	---

### Defaults

If no options are specified, information for all filter entries will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display all RMON filter entries and channel information:

```

B5(rw)->show rmon filter

Index= 55508      Channel Index= 628      EntryStatus= valid
-----
Data Offset      0          PktStatus      0
PktStatusMask    0          PktStatusNotMask 0
Owner            ETS,NAC-D
-----
Data
ff ff ff ff ff ff
-----
DataMask
ff ff ff ff ff ff
-----
DataNotMask
00 00 00 00 00 00

```

## set rmon filter

Use this command to configure an RMON filter entry.

### Syntax

```

set rmon filter index channel-index [offset offset] [status status] [smask smask]
[snotmask snotmask] [data data] [dmask dmask] [dnotmask dnotmask] [owner owner]

```

### Parameters

<i>index</i>	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 10. Maximum value is <b>65535</b> .
<i>channel-index</i>	Specifies the channel to which this filter will be applied.
<b>offset</b> <i>offset</i>	(Optional) Specifies an offset from the beginning of the packet to look for matches.
<b>status</b> <i>status</i>	(Optional) Specifies packet status bits that are to be matched.
<b>smask</b> <i>smask</i>	(Optional) Specifies the mask applied to status to indicate which bits are significant.
<b>snotmask</b> <i>snotmask</i>	(Optional) Specifies the inversion mask that indicates which bits should be set or not set
<b>data</b> <i>data</i>	(Optional) Specifies the data to be matched.
<b>dmask</b> <i>dmask</i>	(Optional) Specifies the mask applied to data to indicate which bits are significant.
<b>dnotmask</b> <i>dnotmask</i>	(Optional) Specifies the inversion mask that indicates which bits should be set or not set.
<i>owner</i>	(Optional) Specifies the name of the entity that configured this entry.

### Defaults

If *owner* is not specified, it will be set to **monitor**.

If no other options are specified, none (0) will be applied.



## Mode

Switch command, read-write.

## Example

This example shows how to create RMON filter 1 and apply it to channel 9:

```
B5(rw)->set rmon filter 1 9 offset 30 data 0a154305 dmask ffffffff
```

## clear rmon filter

Use this command to clear an RMON filter entry.

## Syntax

```
clear rmon filter {index index | channel channel}
```

## Parameters

---

<b>index</b> <i>index</i>	Clears a specific filter entry, or all entries belonging to a specific channel.
<b>channel</b> <i>channel</i>	

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear RMON filter entry 1:

```
B5(rw)->clear rmon filter index 1
```

# Packet Capture Commands

Note that packet capture filter is sampling only and does not guarantee receipt of back-to-back packets.

## Purpose

To display RMON capture entries, configure, enable, or disable capture entries, and clear capture entries.

## Commands

For information about...	Refer to page...
show rmon capture	<a href="#">15-22</a>
set rmon capture	<a href="#">15-23</a>
clear rmon capture	<a href="#">15-24</a>

## show rmon capture

Use this command to display RMON capture entries and associated buffer control entries.

### Syntax

```
show rmon capture [index [nodata]]
```

### Parameters

<i>index</i>	(Optional) Displays the specified buffer control entry and all captured packets associated with that entry.
<b>nodata</b>	(Optional) Displays only the buffer control entry specified by index.

### Defaults

If no options are specified, all buffer control entries and associated captured packets will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display RMON capture entries and associated buffer entries:

```
B5(rw)->show rmon capture
Buf.control= 28062 Channel= 38283 EntryStatus= valid
-----
FullStatus      avail      FullAction    lock
Captured packets 251      Capture slice 1518
Download size   100      Download offset 0
Max Octet Requested 50000    Max Octet Granted 50000
Start time      1 days 0 hours 51 minutes 15 seconds
```

```

Owner                monitor

captureEntry= 1      Buff.control= 28062
-----
Pkt ID              9          Pkt time    1 days 0 hours 51 minutes 15 seconds
Pkt Length         93          Pkt status  0
Data:
00 00 5e 00 01 01 00 01 f4 00 7d ce 08 00 45 00
00 4b b4 b9 00 00 40 11 32 5c 0a 15 43 05 86 8d
bf e5 00 a1 0e 2b 00 37 cf ca 30 2d 02 01 00 04
06 70 75 62 6c 69 63 a2 20 02 02 0c 92 02 01 00
02 01 00 30 14 30 12 06 0d 2b 06 01 02 01 10 07
01 01 0b 81 fd 1c 02 01 01 00 11 0b 00

```

## set rmon capture

Use this command to configure an RMON capture entry.

### Syntax

```

set rmon capture index {channel [action {lock}] [slice slice] [loadsize loadsize]
[offset offset] [asksize asksize] [owner owner]}

```

### Parameters

<i>index</i>	Specifies a buffer control entry.
<i>channel</i>	Specifies the channel to which this capture entry will be applied.
<b>action lock</b>	(Optional) Specifies the action of the buffer when it is full as: <ul style="list-style-type: none"> <li><b>lock</b> - Packets will cease to be accepted</li> </ul>
<b>slice slice</b>	(Optional) Specifies the maximum octets from each packet to be saved in a buffer. Currently, the only value allowed is 1518.
<b>loadsize loadsize</b>	(Optional) Specifies the maximum octets from each packet to be downloaded from the buffer. The default is 100.
<b>offset offset</b>	(Optional) Specifies the first octet from each packet that will be retrieved.
<b>asksize asksize</b>	(Optional) Specifies the requested maximum octets to be saved in this buffer. Currently, the only value accepted is -1, which requests as many octets as possible.
<i>owner</i>	(Optional) Specifies the name of the entity that configured this entry.

### Defaults

If not specified, **action** defaults to **lock**.

If not specified, **offset** defaults to **0**.

If not specified, **asksize** defaults to **-1** (which will request as many octets as possible).

If **slice** is not specified, **1518** will be applied.

If **loadsize** is not specified, **100** will be applied.

If *owner* is not specified, it will be set to **monitor**.

## Mode

Switch command, read-write.

## Example

This example shows how to create RMON capture entry 1 to “listen” on channel 628:

```
B5(rw)->set rmon capture 1 628
```

# clear rmon capture

Use this command to clear an RMON capture entry.

## Syntax

```
clear rmon capture index
```

## Parameters

---

<i>index</i>	Specifies the capture entry to be cleared.
--------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear RMON capture entry 1:

```
B5(rw)->clear rmon capture 1
```

## DHCP Server Configuration

This chapter describes the commands to configure the IPv4 DHCP server functionality on a Enterasys B5 switch.

For information about...	Refer to page...
<a href="#">DHCP Overview</a>	16-1
<a href="#">Configuring General DHCP Server Parameters</a>	16-3
<a href="#">Configuring IP Address Pools</a>	16-12

### DHCP Overview

Dynamic Host Configuration Protocol (DHCP) for IPv4 is a network layer protocol that implements automatic or manual assignment of IP addresses and other configuration information to client devices by servers. A DHCP server manages a user-configured pool of IP addresses from which it can make assignments upon client requests. A relay agent passes DHCP messages between clients and servers which are on different physical subnets.

### DHCP Relay Agent

The DHCP/BOOTP relay agent function can be configured on all of the Enterasys B5's routing interfaces. The relay agent can forward a DHCP client's request to a DHCP server located on a different network if the address of the server is configured as a helper address on the receiving interface. The relay agent interface must be a VLAN which is configured with an IP address. Refer to the **ip helper-address** command ("[ip helper-address](#)" on page 19-14) for more information.

### DHCP Server

DHCP server functionality allows the Enterasys B5 switch to provide basic IP configuration information to a client on the network who requests such information using the DHCP protocol.

DHCP provides the following mechanisms for IP address allocation by a DHCP server:

- Automatic—DHCP server assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address) from a defined pool of IP addresses configured on the server.
- Manual—A client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. This is managed by means of "static" address pools configured on the server.

The amount of time that a particular IP address is valid for a system is called a lease. The Enterasys B5 maintains a lease database which contains information about each assigned IP

address, the MAC address to which it is assigned, the lease expiration, and whether the address assignment is dynamic (automatic) or static (manual). The DHCP lease database is stored in flash memory.

In addition to assigning IP addresses, the DHCP server can also be configured to assign the following to requesting clients:

- Default router(s)
- DNS server(s) and domain name
- NetBIOS WINS server(s) and node name
- Boot file
- DHCP options as defined by RFC 2132



**Note:** A total of 16 address pools, dynamic and/or static, and a maximum of 256 addresses for the entire switch, can be configured on the Enterasys B5.

## Configuring a DHCP Server

For DHCP to function on Enterasys B5 systems, the system has to “know about” the IP network for which the DHCP pool is to be created.

On the B5, there are two ways to configure a DHCP server: one is to associate the DHCP address pool with the switch’s host port IP address, and the other is to associate the DHCP address pool with a routed interface.

Since on a B5 system, the host port IP address cannot fall within a configured routed interface on the system, a typical B5 system configured with routing interfaces will not have a host port IP address. Therefore, all DHCP pools would be associated with routed interfaces.

The following tasks provide basic DHCP server functionality when the DHCP pool is associated with the system’s host IP address. This procedure would typically be used when the B5 system is NOT configured for routing.

1. Configure the system (stack) host port IP address with the **set ip address** command. Once the system’s IP address is configured, the system then “knows” about the configured subnet. For example:

```
set ip address 192.0.0.50 mask 255.255.255.0
```

2. Enable DHCP server functionality on the system with the **set dhcp enable** command.
3. Configure an IP address pool for dynamic IP address assignment. The only *required* steps are to name the pool and define the network number and mask for the pool. Note that the pool has to be in the same subnet and use the same mask as the system host port IP address. For example:

```
set dhcp pool auto-pool network 192.0.0.0 255.255.255.0
```

All DHCP clients served by this switch must be in the same VLAN as the system’s host port.

The following tasks provide basic DHCP server functionality when the DHCP pool is associated with a routed interface.

1. Create a VLAN and add ports to the VLAN. Only DHCP clients associated with this VLAN will be served IP addresses from the DHCP address pool associated with this routed interface (VLAN). In this example, VLAN 6 is created and ports ge.1.1 through ge.1.10 are added to VLAN 6:

```
set vlan create 6
```

```
set port vlan ge.1.1-10 6
```

2. Create a routed interface for the VLAN in router configuration mode. In the following example, an IP address is associated with routed interface VLAN 6:

In router configuration mode:

```
interface vlan 6
no shutdown
ip address 6.6.1.1 255.255.0.0
```

3. Enable DHCP server functionality on the system with the **set dhcp enable** command.
4. Create the DHCP address pool. The only *required* steps are to name the pool and define the network number and mask for the pool. Note that the pool has to be in the same subnet as the routed interface and use the same mask configured on the routed interface. For example:

```
set dhcp pool auto-pool network 6.6.0.0 255.255.0.0
```

DHCP clients in VLAN 6 will be served IP addresses from this DHCP address pool.

Optional DHCP server tasks include:

- You can limit the scope of addresses assigned to a pool for dynamic address assignment with the **set dhcp exclude** command. Up to 128 non-overlapping address ranges can be excluded on the Enterasys B5. For example:

```
set dhcp exclude 192.0.0.1 192.0.0.10
```



**Note:** The IP address of the system's host port or the routed interface is automatically excluded.

- Configure static address pools for manual address assignment. The only *required* steps are to name the pool, configure either the hardware address of the client or the client identifier, and configure the IP address and mask for the manual binding. For example:

```
set dhcp pool static-pool hardware-address 0011.2233.4455
set dhcp pool static-pool host 192.0.0.200 255.255.255.0
```

- Set other DHCP server parameters such as the number of ping packets to be sent before assigning an IP address, or enabling conflict logging.

## Configuring General DHCP Server Parameters

### Purpose

To configure DHCP server parameters, and to display and clear address binding information, server statistics, and conflict information.

### Commands

For information about...	Refer to page...
set dhcp	<a href="#">16-4</a>
set dhcp bootp	<a href="#">16-4</a>
set dhcp conflict logging	<a href="#">16-5</a>
show dhcp conflict	<a href="#">16-5</a>

For information about...	Refer to page...
clear dhcp conflict	<a href="#">16-6</a>
set dhcp exclude	<a href="#">16-7</a>
clear dhcp exclude	<a href="#">16-7</a>
set dhcp ping	<a href="#">16-8</a>
clear dhcp ping	<a href="#">16-8</a>
show dhcp binding	<a href="#">16-9</a>
clear dhcp binding	<a href="#">16-9</a>
show dhcp server statistics	<a href="#">16-10</a>
clear dhcp server statistics	<a href="#">16-11</a>

## set dhcp

Use this command to enable or disable the DHCP server functionality on the Enterasys B5.

### Syntax

```
set dhcp {enable | disable}
```

### Parameters

<b>enable   disable</b>	Enables or disables DHCP server functionality. By default, DHCP server is disabled.
-------------------------	---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example enables DHCP server functionality.

```
B5(rw)->set dhcp enable
```

## set dhcp bootp

Use this command to enable or disable automatic address allocation for BOOTP clients. By default, address allocation for BOOTP clients is disabled. Refer to RFC 1534, "Interoperation Between DHCP and BOOTP," for more information.

### Syntax

```
set dhcp bootp {enable | disable}
```

### Parameters

<b>enable   disable</b>	Enables or disables address allocation for BOOTP clients.
-------------------------	---



## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example enables address allocation for BOOTP clients.

```
B5(rw)->set dhcp bootp enable
```

# set dhcp conflict logging

Use this command to enable conflict logging. By default, conflict logging is enabled. Use the **clear dhcp conflict logging** command to disable conflict logging.

## Syntax

```
set dhcp conflict logging
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example enables DHCP conflict logging.

```
B5(rw)->set dhcp conflict logging
```

# show dhcp conflict

Use this command to display conflict information, for one address or all addresses.

## Syntax

```
show dhcp conflict [address]
```

## Parameters

---

<i>address</i>	[Optional] Specifies the address for which to display conflict information.
----------------	---

---

## Defaults

If no address is specified, conflict information for all addresses is displayed.

## Mode

Read-only.

## Example

This example displays conflict information for all addresses. Note that ping is the only detection method used.

```
B5(ro)->show dhcp conflict
```

IP address	Detection Method	Detection Time
-----	-----	-----
192.0.0.2	Ping	0 days 19h:01m:23s
192.0.0.3	Ping	0 days 19h:00m:46s
192.0.0.4	Ping	0 days 19h:01m:25s
192.0.0.12	Ping	0 days 19h:01m:26s

## clear dhcp conflict

Use this command to clear conflict information for one or all addresses, or to disable conflict logging.

## Syntax

```
clear dhcp conflict {logging | ip-address/ *}
```

## Parameters

logging	Disables conflict logging.
<i>ip-address</i>	Clears the conflict information for the specified IP address.
*	Clears the conflict information for all IP addresses.

## Defaults

None.

## Mode

Switch command, read-write.

## Examples

This example disables DHCP conflict logging.

```
B5(rw)->clear dhcp conflict logging
```

This example clears the conflict information for the IP address 192.0.0.2.

```
B5(rw)->clear dhcp conflict 192.0.0.2
```

## set dhcp exclude

Use this command to configure the IP addresses that the DHCP server should not assign to DHCP clients. Multiple address ranges can be configured but the ranges cannot overlap. Up to 128 non-overlapping address ranges can be excluded.

### Syntax

```
set dhcp exclude low-ipaddr [high-ipaddr]
```

### Parameters

<i>low-ipaddr</i>	Specifies the first IP address in the address range to be excluded from assignment.
<i>high-ipaddr</i>	(Optional) Specifies the last IP address in the address range to be excluded.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example first configures the address pool named "auto1" with 255 addresses for the Class C network 172.20.28.0, with the **set dhcp pool network** command. Then, the example limits the scope of the addresses that can be assigned by a DHCP server by excluding addresses 172.20.28.80 – 100, with the **set dhcp exclude** command.

```
B5(rw)->set dhcp pool auto1 network 172.20.28.0 24
B5(rw)->set dhcp exclude 172.20.28.80 172.20.28.100
```

## clear dhcp exclude

Use this command to clear the configured IP addresses that the DHCP server should not assign to DHCP clients.

### Syntax

```
clear dhcp exclude low-ipaddr [high-ipaddr]
```

### Parameters

<i>low-ipaddr</i>	Specifies the first IP address in the address range to be cleared.
<i>high-ipaddr</i>	(Optional) Specifies the last IP address in the address range to be cleared.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example clears the previously excluded range of IP addresses between 192.168.1.88 through 192.168.1.100.

```
B5(rw)->clear dhcp exclude 192.168.1.88 192.168.1.100
```

## set dhcp ping

Use this command to configure the number of ping packets the DHCP server sends to an IP address before assigning the address to a requesting client.

### Syntax

```
set dhcp ping packets number
```

### Parameters

---

<b>packets</b> <i>number</i>	Specifies the number of ping packets to be sent. The value of number can be 0, or range from 2 to 10. Entering 0 disables this function. The default value is 2 packets.
------------------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example sets the number of ping packets sent to 3.

```
B5(rw)->set dhcp ping packets 3
```

## clear dhcp ping

Use this command to reset the number of ping packets sent by the DHCP server back to the default value of 2.

### Syntax

```
clear dhcp ping packets
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example resets the number of ping packets sent back to the default value.

```
B5(rw)->clear dhcp ping packets
```

## show dhcp binding

Use this command to display binding information for one or all IP addresses.

### Syntax

```
show dhcp binding [ip-address]
```

### Parameters

<i>ip-address</i>	(Optional) Specifies the IP address for which to display binding information.
-------------------	---

### Defaults

If no IP address is specified, binding information for all addresses is displayed.

### Mode

Read-only.

### Example

This example displays binding information about all addresses.

```
B5(rw)->show dhcp binding
IP address           Hardware Address      Lease Expiration      Type
-----
192.0.0.6             00:33:44:56:22:39    00:11:02              Automatic
192.0.0.8             00:33:44:56:22:33    00:10:22              Automatic
192.0.0.10            00:33:44:56:22:34    00:09:11              Automatic
192.0.0.11            00:33:44:56:22:35    00:10:05              Automatic
192.0.0.12            00:33:44:56:22:36    00:10:30              Automatic
192.0.0.13            00:33:44:56:22:37    infinite              Manual
192.0.0.14            00:33:44:56:22:38    infinite              Manual
```

## clear dhcp binding

Use this command to clear (delete) one or all dynamic (automatic) DHCP address bindings.

### Syntax

```
clear dhcp binding {ip-addr | *}
```

### Parameters

<i>ip-addr</i>	Specifies the IP address for which to clear/delete the DHCP binding.
*	Deletes all dynamic address bindings.

### Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command clears only dynamic (automatic) DHCP bindings. Use the command `clear dhcp pool host` to clear manually configured DHCP bindings.

## Example

This example deletes the dynamic DHCP address binding for IP address 192.168.1.1.

```
B5(rw)->clear dhcp binding 192.168.1.1
```

# show dhcp server statistics

Use this command to display DHCP server statistics.

## Syntax

```
show dhcp server statistics
```

## Parameters

None.

## Defaults

None.

## Mode

Read-only.

## Example

This example displays server statistics.

```
B5(ro)->show dhcp server statistics
```

```
Automatic Bindings          36
Expired Bindings            6
Malformed Bindings         0
Messages                    Received
-----
DHCP DISCOVER              382
DHCP REQUEST               3855
DHCP DECLINE                0
DHCP RELEASE                67
DHCP INFORM                 1

Messages                    Sent
-----
DHCP OFFER                  381
DHCP ACK                    727
DHCP NACK                    2
```

---

## clear dhcp server statistics

Use this command to clear all DHCP server counters.

### Syntax

```
clear dhcp server statistics
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example clears all DHCP server counters.

```
B5(rw)->clear dhcp server statistics
```

# Configuring IP Address Pools

## Manual Pool Configuration Considerations

- The subnet of the IP address being issued should be on the same subnet as the ingress interface (that is, the subnet of the host IP address of the switch, or if routing interfaces are configured, the subnet of the routing interface).
- A manual pool can be configured using either the client's hardware address (**set dhcp pool hardware-address**) or the client's client-identifier (**set dhcp pool client-identifier**), but using both is not recommended.
- If the incoming DHCP request packet contains a client-identifier, then a manual pool configured with that client-identifier must exist on the switch in order for the request to be processed. The hardware address is not checked.
- A hardware address and type (Ethernet or IEEE 802) configured in a manual pool is checked only when a client-identifier is not also configured for the pool and the incoming DHCP request packet does not include a client-identifier option.

## Purpose

To configure and clear DHCP address pool parameters, and to display address pool configuration information.



**Note:** A total of 16 address pools, dynamic and/or static, can be configured on the Enterasys B5.

## Commands

For information about...	Refer to page...
set dhcp pool	<a href="#">16-13</a>
clear dhcp pool	<a href="#">16-14</a>
set dhcp pool network	<a href="#">16-14</a>
clear dhcp pool network	<a href="#">16-15</a>
set dhcp pool hardware-address	<a href="#">16-15</a>
clear dhcp pool hardware-address	<a href="#">16-16</a>
set dhcp pool host	<a href="#">16-16</a>
clear dhcp pool host	<a href="#">16-17</a>
set dhcp pool client-identifier	<a href="#">16-17</a>
clear dhcp pool client-identifier	<a href="#">16-18</a>
set dhcp pool client-name	<a href="#">16-19</a>
clear dhcp pool client-name	<a href="#">16-19</a>
set dhcp pool bootfile	<a href="#">16-20</a>
clear dhcp pool bootfile	<a href="#">16-20</a>



For information about...	Refer to page...
set dhcp pool next-server	<a href="#">16-21</a>
clear dhcp pool next-server	<a href="#">16-21</a>
set dhcp pool lease	<a href="#">16-22</a>
clear dhcp pool lease	<a href="#">16-22</a>
set dhcp pool default-router	<a href="#">16-23</a>
clear dhcp pool default-router	<a href="#">16-23</a>
set dhcp pool dns-server	<a href="#">16-24</a>
clear dhcp pool dns-server	<a href="#">16-24</a>
set dhcp pool domain-name	<a href="#">16-25</a>
clear dhcp pool domain-name	<a href="#">16-25</a>
set dhcp pool netbios-name-server	<a href="#">16-26</a>
clear dhcp pool netbios-name-server	<a href="#">16-26</a>
set dhcp pool netbios-node-type	<a href="#">16-27</a>
clear dhcp pool netbios-node-type	<a href="#">16-27</a>
set dhcp pool option	<a href="#">16-28</a>
clear dhcp pool option	<a href="#">16-29</a>
show dhcp pool configuration	<a href="#">16-29</a>

## set dhcp pool

Use this command to create and assign a name to a DHCP server pool of addresses. Up to 16 address pools may be configured on a Enterasys B5. Note that entering this command is not required to create an address pool before configuring other address pool parameters.

### Syntax

```
set dhcp pool poolname
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example creates an address pool named "auto1."

```
B5(rw)->set dhcp pool auto1
```

## clear dhcp pool

Use this command to delete a DHCP server pool of addresses.

### Syntax

```
clear dhcp pool poolname
```

### Parameters

---

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example deletes the address pool named "auto1."

```
B5(rw)->clear dhcp pool auto1
```

## set dhcp pool network

Use this command to configure the subnet number and mask for an automatic DHCP address pool.

### Syntax

```
set dhcp pool poolname network number {mask | prefix-length}
```

### Parameters

---

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>number</i>	Specifies an IP subnet for the address pool.
<i>mask</i>	Specifies the subnet mask in dotted quad notation.
<i>prefix-length</i>	Specifies the subnet mask as an integer.

---

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

Use this command to configure a set of IP addresses to be assigned by the DHCP server using the specified address pool. In order to limit the scope of the addresses configured with this command, use the [set dhcp exclude](#) command on page [16-7](#).

## Examples

This example configures the IP subnet 172.20.28.0 with a prefix length of 24 for the automatic DHCP pool named "auto1." Alternatively, the mask could have been specified as 255.255.255.0.

```
B5(rw)->set dhcp pool auto1 network 172.20.28.0 24
```

This example limits the scope of 255 addresses created for the Class C network 172,20.28.0 by the previous example, by excluding addresses 172.20.28.80 – 100.

```
B5(rw)->set dhcp exclude 172.20.28.80 172.20.28.100
```

## clear dhcp pool network

Use this command to remove the network number and mask of a DHCP server pool of addresses.

### Syntax

```
clear dhcp pool poolname network
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example deletes the network and mask from the address pool named "auto1."

```
B5(rw)->clear dhcp pool auto1 network
```

## set dhcp pool hardware-address

Use this command to configure the MAC address of the DHCP client and create an address pool for manual binding. You can use either this command or the **set dhcp pool client-identifier** command to create a manual binding pool, but using both is not recommended.

### Syntax

```
set dhcp pool poolname hardware-address hw-addr [type]
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>hw-addr</i>	Specifies the MAC address of the client's hardware platform. This value can be entered using dotted hexadecimal notation or colons.
<i>type</i>	(Optional) Specifies the protocol of the hardware platform. Valid values are 1 for Ethernet or 6 for IEEE 802. Default value is 1, Ethernet.

## Defaults

If no *type* is specified, Ethernet is assumed.

## Mode

Switch command, read-write.

## Example

This example specifies 0001.f401.2710 as the Ethernet MAC address for the manual address pool named "manual1." Alternatively, the MAC address could have been entered as 00:01:f4:01:27:10.

```
B5(rw)->set dhcp pool manual1 hardware-address 0001.f401.2710
```

# clear dhcp pool hardware-address

Use this command to remove the hardware address of a DHCP client from a manual binding address pool.

## Syntax

```
clear dhcp pool poolname hardware-address
```

## Parameters

---

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example deletes the client hardware address from the address pool named "manual1."

```
B5(rw)->clear dhcp pool manual1 hardware-address
```

# set dhcp pool host

Use this command to configure an IP address and network mask for a manual DHCP binding.

## Syntax

```
set dhcp pool poolname host ip-address [mask | prefix-length]
```

## Parameters

---

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>ip-address</i>	Specifies the IP address for manual binding.

---

---

<i>mask</i>	(Optional) Specifies the subnet mask in dotted quad notation.
<i>prefix-length</i>	(Optional) Specifies the subnet mask as an integer.

---

## Defaults

If a mask or prefix is not specified, the class A, B, or C natural mask will be used.

## Mode

Switch command, read-write.

## Example

This example shows how to configure the minimum requirements for a manual binding address pool. First, the hardware address of the client's hardware platform is configured, followed by configuration of the address to be assigned to that client manually.

```
B5(rw)->set dhcp pool manual1 hardware-address 0001.f401.2710
B5(rw)->set dhcp pool manual1 host 15.12.1.99 255.255.248.0
```

# clear dhcp pool host

Use this command to remove the host IP address from a manual binding address pool.

## Syntax

```
clear dhcp pool poolname host
```

## Parameters

---

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example deletes the host IP address from the address pool named "manual1."

```
B5(rw)->clear dhcp pool manual1 host
```

# set dhcp pool client-identifier

Use this command to configure the client identifier of the DHCP client and create an address pool for manual binding. You can use either this command or the **set dhcp pool hardware-address** command to create a manual binding pool, but using both is not recommended.

## Syntax

```
set dhcp pool poolname client-identifier id
```

## Parameters

---

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>id</i>	Specifies the unique client identifier for this client. The value must be entered in xx:xx:xx:xx:xx:xx format.

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The client identifier is formed by concatenating the media type and the MAC address. For example, if the client hardware type is Ethernet and the client MAC address is 00:01:22:33:44:55, then the client identifier configured with this command must be 01:00:01:22:33:44:55.

## Example

This example shows how to configure the minimum requirements for a manual binding address pool, using a client identifier rather than the hardware address of the client's hardware platform.

```
B5(rw)->set dhcp pool manual2 client-identifier 01:00:01:22:33:44:55
B5(rw)->set dhcp pool manual2 host 10.12.1.10 255.255.255.0
```

# clear dhcp pool client-identifier

Use this command to remove the unique identifier of a DHCP client from a manual binding address pool.

## Syntax

```
clear dhcp pool poolname client-identifier
```

## Parameters

---

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example deletes the client identifier from the address pool named "manual1."

```
B5(rw)->clear dhcp pool manual1 client-identifier
```

## set dhcp pool client-name

Use this command to assign a name to a DHCP client when creating an address pool for manual binding.

### Syntax

```
set dhcp pool poolname client-name name
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>name</i>	Specifies the name to be assigned to this client. Client names may be up to 31 characters in length.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example configures the client name “appsvr1” to the manual binding pool “manual2.”

```
B5(rw)->set dhcp pool manual2 client-identifier 01:22:33:44:55:66
B5(rw)->set dhcp pool manual2 host 10.12.1.10 255.255.255.0
B5(rw)->set dhcp pool manual2 client-name appsvr1
```

## clear dhcp pool client-name

Use this command to delete a DHCP client name from an address pool for manual binding.

### Syntax

```
clear dhcp pool poolname client-name
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example deletes the client name from the manual binding pool “manual2.”

```
B5(rw)->clear dhcp pool manual2 client-name
```

## set dhcp pool bootfile

Use this command to specify a default boot image for the DHCP clients who will be served by the address pool being configured.

### Syntax

```
set dhcp pool poolname bootfile filename
```

### Parameters

---

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>filename</i>	Specifies the boot image file name.

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example sets the boot image filename for address pool named "auto1."

```
B5(rw)->set dhcp pool auto1 bootfile image1.img
```

## clear dhcp pool bootfile

Use this command to remove a default boot image from the address pool being configured.

### Syntax

```
clear dhcp pool poolname bootfile
```

### Parameters

---

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example removes the boot image filename from address pool named "auto1."

```
B5(rw)->clear dhcp pool auto1 bootfile
```



## set dhcp pool next-server

Use this command to specify the file server from which the default boot image is to be loaded by the client.

### Syntax

```
set dhcp pool poolname next-server ip-address
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>ip-address</i>	Specifies the IP address of the file server the DHCP client should contact to load the default boot image.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example specifies the file server from which clients being served by address pool "auto1" should download the boot image file "image1.img."

```
B5(rw)->set dhcp pool auto1 bootfile image1.img
B5(rw)->set dhcp pool auto1 next-server 10.1.1.10
```

## clear dhcp pool next-server

Use this command to remove the boot image file server from the address pool being configured.

### Syntax

```
clear dhcp pool poolname next-server
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example removes the file server from address pool "auto1."

```
B5(rw)->clear dhcp pool auto1 next-server
```

## set dhcp pool lease

Use this command to specify the duration of the lease for an IP address assigned by the DHCP server from the address pool being configured.

### Syntax

```
set dhcp pool poolname lease {days [hours [minutes]] | infinite}
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>days</i>	Specifies the number of days an address lease will remain valid. Value can range from 0 to 59.
<i>hours</i>	(Optional) When a <i>days</i> value has been assigned, specifies the number of hours an address lease will remain valid. Value can range from 0 to 1439.
<i>minutes</i>	(Optional) When a <i>days</i> value and an <i>hours</i> value have been assigned, specifies the number of minute an address lease will remain valid. Value can range from 0 to 86399.
<b>infinite</b>	Specifies that the duration of the lease will be unlimited.

### Defaults

If no lease time is specified, a lease duration of 1 day is configured.

### Mode

Switch command, read-write.

### Example

This example configures a lease duration of 12 hours for the address pool being configured. Note that to configure a lease time less than one day, enter 0 for days, then the number of hours and minutes.

```
B5(rw)->set dhcp pool auto1 lease 0 12
```

## clear dhcp pool lease

Use this command to restore the default lease time value of one day for the address pool being configured.

### Syntax

```
clear dhcp pool poolname lease
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

### Defaults

Clears the lease time for this address pool to the default value of one day.

## Mode

Switch command, read-write.

## Example

This example restores the default lease duration of one day for address pool “auto1.”

```
B5(rw)->clear dhcp pool auto1 lease
```

# set dhcp pool default-router

Use this command to specify a default router list for the DHCP clients served by the address pool being configured. Up to 8 default routers can be configured.

## Syntax

```
set dhcp pool poolname default-router address [address2 ... address8]
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>address</i>	Specifies the IP address of a default router.
<i>address2</i> ... <i>address8</i>	(Optional) Specifies, in order of preference, up to 7 additional default router addresses.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example assigns a default router at 10.10.10.1 to the address pool named “auto1.”

```
B5(rw)->set dhcp pool auto1 default-router 10.10.10.1
```

# clear dhcp pool default-router

Use this command to delete the default routers configured for this address pool.

## Syntax

```
clear dhcp pool poolname default-router
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example removes the default router from the address pool "auto1."

```
B5(rw)->clear dhcp pool auto1 default-router
```

# set dhcp pool dns-server

Use this command to specify one or more DNS servers for the DHCP clients served by the address pool being configured. Up to 8 DNS servers can be configured.

## Syntax

```
set dhcp pool poolname dns-server address [address2 ... address8]
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>address</i>	Specifies the IP address of a DNS server.
<i>address2</i> ... <i>address8</i>	(Optional) Specifies, in order of preference, up to 7 additional DNS server addresses.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example assigns a DNS server at 10.14.10.1 to the address pool "auto1."

```
B5(rw)->set dhcp pool auto1 dns-server 10.14.10.1
```

# clear dhcp pool dns-server

Use this command to remove the DNS server list from the address pool being configured.

## Syntax

```
clear dhcp pool poolname dns-server
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example removes the DNS server list from the address pool "auto1."

```
B5(rw)->clear dhcp pool auto1 dns-server
```

# set dhcp pool domain-name

Use this command to specify a domain name to be assigned to DHCP clients served by the address pool being configured.

## Syntax

```
set dhcp pool poolname domain-name domain
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>domain</i>	Specifies the domain name string. The domain name can be up to 255 characters in length.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example assigns the "mycompany.com" domain name to the address pool "auto1."

```
B5(rw)->set dhcp pool auto1 domain-name mycompany.com
```

# clear dhcp pool domain-name

Use this command to remove the domain name from the address pool being configured.

## Syntax

```
clear dhcp pool poolname domain-name
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example removes the domain name from the address pool "auto1."

```
B5(rw)->clear dhcp pool auto1 domain-name
```

# set dhcp pool netbios-name-server

Use this command to assign one or more NetBIOS name servers for the DHCP clients served by the address pool being configured. Up to 8 NetBIOS name servers can be configured.

## Syntax

```
set dhcp pool poolname netbios-name-server address [address2 ... address8]
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>address</i>	Specifies the IP address of a NetBIOS name server.
<i>address2</i> ... <i>address8</i>	(Optional) Specifies, in order of preference, up to 7 additional NetBIOS name server addresses.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example assigns a NetBIOS name server at 10.15.10.1 to the address pool being configured.

```
B5(rw)->set dhcp pool auto1 netbios-name-server 10.15.10.1
```

# clear dhcp pool netbios-name-server

Use this command to remove the NetBIOS name server list from the address pool being configured.

```
clear dhcp pool poolname netbios-name-server
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example removes the NetBIOS name server list from the address pool auto1.

```
B5(rw)->clear dhcp pool auto1 netbios-name-server
```

# set dhcp pool netbios-node-type

Use this command to specify a NetBIOS node (server) type for the DHCP clients served by the address pool being configured.

## Syntax

```
set dhcp pool poolname netbios-node-type {b-node | h-node | p-node | m-node}
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<b>b-node</b>	Specifies the NetBIOS node type to be broadcast (no WINS).
<b>h-node</b>	Specifies the NetBIOS node type to be hybrid (WINS, then broadcast).
<b>p-node</b>	Specifies the NetBIOS node type to be peer (WINS only).
<b>m-node</b>	Specifies the NetBIOS node type to be mixed (broadcast, then WINS).

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example specifies hybrid as the NetBIOS node type for the address pool "auto1."

```
B5(rw)->set dhcp pool auto1 netbios-node-type h-node
```

# clear dhcp pool netbios-node-type

Use this command to remove the NetBIOS node type from the address pool being configured.

## Syntax

```
clear dhcp pool poolname netbios-node-type
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example removes the NetBIOS node type from the address pool "auto1."

```
B5(rw)->clear dhcp pool auto1 netbios-node-type
```

# set dhcp pool option

Use this command to configure DHCP options, described in RFC 2132.

## Syntax

```
set dhcp pool poolname option code {ascii string | hex string-list | ip address-list}
```

## Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>code</i>	Specifies the DHCP option code, as defined in RFC 2132. Value can range from 1 to 254.
<i>ascii string</i>	Specifies the data in ASCII format. An ASCII character string containing a space must be enclosed in quotations.
<i>hex string-list</i>	Specifies the data in HEX format. Up to 8 HEX strings can be entered.
<i>ip address-list</i>	Specifies the data in IP address format. Up to 8 IP addresses can be entered.

## Defaults

None.

## Mode

Switch command, read-write.

## Examples

This example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. In this case, IP forwarding is enabled with the 01 value.

```
B5(rw)->set dhcp pool auto1 option 19 hex 01
```

This example configures DHCP option 72, which assigns one or more Web servers for DHCP clients. In this case, two Web server addresses are configured.

```
B5(rw)->set dhcp pool auto1 option 72 ip 168.24.3.252 168.24.3.253
```



## clear dhcp pool option

Use this command to remove a DHCP option from the address pool being configured.

### Syntax

```
clear dhcp pool poolname option code
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
<i>code</i>	Specifies the DHCP option code, as defined in RFC 2132. Value can range from 1 to 254.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example removes option 19 from address pool "auto1."

```
B5(rw)->clear dhcp pool auto1 option 19
```

## show dhcp pool configuration

Use this command to display configuration information for one or all address pools.

### Syntax

```
show dhcp pool configuration {poolname | all}
```

### Parameters

<i>poolname</i>	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
-----------------	--

### Defaults

None.

### Mode

Read-only.

### Example

This example displays configuration information for all address pools.

```
B5(rw)->show dhcp pool configuration all
```

```
Pool: Atg_Pool
Pool Type                               Dynamic
```

show dhcp pool configuration

---

```
Network          192.0.0.0 255.255.255.0
Lease Time       1 days 0 hrs 0 mins
Default Routers  192.0.0.1

Pool: static1
Pool Type        Manual
Client Name      appsvr1
Client Identifier 01:00:01:f4:01:27:10
Host             10.1.1.1 255.0.0.0
Lease Time       infinite
Option          19 hex 01

Pool: static2
Pool Type        Manual
Hardware Address 00:01:f4:01:27:10
Hardware Address Type ieee802
Host             192.168.10.1 255.255.255.0
Lease Time       infinite
```

## DHCP Snooping and Dynamic ARP Inspection

This chapter describes two security features:

- DHCP snooping, which monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP messages and to build a database of authorized address bindings
- Dynamic ARP inspection, which uses the bindings database created by the DHCP snooping feature to reject invalid and malicious ARP packets

For information about...	Refer to page...
<a href="#">DHCP Snooping Overview</a>	17-1
<a href="#">DHCP Snooping Commands</a>	17-4
<a href="#">Dynamic ARP Inspection Overview</a>	17-16
<a href="#">Dynamic ARP Inspection Commands</a>	17-20

### DHCP Snooping Overview

DHCP snooping monitors DHCP messages between DHCP clients and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized.

DHCP snooping is disabled globally and on all VLANs by default. Ports are untrusted by default. DHCP snooping must be enabled globally and on specific VLANs. Ports within the VLANs must be configured as trusted or untrusted. DHCP servers must be reached through trusted ports.

DHCP snooping enforces the following security rules:

- DHCP packets from a DHCP server (DHCP OFFER, DHCP ACK, DHCP NAK) are dropped if received on an untrusted port.
- DHCP RELEASE and DHCP DECLINE messages are dropped if they are for a MAC address in the snooping database but the binding's interface in the database is different from the interface where the message was received.
- On untrusted interfaces, the switch drops DHCP packets whose source MAC address does not match the client hardware address. This feature is a configurable option.

### DHCP Message Processing

The hardware identifies all incoming DHCP packets on ports where DHCP snooping is enabled. On untrusted ports, the hardware traps all incoming DHCP packets to the CPU. On trusted ports,

the hardware forwards client messages and copies server messages to the CPU so DHCP snooping can learn the binding.

The DHCP snooping application processes incoming DHCP messages. For DHCP RELEASE and DHCP DECLINE messages, the application compares the receive interface and VLAN with the client's interface and VLAN in the bindings database. If the interfaces do not match, the application logs the event and drops the message. For valid client messages, DHCP snooping compares the source MAC address to the DHCP client hardware address. Where there is a mismatch, DHCP snooping logs and drops the packet. You can disable this feature using the **set dhcpsnooping verify mac-address disable** command.



**Note:** If the switch has been configured as a DHCP relay agent, to forward client requests to a DHCP server that does not reside on the same broadcast domain as the client, MAC address verification should be disabled in order to allow DHCP RELEASE packets to be processed by the DHCP snooping functionality and client bindings removed from the bindings database.

DHCP snooping can be configured on switching VLANs and routing VLANs. When a DHCP packet is received on a routing VLAN, the DHCP snooping application applies its filtering rules and updates the bindings database. If a client message passes filtering rules, the message is placed into the software forwarding path, where it may be processed by the DHCP relay agent, the local DHCP server, or forwarded as an IP packet.

DHCP snooping forwards valid DHCP client messages received on non-routing VLANs. The message is forwarded on all trusted interfaces in the VLAN. If a DHCP relay agent or local DHCP server co-exist with the DHCP snooping feature, DHCP client messages will be sent to the DHCP relay agent or local DHCP server to process further.

The DHCP snooping application does not forward server messages since they are forwarded in hardware.

## Building and Maintaining the Database

The DHCP snooping application uses DHCP messages to build and maintain the bindings database. The bindings database includes only data for clients on untrusted ports. The bindings database includes the following information for each entry:

- Client MAC address
- Client IP address
- Time when client's lease expires
- Client VLAN ID
- Client port

DHCP snooping creates a tentative binding from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to a port (the port where the DHCP client message was received). Tentative bindings are completed when DHCP snooping learns the client's IP address from a DHCP ACK message on a trusted port. DHCP snooping removes bindings in response to DECLINE, RELEASE, and NACK messages. The DHCP snooping application ignores the ACK messages sent in reply to the DHCP Inform messages received on trusted ports. You can also enter static bindings into the bindings database.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database.

If the absolute lease time of a snooping database entry expires, then that entry will be removed. Care should be taken to ensure that system time is consistent across the reboots. Otherwise, snooping entries will not expire properly. If a host sends a DHCP RELEASE message while the

switch is rebooting, when the switch receives a DHCP DISCOVERY or REQUEST message, the client's binding will go to a tentative binding state.

## Rate Limiting

To protect the switch against DHCP attacks when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds a configurable limit, DHCP snooping brings down the interface. Use the **set port enable** command to re-enable the interface. Both the rate and the burst interval can be configured.

## Basic Configuration

The following configuration procedure does not change the write delay to the snooping database or any of the default rate limiting values. Additional configuration notes follow this procedure.

### Procedure 17-1 Basic Configuration for DHCP Snooping

Step	Task	Command(s)
1.	Enable DHCP snooping globally on the switch.	<b>set dhcpsnooping enable</b>
2.	Determine where DHCP clients will be connected and enable DHCP snooping on their VLANs.	<b>set dhcpsnooping vlan <i>vlan-list</i> enable</b>
3.	Determine which ports will be connected to the DHCP server and configure them as trusted ports.	<b>set dhcpsnooping trust port <i>port-string</i> enable</b>
4.	If desired, enable logging of invalid DHCP messages on specific ports.	<b>set dhcpsnooping log-invalid port <i>port-string</i> enable</b>
5.	If desired, add static bindings to the database.	<b>set dhcpsnooping binding <i>mac-address</i> vlan <i>vlan-id</i> ipaddr port <i>port-string</i></b>

## Configuration Notes

### DHCP Server

- When the switch is operating in switch mode, then the DHCP server and DHCP clients must be in the same VLAN.
- If the switch is in routing mode (on those platforms that support routing), then the DHCP server can be remotely connected to a routing interface, or running locally.
- If the DHCP server is remotely connected, then the use of an IP helper address is required and MAC address verification should be disabled (**set dhcpsnooping verify mac-address disable**).
- The DHCP server must use Scopes in order to provide the IP addresses per VLAN.
- DHCP snooping must be enabled on the interfaces where the DHCP clients are connected, and the interfaces must be untrusted DHCP snooping ports.
- The routing interface that is connected to the DHCP server must be enabled for DHCP snooping and must be a trusted DHCP snooping port.

## DHCP Snooping Commands

For information about...	Refer to page...
<a href="#">set dhcpsnooping</a>	17-4
<a href="#">set dhcpsnooping vlan</a>	17-5
<a href="#">set dhcpsnooping database write-delay</a>	17-5
<a href="#">set dhcpsnooping trust</a>	17-6
<a href="#">set dhcpsnooping binding</a>	17-7
<a href="#">set dhcpsnooping verify</a>	17-7
<a href="#">set dhcpsnooping log-invalid</a>	17-8
<a href="#">set dhcpsnooping limit</a>	17-9
<a href="#">show dhcpsnooping</a>	17-10
<a href="#">show dhcpsnooping database</a>	17-11
<a href="#">show dhcpsnooping port</a>	17-11
<a href="#">show dhcpsnooping binding</a>	17-12
<a href="#">show dhcpsnooping statistics</a>	17-13
<a href="#">clear dhcpsnooping binding</a>	17-14
<a href="#">clear dhcpsnooping statistics</a>	17-14
<a href="#">clear dhcpsnooping database</a>	17-14
<a href="#">clear dhcpsnooping limit</a>	17-15

### set dhcpsnooping

Use this command to enable or disable DHCP snooping globally.

#### Syntax

```
set dhcpsnooping {enable | disable}
```

#### Parameters

<b>enable</b>	Enable DHCP snooping globally on the switch.
<b>disable</b>	Disable DHCP snooping globally on the switch.

#### Defaults

Disabled globally.

#### Mode

Switch command, read-write.

#### Usage

By default, DHCP snooping is disabled globally and on all VLANs. You must enable it globally with this command, and then enable it on specific VLANs.

## Example

The following example enables DHCP snooping globally.

```
B5(rw)->set dhcp snooping enable
```

## set dhcp snooping vlan

Use this command to enable or disable DHCP snooping on a VLAN or range of VLANs.

### Syntax

```
set dhcp snooping vlan vlan-range {enable | disable}
```

### Parameters

<i>vlan-range</i>	Specifies the VLAN or range of VLANs on which DHCP snooping is to be enabled or disabled.
<b>enable   disable</b>	Enables or disables DHCP snooping for the specified VLANs.

### Defaults

DHCP snooping is disabled by default on all VLANs.

### Mode

Switch command, read-write.

### Usage

By default, DHCP snooping is disabled globally and on all VLANs. You must enable it globally with the **set dhcp snooping** command, and then enable it on specific VLANs with this command.

### Example

This example enables DHCP snooping on VLANs 10 through 20.

```
B5(rw)->set dhcp snooping vlan 10-20 enable
```

## set dhcp snooping database write-delay

Use this command to specify the interval between updates to the stored bindings database.

### Syntax

```
set dhcp snooping database write-delay seconds
```

### Parameters

<i>second</i>	Specify the interval in seconds between updates to the stored bindings database. The value can range from 15 to 86400 seconds.
---------------	--

### Defaults

Every 5 minutes (300 seconds).

## Mode

Switch command, read-write.

## Usage

When a switch learns of new bindings or when it loses bindings, the switch updates the entries in the bindings database according to the write delay timer. The switch also updates the entries in the binding file. The frequency at which the file is updated is based on the delay configured with this command, and the updates are batched.

## Example

The following example specifies that the stored database should be updated once an hour.

```
B5(rw)->set dhcp snooping database write-delay 3600
```

# set dhcp snooping trust

Use this command to enable or disable a port as a DHCP snooping trusted port.

## Syntax

```
set dhcp snooping trust port port-string {enable | disable}
```

## Parameters

<b>port</b> <i>port-string</i>	Specifies the port or ports to be enabled or disabled as trusted ports. The ports can be physical ports or LAGs that are members of a VLAN.
<b>enable   disable</b>	Enables or disables the specified ports as trusted ports.

## Defaults

By default, ports are untrusted.

## Mode

Switch command, read-write.

## Usage

In order for DHCP snooping to operate, snooping has to be enabled globally and on specific VLANs, and the ports within the VLANs have to be configured as trusted or untrusted. On trusted ports, DHCP client messages are forwarded directly by the hardware. On untrusted ports, client messages are given to the DHCP snooping application.

The DHCP snooping application builds the bindings database from client messages received on untrusted ports. DHCP snooping creates a “tentative binding” from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to the port on which the message packet was received. Tentative bindings are completed when DHCP snooping learns the client’s IP address from a DHCP ACK message on a trusted port.

The ports on the switch through which DHCP servers are reached must be configured as trusted ports so that packets received from those ports will be forwarded to clients. DHCP packets from a DHCP server (DHCP OFFER, DHCP ACK, DHCP NAK) are dropped if received on an untrusted port.



## Example

This example configures port ge.1.1 as a trusted port.

```
B5(rw)->set dhcp snooping trust port ge.1.1 enable
```

## set dhcp snooping binding

Use this command to add a static DHCP binding to the DHCP snooping database.

### Syntax

```
set dhcp snooping binding mac-address vlan vlan-id ipaddr port port-string
```

### Parameters

<i>mac-address</i>	Specifies the MAC address of the binding entry.
<b>vlan</b> <i>vlan-id</i>	Specifies the VLAN of the binding entry.
<i>ipaddr</i>	Specifies the IP address of the binding entry.
<b>port</b> <i>port-string</i>	Specifies the port of the binding entry.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

When enabled globally and on VLANs, DHCP snooping builds its bindings database from DHCP client messages received on untrusted ports. Such entries in the database are dynamic entries which will be removed in response to valid DECLINE, RELEASE, and NACK messages or when the absolute lease time of the entry expires.

You can add static entries to the bindings database with this command.

### Example

This example creates a static entry, associating MAC address 00:01:02:33:44:55 with IP address 192.168.10.10 and VLAN 10, port ge.1.1.

```
B5(rw)->set dhcp snooping binding 00:01:02:33:44:55 vlan 10 192.168.10.10 port ge.1.1
```

## set dhcp snooping verify

Use this command to enable or disable DHCP snooping to filter on source MAC address.

### Syntax

```
set dhcp snooping verify mac-address {enable | disable}
```

## Parameters

<b>enable</b>	Enables verification of the source MAC address in client messages against the client hardware address.
<b>disable</b>	Disables verification of the source MAC address in client messages against the client hardware address.

## Defaults

Source MAC address verification is enabled by default.

## Mode

Switch command, read-write.

## Usage

When this verification is enabled, the DHCP snooping application compares the source MAC address contained in valid client messages with the client's hardware address. If there is a mismatch, DHCP snooping logs the event and drops the packet.

Use the **show dhcp snooping** command to display the status (enabled or disabled) of source MAC address verification for each interface in an enabled VLAN. The **show dhcp snooping statistics** command shows the actual number of MAC verification errors that occurred on untrusted ports.

## Example

This example disables source MAC address verification and logging.

```
B5(rw)->set dhcp snooping verify mac-address disable
```

# set dhcp snooping log-invalid

Use this command to enable or disable logging of invalid DHCP messages on ports.

## Syntax

```
set dhcp snooping log-invalid port port-string {enable | disable}
```

## Parameters

<b>port</b> <i>port-string</i>	Specifies the port or ports on which to enable or disable logging of invalid packets.
<b>enable   disable</b>	Enables or disables logging on the specified ports.

## Defaults

Disabled.

## Mode

Switch command, read-write.

## Usage

The DHCP snooping application processes incoming DHCP messages. For DHCPRELEASE and DHCPDECLINE messages, the application compares the receive interface and VLAN with the

client's interface and VLAN in the bindings database. If the interfaces do not match, the application logs the event if logging has been enabled.

Use the **show dhcp snooping** command to display the status (enabled or disabled) of logging invalid packets for each interface in an enabled VLAN. The **show dhcp snooping statistics** command shows the actual number of server messages received on untrusted ports.

## Example

This example enables logging of invalid DHCP messages on port ge.1.1 and then displays the DHCP configuration settings.

```
B5(rw)->set dhcp snooping log invalid port ge.1.1 enable
```

```
B5(su)->show dhcp snooping
```

```
DHCP snooping is Disabled
```

```
DHCP snooping source MAC verification is enabled
```

```
DHCP snooping is enabled on the following VLANs:
```

```
3
```

Interface	Trusted	Log Invalid Pkts
ge.1.1	No	Yes
ge.1.2	No	No
ge.1.3	Yes	No

## set dhcp snooping limit

Use this command to configure rate limiting parameters for incoming DHCP packets on a port or ports.

### Syntax

```
set dhcp snooping limit port-string {none | rate pps {burst interval secs}}
```

### Parameters

<i>port-string</i>	Specifies the port or ports to which to apply these rate limiting parameters.
<b>none</b>	Configures no limit on incoming DHCP packets.
<b>rate</b> <i>pps</i>	Specifies a rate limit in packets per second. The value of <i>pps</i> can range from 0 to 100 packets per second.
<b>burst interval</b> <i>secs</i>	Specifies a burst interval in seconds. The value of <i>secs</i> can range from 1 to 15 seconds.

### Defaults

Rate = 15 packets per second

Burst Interval = 1 second

### Mode

Switch command, read-write.

## Usage

To protect the switch from DHCP attacks when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit, DHCP snooping brings down the interface. You can re-enable the interface with the **set port enable** command. Both the rate and the burst interval can be configured.

You can display the currently configured rate limit parameters with the **show dhcp snooping port** command.

## Example

This example configures rate limit parameters on port ge.1.1.

```
B5(rw)->set dhcp snooping limit ge.1.1 rate 20 burst interval 2
```

```
B5(rw)->show dhcp snooping port ge.1.1
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
ge.1.1	No	20	2

## show dhcp snooping

Use this command to display DHCP snooping configuration parameters.

### Syntax

```
show dhcp snooping
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

## Usage

This command displays the status (enabled or disabled) of DHCP snooping globally, lists the VLANs on which DHCP snooping is enabled, displays whether source MAC address verification is enabled or disabled, and for ports that are enabled for snooping, displays whether they are trusted or untrusted and whether logging of invalid packets has been enabled.

## Example

This example shows the output of the **show dhcp snooping** command.

```
B5(su)->show dhcp snooping
```

```
DHCP snooping is Enabled
```

```
DHCP snooping source MAC verification is enabled
```

```
DHCP snooping is enabled on the following VLANs:
```

3

Interface	Trusted	Log Invalid Pkts
-----	-----	-----
ge.1.47	Yes	No
ge.1.48	No	No
lag.0.1	No	No

## show dhcp snooping database

Use this command to display DHCP snooping database configuration parameters.

### Syntax

```
show dhcp snooping database
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

This command displays where the database file is stored (locally) and what the write delay value is.

### Example

This example shows the output of the **show dhcp snooping database** command.

```
B5(su)->show dhcp snooping database
agent url: local

write-delay: 300
```

## show dhcp snooping port

Use this command to display DHCP snooping configuration parameters for specific ports.

### Syntax

```
show dhcp snooping port port-string
```

### Parameters

<i>port-string</i>	Specifies the port or ports for which to display configuration information.
--------------------	---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command displays the trust state and rate limiting parameters configured on the specified ports.

## Example

This example shows the output of the **show dhcp snooping port** command.

```

B5(su)->show dhcp snooping port ge.1.1
Interface      Trust State      Rate Limit      Burst Interval
              (pps)           (seconds)
-----
ge.1.1         No               20              2

```

# show dhcp snooping binding

Use this command to display the contents of the DHCP snooping bindings database.

## Syntax

```
show dhcp snooping binding [dynamic | static] [port port-string] [vlan vlan-id]
```

## Parameters

<b>dynamic</b>   <b>static</b>	(Optional) Limits the display of bindings in the database by type of entry, either dynamic or static.
<b>port</b> <i>port-string</i>	(Optional) Limits the display of bindings in the database by port.
<b>vlan</b> <i>vlan-id</i>	(Optional) Limits the display of bindings in the database by VLAN id.

## Defaults

If no parameters are entered, all bindings in the database are displayed.

## Mode

Switch command, read-write.

## Usage

This command displays information about the DHCP bindings in the DHCP snooping database.

## Example

This example shows the output of the **show dhcp snooping binding** command when no parameters are entered.

```

B5(su)->show dhcp snooping binding
Total number of bindings: 2

```

MAC Address	IP Address	VLAN	Interface	Type	Lease (min)
00:02:B3:06:60:80	192.168.10.10	3	ge.1.1	STATIC	
00:0F:FE:00:13:04	192.168.20.1	5	ge.1.30	DYNAMIC	1440

## show dhcpsnooping statistics

Use this command to display DHCP snooping statistics for untrusted ports.

### Syntax

```
show dhcpsnooping statistics
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

The DHCP snooping application processes incoming DHCP messages on enabled untrusted interfaces. For DHCP RELEASE and DHCP DECLINE messages, the application compares the receive interface and VLAN with the client's interface and VLAN in the bindings database. If the interfaces do not match, the application logs the event (if logging of invalid messages is enabled) and drops the message. If source MAC verification is enabled, for valid client messages, DHCP snooping compares the source MAC address to the DHCP client hardware address. Where there is a mismatch, DHCP snooping logs and drops the packet.

This command displays, for each enabled untrusted interface, the number of source MAC verification failures and client interface mismatches that occurred since the last time these statistics were cleared.

Since DHCP servers should not be connected through an untrusted port, the DHCP snooping application will drop incoming DHCP server messages on untrusted interfaces and increment a counter that is displayed with this command.

### Example

This example shows the output of the **show dhcpsnooping statistics** command.

```
B5(su)->show dhcpsnooping statistics
  Interface   MAC Verify   Client Ifc   DHCP Server
             Failures     Mismatch     Msgs Rec'd
-----
ge.1.48      0            0            0
lag.0.1      0            0            0
```

## clear dhcp snooping binding

Use this command to remove bindings from the DHCP snooping bindings database.

### Syntax

```
clear dhcp snooping binding [port port-string | mac mac-addr]
```

### Parameters

---

<b>port</b> <i>port-string</i>	(Optional) Specifies the entry or entries to remove by port identifier.
<b>mac</b> <i>mac-addr</i>	(Optional) Specifies the entry to remove by MAC address.

---

### Defaults

If no parameters are entered, all bindings (static and dynamic) are removed.

### Mode

Switch command, read-write.

### Example

This example clears the static binding entry that includes port ge.1.2.

```
B5(su)->clear dhcp snooping binding port ge.1.2
```

## clear dhcp snooping statistics

Use this command to clear the DHCP snooping statistics counters.

### Syntax

```
clear dhcp snooping statistics
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example clears the DHCP snooping statistics counters for all enabled untrusted ports.

```
B5(su)->clear dhcp snooping statistics
```

## clear dhcp snooping database

Use this command to return the write delay value to its default value of 300 seconds.



## Syntax

```
clear dhcp snooping database [write-delay]
```

## Parameters

---

<b>write-delay</b>	(Optional) Specifies that the write delay value should be returned to the default value of 300 seconds.
--------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command will set the database write delay value to the default of 300 seconds.

## Example

This example sets the database storage location to the default of local.

```
B5(su)->clear dhcp snooping database
```

# clear dhcp snooping limit

Use this command to reset the rate limit values to the defaults of 15 packets per second with a burst interval of 1 second.

## Syntax

```
clear dhcp snooping limit port-string
```

## Parameters

---

<i>port-string</i>	Specifies the port or ports to which this command applies.
--------------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example resets the rate limit values to their defaults on port ge.1.1.

```
B5(su)->clear dhcp snooping limit ge.1.1
```

## Dynamic ARP Inspection Overview

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. ARP poisoning is a tactic where an attacker injects false ARP packets into the subnet, normally by broadcasting ARP responses in which the attacker claims to be someone else. By poisoning the ARP cache, a malicious user can intercept the traffic intended for other hosts on the network.

The Dynamic ARP Inspection application performs ARP packet validation. When DAI is enabled, it verifies that the sender MAC address and the source IP address are a valid pair in the DHCP snooping binding database and drops ARP packets whose sender MAC address and sender IP address do not match an entry in the database. Additional ARP packet validation can be configured.

If DHCP snooping is disabled on the ingress VLAN or the receive interface is trusted for DHCP snooping, ARP packets are dropped.

### Functional Description

DAI is enabled on VLANs, effectively enabling DAI on the interfaces (physical ports or LAGs) that are members of that VLAN. Individual interfaces are configured as trusted or untrusted. The trust configuration for DAI is independent of the trust configuration for DHCP snooping. A trusted port is a port the network administrator does not consider to be a security threat. An untrusted port is one which could potentially be used to launch a network attack.

DAI considers all physical ports and LAGs untrusted by default.

### Static Mappings

Static mappings are useful when hosts configure static IP addresses, DHCP snooping cannot be run, or other switches in the network do not run dynamic ARP inspection. A static mapping associates an IP address to a MAC address on a VLAN. DAI consults its static mappings before it consults DHCP snooping — thus, static mappings have precedence over DHCP snooping bindings.

ARP ACLs are used to define static mappings for DAI. In this implementation, only the subset of ARP ACL syntax required for DAI is supported. ARP ACLs are completely independent of ACLs used for QoS. A maximum of 100 ARP ACLs can be configured. Within an ACL, a maximum of 20 rules can be configured.

### Optional ARP Packet Validation

If optional ARP packet validation has been configured, DAI verifies that the sender MAC address equals the source MAC address in the Ethernet header. Additionally, the option to verify that the target MAC address equals the destination MAC address in the Ethernet header can be configured. This check only applies to ARP responses, since the target MAC address is unspecified in ARP requests.

You can also enable IP address checking. When this option is enabled, DAI drops ARP packets with an invalid IP address. The following IP addresses are considered invalid:

- 0.0.0.0
- 255.255.255.255
- All IP multicast addresses
- All class E addresses (240.0.0.0/4)

- Loopback addresses (in the range 127.0.0.0/8)

## Logging Invalid Packets

By default, DAI writes a log message to the normal buffered log for each invalid ARP packet it drops. You can configure DAI to not log invalid packets for specific VLANs.

## Packet Forwarding

DAI forwards valid ARP packets whose destination MAC address is not local. The ingress VLAN could be a switching or routing VLAN. ARP requests are flooded in the VLAN. ARP responses are unicast toward their destination. DAI queries the MAC address table to determine the outgoing port. If the destination MAC address is local, DAI gives valid ARP packets to the ARP application.

## Rate Limiting

To protect the switch from DHCP attacks when DAI is enabled, the DAI application enforces a rate limit for ARP packets received on untrusted interfaces. DAI monitors the receive rate on each interface separately. If the receive rate exceeds a configurable limit, DAI error disables the interface, which effectively brings down the interface. You can use the **set port enable** command to reenable the port.

You can configure both the rate and the burst interval. The default rate is 15 pps on each untrusted interface with a range of 0 to 50 pps. The default burst interval is 1 second with a range to 1 to 15 seconds.. The rate limit cannot be set on trusted interfaces since ARP packets received on trusted interfaces do not come to the CPU.

## Eligible Interfaces

Dynamic ARP inspection is enabled per VLAN, effectively enabling DAI on the members of the VLAN, either physical ports or LAGs. Trust is specified on the VLAN members.

DAI may be connected to:

- A single host through a trusted link (for example, a server)
- If multiple hosts need to be connected, there must be a switch between the router and the hosts, with DAI enabled on that switch

## Interaction with Other Functions

- DAI relies on the DHCP snooping application to verify that a {IP address, MAC address, VLAN, interface} tuple is valid.
- DAI registers with dot1q to receive notification of VLAN membership changes for the VLANs where DAI is enabled.
- DAI tells the driver about each untrusted interface (physical port or LAG) where DAI is enabled so that the hardware will intercept ARP packets and send them to the CPU.

## Basic Configuration

The following basic configuration does not change the default rate limiting parameters.

### Procedure 17-2 Basic Dynamic ARP Inspection Configuration

Step	Task	Command(s)
1.	Configure DHCP snooping.	Refer to <a href="#">Procedure 17-1</a> on page 17-3.
2.	Enable ARP inspection on the VLANs where clients are connected, and optionally, enable logging of invalid ARP packets.	<code>set arpinspection vlan <i>vlan-range</i> [logging]</code>
3.	Determine which ports are not security threats and configure them as DAI trusted ports.	<code>set arpinspection trust port <i>port-string</i> enable</code>
4.	If desired, configure optional validation parameters.	<code>set arpinspection validate {[src-mac] [dst-mac] [ip]}</code>
5.	If desired, configure static mappings for DAI by creating ARP ACLs: <ul style="list-style-type: none"> <li>• Create the ARP ACL</li> <li>• Apply the ACL to a VLAN</li> </ul>	<code>set arpinspection filter <i>name</i> permit ip host <i>sender-ipaddr</i> mac host <i>sender-macaddr</i></code> <code>set arpinspection filter <i>name</i> vlan <i>vlan-range</i> [static]</code>

## Example Configuration



**Note:** This example applies only to platforms that support routing.

The following example configures DHCP snooping and dynamic ARP inspection in a routing environment using RIP. The example configures two interfaces on the switch, configuring RIP on both interfaces, assigning each to a different VLAN, and then enabling DHCP snooping and dynamic ARP inspection on them:

- Interface ge.1.1, which is connected to a remote DHCP server, on VLAN 192
- Interface ge.1.2, which is connected to DHCP clients, on VLAN 10

In addition, the default VLAN, VLAN 1, is also enabled for DHCP snooping and dynamic ARP inspection.

Since the DHCP server is remote, the switch has been configured as a DHCP relay agent (with the **ip helper-address** command), to forward client requests to the DHCP server. Therefore, MAC address verification is disabled (with the **set dhcp snooping verify mac-address disable** command) in order to allow DHCP RELEASE packets to be processed by the DHCP snooping functionality and client bindings removed from the bindings database

### Router Configuration

```
router
enable
configure
interface vlan 10
no shutdown
ip address 10.2.0.1 255.255.0.0
ip helper-address 192.168.0.200
ip rip send version 2
ip rip receive version 2
ip rip enable
exit

interface vlan 192
no shutdown
ip address 192.168.0.1 255.255.255.0
ip rip send version 2
ip rip receive version 2
ip rip enable
exit
router rip
exit
```

### VLAN Configuration

```
set vlan create 10
set vlan create 192
clear vlan egress 1 ge.1.1-2
```

```
set vlan egress 10 ge.1.2 untagged
set vlan egress 192 ge.1.1 untagged
```

## DHCP Snooping Configuration

```
set dhcpsnooping enable
set dhcpsnooping vlan 1 enable
set dhcpsnooping vlan 10 enable
set dhcpsnooping vlan 192 enable
set dhcpsnooping verify mac-address disable
set dhcpsnooping trust port ge.1.1 enable
```

## Dynamic ARP Inspection Configuration

```
set arpinspection vlan 1
set arpinspection vlan 10
set arpinspection vlan 192
set arpinspection trust port ge.1.1 enable
```

# Dynamic ARP Inspection Commands

For information about...	Refer to page...
<a href="#">set arpinspection vlan</a>	17-20
<a href="#">set arpinspection trust</a>	17-21
<a href="#">set arpinspection validate</a>	17-22
<a href="#">set arpinspection limit</a>	17-23
<a href="#">set arpinspection filter</a>	17-24
<a href="#">show arpinspection access-list</a>	17-24
<a href="#">show arpinspection ports</a>	17-25
<a href="#">show arpinspection vlan</a>	17-26
<a href="#">show arpinspection statistics</a>	17-26
<a href="#">clear arpinspection validate</a>	17-27
<a href="#">clear arpinspection vlan</a>	17-28
<a href="#">clear arpinspection filter</a>	17-29
<a href="#">clear arpinspection limit</a>	17-30
<a href="#">clear arpinspection statistics</a>	17-31

## set arpinspection vlan

Use this command to enable dynamic ARP inspection on one or more VLANs, and optionally, enable logging of invalid ARP packets.

### Syntax

```
set arpinspection vlan vlan-range [logging]
```

## Parameters

<i>vlan-range</i>	Specifies the VLAN or range of VLANs on which to enable dynamic ARP inspection.
<b>logging</b>	(Optional) Enables logging of invalid ARP packets for that VLAN.

## Defaults

Logging is disabled by default.

## Mode

Switch command, read-write.

## Usage

This command enables dynamic ARP inspection (DAI) on one or more VLANs. When DAI is enabled on a VLAN, DAI is effectively enabled on the interfaces (physical ports or LAGs) that are members of that VLAN.

DAI uses the DHCP snooping bindings database to verify that the sender MAC address and the source IP address are a valid pair in the database. ARP packets whose sender MAC address and sender IP address do not match an entry in the database are dropped.

If logging is enabled, invalid ARP packets are also logged.

## Example

This example enables DAI on VLANs 2 through 5 and also enables logging of invalid ARP packets on those VLANs.

```
B5(su)->set arpinspection vlan 2-5 logging
```

# set arpinspection trust

Use this command to enable or disable a port as a dynamic ARP inspection trusted port.

## Syntax

```
set arpinspection trust port port-string {enable | disable}
```

## Parameters

<i>port-string</i>	Specifies the port or ports to be enabled or disabled as DAI trusted ports. The ports can be physical ports or LAGs that are members of a VLAN.
<b>enable   disable</b>	Enables or disables the specified ports as trusted for DAI.

## Defaults

By default, all physical ports and LAGs are untrusted.

## Mode

Switch command, read-write.

## Usage

Individual interfaces are configured as trusted or untrusted. The trust configuration for DAI is independent of the trust configuration for DHCP snooping. A trusted port is a port the network administrator does not consider to be a security threat. An untrusted port is one which could potentially be used to launch a network attack.

DAI considers all physical ports and LAGs untrusted by default. Packets arriving on trusted interfaces bypass all DAI validation checks.

## Example

This example enables port ge.1.1 as trusted for DAI.

```
B5(su)->set arpinspection trust port ge.1.1 enable
```

## set arpinspection validate

Use this command to configure additional optional ARP validation parameters.

### Syntax

```
set arpinspection validate {[src-mac] [dst-mac] [ip]}
```

### Parameters

<b>src-mac</b>	Specifies that DAI should verify that the sender MAC address equals the source MAC address in the Ethernet header.
<b>dst-mac</b>	Specifies that DAI should verify that the target MAC address equals the destination MAC address in the Ethernet header.  This check only applies to ARP responses, since the target MAC address is unspecified in ARP requests.
<b>ip</b>	Specifies that DAI should check the IP address and drop ARP packets with an invalid address. An invalid address is one of the following: <ul style="list-style-type: none"><li>• 0.0.0.0</li><li>• 255.255.255.255</li><li>• All IP multicast addresses</li><li>• All class E addresses (240.0.0.0/4)</li><li>• Loopback addresses (in the range 127.0.0.0/8)</li></ul>

### Defaults

All parameters are optional, but at least one parameter must be specified.

### Mode

Switch command, read-write.

### Usage

This command adds additional validation of ARP packets by DAI, beyond the basic validation that the ARP packet's sender MAC address and sender IP address match an entry in the DHCP snooping bindings database.



## Example

This example adds the optional verification that sender MAC addresses are the same as the source MAC addresses in the Ethernet headers of ARP packets.

```
B5(su)->set arpinspection validate src-mac
```

## set arpinspection limit

Use this command to configure rate limiting parameters for incoming ARP packets on a port or ports

### Syntax

```
set arpinspection limit port port-string {none | rate pps {burst interval secs}}
```

### Parameters

<i>port-string</i>	Specifies the port or ports to which to apply these rate limiting parameters.
<b>none</b>	Configures no limit on incoming ARP packets.
<b>rate</b> <i>pps</i>	Specifies a rate limit in packets per second. The value of <i>pps</i> can range from 0 to 50 packets per second.
<b>burst interval</b> <i>secs</i>	Specifies a burst interval in seconds. The value of <i>secs</i> can range from 1 to 15 seconds.

### Defaults

Rate = 15 packets per second

Burst Interval = 1 second

### Mode

Switch command, read-write.

### Usage

To protect the switch against DHCP attacks when DAI is enabled, the DAI application enforces a rate limit for ARP packets received on untrusted interfaces. DAI monitors the receive rate on each interface separately. If the receive rate exceeds the limit configured with this command, DAI disables the interface, which effectively brings down the interface. You can use the **set port enable** command to reenab the port.

You can configure both the rate and the burst interval. The default rate is 15 pps on each untrusted interface with a range of 0 to 50 pps. The default burst interval is 1 second with a range to 1 to 15 seconds.. The rate limit cannot be set on trusted interfaces since ARP packets received on trusted interfaces do not come to the CPU.

## Example

This example sets the rate to 20 packets per second and the burst interval to 2 seconds on ports ge.1.1 and ge.1.2.

```
B5(su)->set arpinspection limit port ge.1.1-2 rate 20 burst interval 2
```

## set arpinspection filter

Use this command to create an ARP ACL and then to assign an ACL to a VLAN, optionally as a static mapping.

### Syntax

```
set arpinspection filter name {permit ip host sender-ipaddr mac host
sender-macaddr | vlan vlan-range [static]}
```

### Parameters

<i>name</i>	Specifies the name of the ARP ACL.
<b>permit</b>	Specifies that a permit rule is being created.
<b>ip host</b> <i>sender-ipaddr</i>	Specifies the IP address in the rule being created.
<b>mac host</b> <i>sender-macaddr</i>	Specifies the MAC address in the rule being created.
<b>vlan</b> <i>vlan-range</i>	Specifies the VLAN or VLANs to which this ARP ACL is assigned.
<b>static</b>	(Optional) Specifies that this ARP ACL configures static mappings for the VLAN or VLANs.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

ARP ACLs are used to define static mappings for DAI. ARP ACLs are completely independent of ACLs used for QoS. A maximum of 100 ARP ACLs can be configured. Within an ACL, a maximum of 20 rules can be configured.

A static mapping associates an IP address to a MAC address on a VLAN. DAI consults its static mappings before it consults the DHCP snooping bindings database — thus, static mappings have precedence over DHCP snooping bindings.

### Example

This example creates an ACL named staticARP and creates a permit rule for IP address 192.168.1.10. Then, the ACL is assigned to a VLAN as a static mapping.

```
B5(su)->set arpinspection filter staticARP permit ip host 192.168.1.10 mac host
00:01:22:33:44:55
```

```
B5(su)->set arpinspection filter staticARP vlan 10 static
```

## show arpinspection access-list

Use this command to display ARP access list configuration information.

### Syntax

```
show arpinspection access-list [acl-name]
```

## Parameters

---

<i>acl-name</i>	(Optional) Specifies the ARP ACL to display.
-----------------	--

---

## Defaults

If a specific ACL is not specified, information about all configured ARP ACLs is displayed.

## Mode

Switch command, read-write.

## Example

This example displays information about the ARP ACL named staticARP.

```
B5(su)->show arpinspection access-list staticARP
ARP access list  staticARP
    permit ip host 192.168.1.10 mac host 00:01:22:33:44:55
    permit ip host 192.168.1.20 mac host 00:0A:11:22:33:66
```

# show arpinspection ports

Use this command to display the ARP configuration of one or more ports.

## Syntax

```
show arpinspection ports [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Specifies the port or ports for which to display ARP configuration information.
--------------------	--

---

## Defaults

If a port-string is not specified, information about all DAI-enabled untrusted ports is displayed.

## Mode

Switch command, read-write.

## Example

This example displays the ARP configuration of lag.0.1.

```
B5(su)->show arpinspection ports lag.0.1
Interface      Trust State      Rate Limit      Burst Interval
              (pps)           (seconds)
-----
lag.0.1        No                15                1
```

## show arpinspection vlan

Use this command to display the ARP configuration of one or more VLANs.

### Syntax

```
show arpinspection vlan vlan-range
```

### Parameters

---

<i>vlan-range</i>	Specifies the VLANs for which to display configuration information.
-------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example displays ARP configuration information for VLAN 5.

```
B5(su)->show arpinspection vlan 5
```

```
Source MAC Validation           Disabled
Destination MAC Validation     Disabled
IP Address Validation          Disabled
```

Vlan	Configuration	Log Invalid	ACL Name	Static flag
-----	-----	-----	-----	-----
5	Disabled	Enabled	staticARP	Enabled

## show arpinspection statistics

Use this command to display ARP statistics for all DAI-enabled VLANs or for specific VLANs.

### Syntax

```
show arpinspection statistics [vlan vlan-range]
```

### Parameters

---

<i>vlan vlan-range</i>	(Optional) Specifies the VLANs for which to display statistics.
------------------------	---

---

### Defaults

If no VLANs are specified, limited statistics for all DAI-enabled VLANs is displayed.

### Mode

Switch command, read-write.

### Usage

When no specific VLANs are entered, this command displays the number of Forwarded and Dropped ARP packets per DAI-enabled VLAN. When one or more VLANs are specified, this command displays more detailed statistics.

## Examples

This example shows what is displayed when no VLANs are specified.

```
B5(su)->show arpinspection statistics
```

VLAN	Forwarded	Dropped
5	0	0

This example shows what information is displayed when one or more VLANs are specified.

```
B5(su)->show arpinspection statistics vlan 5
```

VLAN	DHCP Drops	ACL Drops	DHCP Permits	ACL Permits	Bad Src MAC	Bad Dest MAC	Invalid IP
5	0	0	0	0	0	0	0

## clear arpinspection validate

Use this command to remove additional optional ARP validation parameters that were previously configured.

### Syntax

```
clear arpinspection validate {[src-mac] [dst-mac] [ip]}
```

### Parameters

<b>src-mac</b>	Clear, or remove, the verification that the sender MAC address equals the source MAC address in the Ethernet header.
<b>dst-mac</b>	Clear, or remove, the verification that the target MAC address equals the destination MAC address in the Ethernet header.
<b>ip</b>	Clear, or remove, checking the IP address and dropping ARP packets with an invalid address.

### Defaults

All parameters are optional, but at least one parameter must be specified.

### Mode

Switch command, read-write.

### Usage

This command removes previously configured additional validation of ARP packets by DAI, beyond the basic validation that the ARP packet's sender MAC address and sender IP address match an entry in the DHCP snooping bindings database.

Use the **show arpinspection vlan** command to display the current status of the additional validation rules.

### Example

This example removes all 3 additional validation conditions.

```
B5(su)->clear arpinspection validate src-mac dst-mac ip
```

## clear arpinspection vlan

Use this command to disable dynamic ARP inspection on one or more VLANs or to disable logging of invalid ARP packets on one or more VLANs.

### Syntax

```
clear arpinspection vlan vlan-range [logging]
```

### Parameters

<i>vlan-range</i>	Specifies the VLAN or range of VLANs on which to disable dynamic ARP inspection.
<b>logging</b>	(Optional) Disable logging of invalid ARP packets for the specified VLANs.

### Defaults

If logging is enabled for the specified VLAN but **logging** is not entered with this command, logging will remain enabled.

### Mode

Switch command, read-write.

### Usage

You can use this command to disable dynamic ARP inspection on one or more VLANs, or you can disable logging of invalid ARP packets on specified VLANs. To disable both logging and DAI, you must enter this command twice.

### Example

This example first displays the DAI configuration for VLAN 5, then disables DAI on VLAN 5, then disables logging of invalid ARP packets on VLAN 5.

```
B5(su)->show arpinspection vlan 5
```

```
Source MAC Validation           Disabled
Destination MAC Validation      Disabled
IP Address Validation           Disabled
```

Vlan	Configuration	Log Invalid	ACL Name	Static flag
5	Enabled	Enabled	staticARP	Enabled

```
B5(su)->clear arpinspection vlan 5
```

```
B5(su)->show arpinspection vlan 5
```

```
Source MAC Validation           Disabled
Destination MAC Validation      Disabled
IP Address Validation           Disabled
```

Vlan	Configuration	Log Invalid	ACL Name	Static flag
5	Disabled	Enabled	staticARP	Enabled

```
B5(su)->clear arpinspection vlan 5 logging
```

```
B5(su)->show arpinspection vlan 5
```

```
Source MAC Validation           Disabled
Destination MAC Validation     Disabled
IP Address Validation          Disabled
```

Vlan	Configuration	Log Invalid	ACL Name	Static flag
5	Disabled	Disabled	staticARP	Enabled

## clear arpinspection filter

Use this command to remove an ARP ACL from a VLAN or from the switch, or to remove a permit rule from an existing ACL, or to change the status of static mapping to disabled.

### Syntax

```
clear arpinspection filter name [permit ip host sender-ipaddr mac host
sender-macaddr] | [vlan vlan-range [static]
```

### Parameters

<i>name</i>	Specifies the name of the ARP ACL.
<b>permit</b>	(Optional) Specifies that a permit rule is being deleted.
<b>ip host</b> <i>sender-ipaddr</i>	Specifies the IP address in the rule being deleted.
<b>mac host</b> <i>sender-macaddr</i>	Specifies the MAC address in the rule being deleted.
<b>vlan</b> <i>vlan-range</i>	(Optional) Specifies the VLAN or VLANs to which this command should apply. Remove the ACL from the VLAN, if <b>static</b> is not specified also.
<b>static</b>	(Optional) Specifies that static mapping should be disabled for this ARP ACL for the specified VLAN or VLANs.

### Defaults

If only the name is specified, the ACL is deleted from the switch.

### Mode

Switch command, read-write.

### Usage

You can use this command to:

- Remove a configured ARP ACL from the switch, or
- Remove a permit rule from a configured ARP ACL, or
- Remove the association of an ARP ACL with a VLAN or VLANs, or
- Disable static mapping of an ARP ACL associated with a VLAN or VLANs.

Use the **set arpinspection filter** command to create and assign an ARP ACL.

Use the **show arpinspection access-list** command to display currently configured ARP ACLs.

## Examples

This example removes a permit rule from the ARP ACL named staticARP.

```
B5(su)->clear arpinspection filter staticARP permit ip host 192.168.1.10 mac host 00:01:22:33:44:55
```

This example disables static mapping of the ARP ACL named staticARP that is associated with VLAN 5.

```
B5(su)->clear arpinspection filter staticARP vlan 5 static
```

This example removes the ARP ACL named staticARP from VLAN 5.

```
B5(su)->clear arpinspection filter staticARP vlan 5
```

This example removes the ARP ACL named staticARP from the switch completely.

```
B5(su)->clear arpinspection filter staticARP
```

## clear arpinspection limit

Use this command to return the DAI rate limiting values to their default values for a port or range of ports.

### Syntax

```
clear arpinspection limit port port-string
```

### Parameters

---

<i>port-string</i>	Specifies the ports on which to return the rate limiting values to defaults.
--------------------	--

---

### Defaults

Rate = 15 packets per second

Burst Interval = 1 second

### Mode

Switch mode, read-write.

### Usage

Use the **set arpinspection limit** command to change the values of the rate limit and burst interval.

Use the **show arpinspection ports** command to display the currently configured rate limits.

### Example

This example returns the DAI rate limiting values to their defaults for port ge.1.1.

```
B5(su)->clear arpinspection limit port ge.1.1
```



---

## clear arpinspection statistics

Use this command to clear all dynamic ARP inspection statistics.

### Syntax

```
clear arpinspection statistics
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example clears all DAI statistics from the switch.

```
B5(su)->clear arpinspection statistics
```



## Preparing for Router Mode

This chapter describes how to prepare the switch for routing.

For information about...	Refer to page...
<a href="#">Pre-Routing Configuration Tasks</a>	18-1
<a href="#">Enabling Router Configuration Modes</a>	18-2

### Pre-Routing Configuration Tasks

Startup and general configuration of the Enterasys B5 switch must occur from the switch CLI. For details on how to start the switch and configure general platform settings, refer to [Chapter 1, Introduction](#), [Chapter 2, Configuring Switches in a Stack](#), and [Chapter 3, Basic Configuration](#).

Once startup and general switch settings are complete, IP configuration and other router-specific commands can be executed when the switch is in router mode. For details on how to enable router mode from the switch CLI, refer to [Table 18-2](#) in [Enabling Router Configuration Modes](#).

The following pre-routing tasks must be performed from the switch CLI:

- Starting up the CLI. (“[Using the Command Line Interface](#)” on page 1-6)
- Setting the system password. (“[set password](#)” on page 3-5)
- Configuring basic platform settings, such as host name, system clock, and terminal display settings. (“[Setting Basic Switch Properties](#)” on page 3-9)
- Setting the system IP address. (“[set ip address](#)” on page 3-10)
- Creating and enabling VLANs. ([Chapter 10](#))
- File management tasks, including uploading or downloading flash or text configuration files, and displaying directory and file contents. (“[Managing Switch Configuration and Files](#)” on page 3-38)
- Configuring the switch to run in router mode. (“[Enabling Router Configuration Modes](#)” on page 18-2)



**Note:** The command prompts used as examples in [Table 18-1](#) and throughout this guide show switch operation for a user in admin (su) access mode, and a system where the VLAN 1 interface has been configured for routing. The prompt changes depending on your current configuration mode, your specific switch, and the interface types and numbers configured for routing on your system.

**Table 18-1 Enabling the Switch for Routing**

Step	To do this task...	Type this command...	At this prompt...	For details, see...
1	From admin (su) mode, enable router mode.	<b>router</b>	<b>Switch:</b> B5(su)->	
2	Enable router Privileged EXEC mode.	<b>enable</b>	<b>Router:</b> B5(su)->router>	
3	Enable global router configuration mode.	<b>configure</b>	<b>Router:</b> B5(su)->router#	
4	Enable interface configuration mode using the routing VLAN or loopback id.	<b>interface</b> {vlan <i>vlan-id</i>   <b>loopback</b> <i>loop-id</i> }	<b>Router:</b> B5(su)->router(Config)#	<a href="#">"interface"</a> on page 19-2
5	Assign an IP address to the routing interface.	<b>ip address</b> { <i>ip-address ip-mask</i> }	<b>Router:</b> B5(su)->router (Config-if (Vlan 1))#	<a href="#">"interface"</a> on page 19-2
6	Enable the interface for IP routing.	<b>no shutdown</b>	<b>Router:</b> B5(su)->router(Config-if (Vlan 1))#	<a href="#">"no shutdown"</a> on page 19-6

## Example

The following example shows how to configure VLAN 1 on IP address 182.127.63.1 255.255.255.0 as a routing interface.

```
B5(su)->router
B5(su)->router>enable
B5(su)->router#configure
  Enter configuration commands:
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip address 182.127.63.1 255.255.255.0
B5(su)->router(Config-if(Vlan 1))#no shutdown
```

## Enabling Router Configuration Modes

The Enterasys B5 CLI provides different modes of router operation for issuing a subset of commands from each mode. [Table 18-2](#) describes these modes of operation.

**Table 18-2 Router CLI Configuration Modes**

Use this mode...	To...	Access method...	Resulting Prompt...
Privileged EXEC Mode	Set system operating parameters	From the switch CLI: Type <b>router</b> , then	B5(su)->router>
	Show configuration parameters	Type <b>enable</b> .	B5(su)->router#
	Save/copy configurations		
Global Configuration Mode	Set system-wide parameters.	Type <b>configure</b> from Privileged EXEC mode.	B5(su)->router (Config)#
Interface Configuration Mode	Configure router interfaces.	Type <b>interface vlan</b> or <b>loopback</b> and the interface's id from Global Configuration mode.	B5(su)->router(Config-if (Vlan 1))# B5(su)->router(Config-if (Lpbk 1))#

**Table 18-2 Router CLI Configuration Modes (Continued)**

Use this mode...	To...	Access method...	Resulting Prompt...
Router Configuration Mode	Set IP protocol parameters.	Type <b>router</b> and the protocol <i>name</i> from Global or Interface Configuration mode.	B5(su)->router(Config-router)#



**Note:** To jump to a lower configuration mode, type **exit** at the command prompt. To revert back to switch CLI, type **exit** from Privileged EXEC router mode.



## IP Configuration

This chapter describes the Internet Protocol (IP) configuration set of commands and how to use them.



**Router:** Unless otherwise noted, the commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to “[Enabling Router Configuration Modes](#)” on page 18-2.

For information about...	Refer to page...
<a href="#">Configuring Routing Interface Settings</a>	<a href="#">19-1</a>
<a href="#">Reviewing and Configuring the ARP Table</a>	<a href="#">19-8</a>
<a href="#">Configuring Broadcast Settings</a>	<a href="#">19-12</a>
<a href="#">Reviewing IP Traffic and Configuring Routes</a>	<a href="#">19-15</a>
<a href="#">Configuring ICMP Redirects</a>	<a href="#">19-18</a>

## Configuring Routing Interface Settings

### Purpose

To enable routing interface configuration mode on the device, to create routing interfaces, to review the usability status of interfaces configured for IP, to set IP addresses for interfaces, to enable interfaces for IP routing at device startup, and to review the running configuration.

### Commands

For information about...	Refer to page...
<code>show interface</code>	<a href="#">19-2</a>
<code>interface</code>	<a href="#">19-2</a>
<code>show ip interface</code>	<a href="#">19-4</a>
<code>ip address</code>	<a href="#">19-5</a>
<code>no shutdown</code>	<a href="#">19-6</a>
<code>no ip routing</code>	<a href="#">19-6</a>
<code>show running-config</code>	<a href="#">19-7</a>

## show interface

Use this command to display information about one or more interfaces (VLANs or loopbacks) configured on the router.

### Syntax

```
show interface [vlan vlan-id] [loopback loop-id]
```

### Parameters

<b>vlan</b> <i>vlan-id</i>	(Optional) Displays interface information for a specific VLAN interface. This interface must be configured for IP routing as described in “ <a href="#">Pre-Routing Configuration Tasks</a> ” on page 18-1.
<b>loopback</b> <i>loop-id</i>	(Optional) Displays interface information for a specific loopback interface.

### Defaults

If interface type is not specified, information for all routing interfaces will be displayed.

### Mode

Any router mode.

### Examples

This example shows how to display information for all interfaces configured on the router. For a detailed description of this output, refer to [Table 19-1](#):

```
B5(su)->router#show interface
Vlan 1 is Administratively DOWN
Vlan 1 is Operationally DOWN
Internet Address is 10.10.1.1 , Subnet Mask is 255.255.255.0
Mac Address is: 001F.4554.EAA5
The name of this device is Vlan 1
The MTU is 1500 bytes
The bandwidth is 0 Mb/s
Encapsulation type Ethernet
ARP Timeout: 14400 seconds
```

This example shows how to display information for loopback interface 1.

```
B5(su)->router#show interface loopback 1

Loopback 1 is Administratively UP
Loopback 1 is Operationally UP
Internet Address is 10.1.192.100, Subnet Mask is 255.255.255.0
The name of this device is Loopback 1
The MTU is 1500 bytes
```

## interface

Use this command to configure interfaces for IP routing.

### Syntax

```
interface vlan vlan-id | loopback loop-id
```



## Parameters

<b>vlan</b> <i>vlan-id</i>	Specifies the number of the VLAN interface to be configured for routing. This interface must be configured for IP routing as described in “ <a href="#">Pre-Routing Configuration Tasks</a> ” on page 18-1.
<b>loopback</b> <i>loop-id</i>	Specifies the number of the loopback interface to be configured for routing. The value of <i>loop-id</i> can range from 0 to 7.

## Defaults

None.

## Mode

Router global configuration mode: B5(su)->router(Config)#

## Usage

This command enables interface configuration mode from global configuration mode, and, if the interface has not previously been created, this command creates a new routing interface. For details on configuration modes supported by the Enterasys B5 device and their uses, refer to [Table 18-2](#) in “[Enabling Router Configuration Modes](#)” on page 18-2.

VLANs must be created from the switch CLI before they can be configured for IP routing. For details on creating VLANs and configuring them for IP, refer to “[Enabling Router Configuration Modes](#)” on page 18-2.

Each VLAN interface must be configured for routing separately using the **interface** command. To end configuration on one interface before configuring another, type **exit** at the command prompt. Enabling interface configuration mode is required for completing interface-specific configuration tasks. For an example of how these commands are used, refer to “[Pre-Routing Configuration Tasks](#)” on page 18-1.

A loopback interface is always expected to be up. This interface can provide the source address for sent packets and can receive both local and remote packets. The loopback interface is typically used by routing protocols, but it can also be used for management or network services such as RADIUS, SNMP, Syslog, SNTP, or sFlow. By default, if RADIUS is configured with no host IP address on the device, it will use the loopback interface 0 IP address (if it has been configured) as its source for the NAS-IP attribute. (Administrators can assign where to source management or network service IP packets via the **set interface** commands.)

Each Enterasys B5 system (stack) can support up to 24 routing interfaces. Each interface can be configured for the RIP routing protocol.

## Examples

This example shows how to enter configuration mode for VLAN 1:

```
B5(su)->router#configure
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#
```

This example shows how to enter configuration mode for loopback 1:

```
B5(su)->router#configure
B5(su)->router(Config)#interface loopback 1
B5(su)->router(Config-if(Lpbk 1))#
```

## show ip interface

Use this command to display information, including administrative status, IP address, MTU (Maximum Transmission Unit) size and bandwidth, and ACL configurations, for interfaces configured for IP.

### Syntax

```
show ip interface [vlan vlan-id] [loopback loop-id]
```

### Parameters

<b>vlan</b> <i>vlan-id</i>	(Optional) Displays information for a specific VLAN interface. This interface must be configured for IP routing as described in <a href="#">“Pre-Routing Configuration Tasks”</a> on page 18-1.
<b>loopback</b> <i>loop-id</i>	(Optional) Displays interface information for a specific loopback interface.

### Defaults

If interface type is not specified, status information for all routing interfaces will be displayed.

### Mode

Any router mode.

### Example

This example shows how to display configuration information for VLAN 1:

```
B5(su)->router#show ip interface vlan 1
```

```
Vlan 1 is Admin DOWN
Vlan 1 is Oper DOWN
Primary IP Address is 192.168.10.1    Mask 255.255.255.0
Frame Type Ethernet
MAC-Address 0001.F45C.C993
Incoming Accesslist is not set
MTU is 6145 bytes
ARP Timeout is 1 seconds
Direct Broadcast Disabled
Proxy ARP is Disabled
```

[Table 19-1](#) provides an explanation of the command output.

**Table 19-1 show ip interface Output Details**

Output Field	What It Displays...
Vlan <i>N</i>	Whether the interface is administratively and operationally up or down.
Primary IP Address	Interface's primary IP address and mask. Set using the <b>ip address</b> command as described in <a href="#">“ip address”</a> on page 19-5.
Frame Type	Encapsulation type used by this interface. Set using the <b>arp</b> command as described in <a href="#">“arp”</a> on page 19-9.
MAC-Address	MAC address mapped to this interface.
Incoming Access List	Whether or not an access control list (ACL) has been configured for ingress on this interface using the commands described in <a href="#">“Configuring Access Lists”</a> on page 22-82.

**Table 19-1 show ip interface Output Details (Continued)**

Output Field	What It Displays...
MTU	Interface's Maximum Transmission Unit size.
ARP Timeout	Duration for entries to stay in the ARP table before expiring. Set using the <b>arp timeout</b> command as described in "arp timeout" on page 19-11.
Direct Broadcast	Whether or not IP directed broadcast is enabled. Set using the <b>ip directed-broadcast</b> command described in "ip directed-broadcast" on page 19-12.
Proxy Arp	Whether or not proxy ARP is enabled or disabled for this interface. Set using the <b>ip proxy arp</b> command as described in "ip proxy-arp" on page 19-10.

This example shows the output for a loopback interface.

```
B5(su)->router#show ip interface loopback 2

Loopback 2 is Admin UP
Loopback 2 is Oper DOWN
Primary IP Address is 10.10.10.10      Mask  255.255.255.0
```

## ip address

Use this command to set, remove, or disable a primary or secondary IP address for an interface. The **no** form of this command removes the specified IP address and disables the interface for IP processing.

### Syntax

```
ip address ip-address ip-mask [secondary]
no ip address ip-address ip-mask
```

### Parameters

<i>ip-address</i>	Specifies the IP address of the interface to be added or removed.
<i>ip-mask</i>	Specifies the mask for the associated IP subnet.
<b>secondary</b>	(Optional) Specifies that the configured IP address is a secondary address.

### Defaults

If **secondary** is not specified, the configured address will be the primary address for the interface.

### Mode

Router interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Usage

Refer to the Router Capacities table in the Release Notes for this product for the number of primary and secondary IP interfaces supported by this product.

### Example

This example sets the IP address to 192.168.1.1 and the network mask to 255.255.255.0 for VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip address 192.168.1.1 255.255.255.0
```

## no shutdown

Use this command to enable an interface for IP routing and to allow the interface to automatically be enabled at device startup.

### Syntax

```
no shutdown
shutdown
```

### Parameters

None.

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Usage

The shutdown form of this command disables an interface for IP routing.

### Example

This example shows how to enable VLAN 1 for IP routing:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#no shutdown
```

## no ip routing

Use this command to disable IP routing on the device. By default, IP routing is enabled when interfaces are configured for it as described in “[Configuring Routing Interface Settings](#)” on page 19-1.

### Syntax

```
no ip routing
```

### Parameters

None.

### Mode

Global configuration: B5(su)->router(Config)#

### Defaults

None.

### Example

This example shows how to disable IP routing on the device:

```
B5(su)->router(Config)#no ip routing
```

---

## show running-config

Use this command to display the non-default, user-supplied commands entered while configuring the device.

### Syntax

```
show running-config
```

### Parameters

None.

### Defaults

None.

### Mode

Any router mode.

### Example

This example shows how to display the current router operating configuration:

```
B5(su)->router#show running-config
!
interface vlan 10
  ip address 99.99.2.10 255.255.255.0
  no shutdown
!
router
  network 99.99.2.0      0.0.0.255
  network 192.168.100.1 0.0.0.0
```

# Reviewing and Configuring the ARP Table

## Purpose

To review and configure the routing ARP table, to enable proxy ARP on an interface, and to set a MAC address on an interface.

## Commands

For information about...	Refer to page...
show ip arp	<a href="#">19-8</a>
arp	<a href="#">19-9</a>
ip proxy-arp	<a href="#">19-10</a>
arp timeout	<a href="#">19-11</a>
clear arp-cache	<a href="#">19-11</a>

## show ip arp

Use this command to display entries in the ARP (Address Resolution Protocol) table. ARP converts an IP address into a physical address.

### Syntax

```
show ip arp [ip-address] [vlan vlan-id] [output-modifier]
```

### Parameters

<i>ip-address</i>	(Optional) Displays ARP entries related to a specific IP address.
<b>vlan</b> <i>vlan-id</i>	(Optional) Displays only ARP entries learned through a specific VLAN interface. This VLAN must be configured for IP routing as described in <a href="#">“Pre-Routing Configuration Tasks”</a> on page 18-1.
<i>output-modifier</i>	(Optional) Displays ARP entries within a specific range. Options are: <ul style="list-style-type: none"> <li>–   <b>begin</b> <i>ip-address</i> — Displays only ARP entries that begin with the specified IP address.</li> <li>–   <b>exclude</b> <i>ip-address</i> — Excludes ARP entries matching the specified IP address.</li> <li>–   <b>include</b> <i>ip-address</i> — Includes ARP entries matching the specified IP address.</li> </ul>

### Defaults

If no parameters are specified, all entries in the ARP cache will be displayed.

### Mode

Any router mode.

## Example

This example shows how to use the **show ip arp** command:

```
B5(su)->router#show ip arp
```

```
Protocol      Address          Age (min) Hardware Addr  Interface
-----
Internet     134.141.235.251  0          0003.4712.7a99  Vlan1
Internet     134.141.235.165  -          0002.1664.a5b3  Vlan1
Internet     134.141.235.167  4          00d0.cf00.4b74  Vlan2
```

```
B5(su)->router#show ip arp 134.141.235.165
```

```
Protocol      Address          Age (min) Hardware Addr  Interface
-----
Internet     134.141.235.165  -          0002.1664.a5b3  Vlan2
```

```
B5(su)->router#show ip arp vlan 2
```

```
Protocol      Address          Age (min) Hardware Addr  Interface
-----
Internet     134.141.235.251  0          0003.4712.7a99  Vlan2
```

[Table 19-2](#) provides an explanation of the command output.

**Table 19-2 show ip arp Output Details**

Output Field	What It Displays...
Protocol	ARP entry's type of network address.
Address	Network address mapped to the entry's MAC address.
Age (min)	Interval (in minutes) since the entry was entered in the table.
Hardware Addr	MAC address mapped to the entry's network address.
Interface	Interface (VLAN or loopback) through which the entry was learned.

## arp

Use this command to add or remove permanent (static) ARP table entries. A multicast MAC address can be used in a static ARP entry. The **no** form of this command removes the specified permanent ARP entry:

### Syntax

```
arp ip-address mac-address
no arp ip-address
```

### Parameters

<i>ip-address</i>	Specifies the IP address of a device on the network. Valid values are IP addresses in dotted decimal notation.
<i>mac-address</i>	Specifies the 48-bit hardware address corresponding to the <i>ip-address</i> expressed in hexadecimal notation.

## Defaults

None.

## Mode

Global configuration: B5(su)->router(Config)#

## Usage

The IP address specified for the static ARP entry must fall within one of the subnets or networks defined on the routed interfaces of the system ( or stack, if applicable). The system can then match the IP address of the static ARP entry with the appropriate routed interface and associate it with the correct VLAN.

Refer to the Router Capacities table in the Release Notes for this product for a listing of the number of static ARP entries supported by this product.

## Example

This example shows how to add a permanent ARP entry for the IP address 130.2.3.1 and MAC address 0003.4712.7a99:

```
B5(su)->router(Config)#arp 130.2.3.1 0003.4712.7a99
```

# ip proxy-arp

Use this command to enable proxy ARP on an interface. The **no** form of this command disables proxy ARP.

## Syntax

```
ip proxy-arp  
no ip proxy-arp
```

## Parameters

None.

## Defaults

Disabled.

## Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Usage

This variation of the ARP protocol allows the router to send an ARP response on behalf of an end node to the requesting host. Proxy ARP can be used to resolve routing issues on end stations that are unable to route in the subnetted environment. The Enterasys B5 will answer to ARP requests on behalf of targeted end stations on neighboring networks. It is disabled by default.

## Example

This example shows how to enable proxy ARP on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1  
B5(su)->router(Config-if(Vlan 1))#ip proxy-arp
```



---

## arp timeout

Use this command to set the duration (in seconds) for dynamically learned entries to remain in the ARP table before expiring. The **no** form of this command restores the default value of 14,400 seconds.

```
arp timeout seconds
no arp timeout
```

### Parameters

---

<i>seconds</i>	Specifies the time in seconds that an entry remains in the ARP cache. Valid values are <b>0 - 65535</b> . A value of 0 specifies that ARP entries will never be aged out.
----------------	---

---

### Defaults

14,400 seconds.

### Mode

Global configuration: B5(su)->router(Config)#

### Example

This example shows how to set the ARP timeout to 7200 seconds:

```
B5(su)->router(Config)#arp timeout 7200
```

## clear arp-cache

Use this command to delete all nonstatic (dynamic) entries from the ARP table.

```
clear arp-cache
```

### Parameters

None.

### Mode

Privileged EXEC: B5(su)->router#

### Defaults

None.

### Example

This example shows how to delete all dynamic entries from the ARP table:

```
B5(su)->router#clear arp-cache
```

# Configuring Broadcast Settings

## Purpose

To configure IP broadcast settings. By default, interfaces on the Enterasys B5 do not forward broadcast packets.

## Commands

For information about...	Refer to page...
ip directed-broadcast	<a href="#">19-12</a>
ip forward-protocol	<a href="#">19-13</a>
ip helper-address	<a href="#">19-14</a>

## ip directed-broadcast

Use this command to enable or disable IP directed broadcasts on an interface. By default, interfaces on the Enterasys B5 do not forward directed broadcasts. The **no** form of this command disables IP directed broadcast on the interface.

### Syntax

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

### Parameters

None.

### Defaults

None.

### Mode

Interface configuration: B5(su)->Router1(Config-if(Vlan 1))#

### Usage

Directed broadcast is an efficient mechanism for communicating with multiple hosts on a network while only transmitting a single datagram. A directed broadcast is a packet sent to all hosts on a specific network or subnet. The directed broadcast address includes the network or subnet fields, with the binary bits of the host portion of the address set to one. For example, for a network with the address 192.168.0.0/16, the directed broadcast address would be 192.168.255.255. For a subnet with the address 192.168.12.0/24, the directed broadcast address would be 192.168.12.255.

In order to minimize broadcast DoS attacks, forwarding of directed broadcasts is disabled by default on the Enterasys B5, as recommended by RFC 2644.

If the ability to send directed broadcasts to a network is required, you should enable directed broadcasts only on the one interface that will be transmitting the datagrams. For example, if a Enterasys B5 has five routed interfaces for the 10, 20, 30, 40, and 50 networks, enabling directed

broadcast only on the 30 network interface will allow anyone from any other networks (10, 20, 40, 50) to send directed broadcast to the 30 network.

## Example

This example shows how to enable IP directed broadcasts on VLAN 1:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip directed-broadcast
```

## ip forward-protocol

Use this command to enable UDP broadcast forwarding and specify which protocols will be forwarded.

### Syntax

```
ip forward-protocol udp [port]
no ip forward-protocol udp [port]
```

### Parameters

<b>udp</b>	Specifies UDP as the IP forwarding protocol.
<i>port</i>	(Optional) Specifies a destination port that controls which UDP services are forwarded.

### Defaults

If *port* is not specified, the following defaults are used:

- Trivial File Transfer Protocol (TFTP) (port 69)
- Domain Naming System (port 53)
- Time service (port 37)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS service (port 49)
- EN-116 Name Service (port 42)

### Mode

Router command, Global configuration: B5(su)->router(Config)#

Router interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Usage

In order to actually forward protocols, you must configure an IP helper address on the individual router interfaces with the command “[ip helper-address](#)” (page 19-14).

If a certain service exists inside the node, and there is no need to forward the request to remote networks, the “no” form of this command should be used to disable the forwarding for the specific port. Such requests will not be automatically blocked from being forwarded just because a service for them exists in the node.

The **no** form of this command removes a UDP port or protocol, disabling forwarding.

## Examples

The following example globally disables IP forwarding for UDP port 69.

```
B5(su)->router(Config)#no ip forward-protocol udp 69
```

The following example disables IP forwarding for UDP port 69 on a specific interface.

```
B5(su)->router(Config)#interface vlan 10
B5(su)->router(Config-if(Vlan 10))#no ip forward-protocol udp 69
```

## ip helper-address

Use this command to enable the DHCP/BOOTP relay agent on a Enterasys B5 routed interface and/or to forward broadcast traffic identified with the `ip forward-protocol` command to a unicast address. Enabling the relay agent allows forwarding of client DHCP/BOOTP requests to a DHCP/BOOTP server that does not reside on the same broadcast domain as the client. Up to 6 IP helper addresses may be configured per interface.

The **no** form of this command disables the forwarding of UDP datagrams to the specified address.

### Syntax

```
ip helper-address address
no ip helper-address address
```

### Parameters

---

<i>address</i>	Address of the host where UDP broadcast packets should be forwarded.
----------------	--

---

### Defaults

None.

### Mode

Interface configuration: B5(su)->Router1(Config-if(Vlan 1))#

### Usage

Typically for DHCP/BootP, when a host requests an IP address, it sends out a DHCP broadcast packet. Normally, the router drops all broadcast packets. However, by executing this command, you enable the routed interface to pass DHCP broadcast frames through, sending them directly to the remote DHCP server's IP address.

The DHCP/BOOTP relay agent will detect DHCP/BOOTP requests based on UDP source and destination ports. It will then make the necessary changes to the packet and send the packet to the DHCP server. The changes include:

- Replacing the destination IP address with the address of the DHCP server,
- Replacing the source IP address with its own address (that is, the IP address of the local routed interface), and
- Within the BOOTP part of the packet, changing the Relay Agent IP address from 0.0.0.0 to the address of the local routed interface.

The last change to the BootP packet "tells" the DHCP server that it needs to assign an IP address that is in the same subnet as the Relay Agent IP. When the response comes from the server, the DHCP/BOOTP relay agent sends it to the host.

For other protocols specified through the `ip forward-protocol` command, the system forwards broadcast UDP traffic as a unicast packet to the specified IP addresses.

## Example

This example show how to have all client DHCP requests for users in VLAN 1 to be forwarded to the remote DHCP server with IP address 192.168.1.28.

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip helper-address 192.168.1.28
```

# Reviewing IP Traffic and Configuring Routes

## Purpose

To review IP traffic and configure routes, to send router ICMP (ping) messages, and to execute traceroute.

## Commands

For information about...	Refer to page...
show ip route	<a href="#">19-15</a>
ip route	<a href="#">19-16</a>
ping	<a href="#">19-17</a>
traceroute	<a href="#">19-17</a>

## show ip route

Use this command to display information about IP routes.

### Syntax

```
show ip route [destination-prefix [destination-prefix-match] | connected | rip |
static | summary]
```

### Parameters

<i>destination-prefix</i> <i>destination-prefix-match</i>	(Optional) Converts the specified address and mask into a prefix and displays any routes that match the prefix.
<b>connected</b>	(Optional) Displays connected routes.
<b>rip</b>	(Optional) Displays routes configured for the RIP routing protocol. For details on configuring RIP, refer to “ <a href="#">Configuring RIP</a> ” on page 20-1.
<b>static</b>	(Optional) Displays static routes.
<b>summary</b>	(Optional) Displays a summary of the IP routing table.

### Defaults

If no parameters are specified, all IP route information will be displayed.

## Mode

Any router mode.

## Usage

The routing table contains all active static routes, all the RIP routes, learned for each network.

## Example

This example shows how to use the **show ip route** command to display all IP route information. A portion of the output is shown:

```
B5(su)->router#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, IA - OSPF interarea
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       E - EGP, i - IS-IS, L1 - IS-IS level-1, LS - IS-IS level-2
       * - candidate default, U - per user static route

R    1.1.1.0/24 [120/2] via 19.0.0.2, Vlan 3803
R    1.2.3.0/24 [120/2] via 19.0.0.2, Vlan 3803
R    1.3.4.0/24 [120/2] via 19.0.0.2, Vlan 3803
R    5.0.0.0/25 [120/2] via 19.0.0.2, Vlan 3803
C    19.0.0.0/30 [0/1] directly connected, Vlan 3803
R    21.21.21.0/30 [120/2] via 19.0.0.2, Vlan 3803
R    24.24.24.0/24 [120/2] via 19.0.0.2, Vlan 3803
R    27.27.27.0/24 [120/2] via 19.0.0.2, Vlan 3803
R    33.9.8.0/28 [120/2] via 19.0.0.2, Vlan 3803
R    34.0.10.192/26 [120/2] via 19.0.0.2, Vlan 3803
R    34.0.11.192/26 [120/2] via 19.0.0.2, Vlan 3803
R    34.0.16.192/26 [120/2] via 19.0.0.2, Vlan 3803
R    34.0.17.192/26 [120/2] via 19.0.0.2, Vlan 3803
R    37.37.37.0/24 [120/2] via 19.0.0.2, Vlan 3803
R    40.1.1.0/24 [120/2] via 19.0.0.2, Vlan 3803
R    50.0.0.0/29 [120/2] via 19.0.0.2, Vlan 3803
R    50.1.1.0/24 [120/2] via 19.0.0.2, Vlan 3803
```

## ip route

Use this command to add or remove a static IP route. The **no** form of this command removes the static IP route.

```
ip route prefix mask dest-addr [distance]
no ip route prefix mask forward-addr
```

## Parameters

<i>prefix</i>	Specifies a destination IP address prefix.
<i>mask</i>	Specifies a destination prefix mask.
<i>dest-addr</i>	Specifies a forwarding (gateway) IP address.
<i>distance</i>	(Optional) Specifies an administrative distance metric for this route. Valid values are 1 (default) to 255. <b>Routes with lower values receive higher preference in route selection.</b>

## Defaults

If *distance* is not specified, the default value of 1 will be applied.

## Mode

Global configuration: B5(su)->router(Config)#

## Example

This example shows how to set IP address 10.1.2.3 as the next hop gateway to destination address 10.0.0.0:

```
B5(su)->router(Config)#ip route 10.0.0.0 255.0.0.0 10.1.2.3
```

# ping

Use this command to test routing network connectivity by sending IP ping requests.

## Syntax

```
ping ip-address
```

## Parameters

<i>ip-address</i>	Specifies the IP address of the system to ping.
-------------------	---

## Defaults

None.

## Mode

Privileged EXEC: B5(su)->router#

## Usage

This command is also available in switch mode.

## Examples

This example shows output from a successful ping to IP address 182.127.63.23:

```
B5(su)->router#ping 182.127.63.23
182.127.63.23 is alive
```

This example shows output from an unsuccessful ping to IP address 182.127.63.24:

```
B5(su)->router#ping 182.127.63.24
no answer from 182.127.63.24
```

# traceroute

Use this command to display a hop-by-hop path through an IP network from the device to a specific destination host. Three ICMP probes will be transmitted for each hop between the source and the traceroute destination.

## Syntax

```
traceroute host
```

## Parameters

<i>host</i>	Specifies a host to which the route of an IP packet will be traced.
-------------	---

## Defaults

None.

## Mode

Privileged EXEC: B5(su)->router#

## Usage

There is also a traceroute command available in switch mode.

## Example

This example shows how to use traceroute to display a round trip path to host 192.141.90.183.

```
B5(su)->router#traceroute 192.141.90.183
Traceroute to 192.141.90.183, 30 hops max, 40 byte packets
 1  10.1.56.1                0.000 ms          0.000 ms          0.000 ms
 2  10.1.48.254              10.000 ms         0.000 ms          0.000 ms
 3  10.1.0.2                  0.000 ms          0.000 ms          0.000 ms
 4  192.141.89.17             0.000 ms          0.000 ms          10.000 ms
 5  192.141.100.13           0.000 ms          10.000 ms         0.000 ms
 6  192.141.100.6            0.000 ms          0.000 ms          10.000 ms
 7  192.141.90.183           0.000 ms          0.000 ms          0.000 ms
```

# Configuring ICMP Redirects

## Purpose

Disable or enable sending ICMP redirect packets to the switch CPU for processing, at a global level and at an interface level. By default, sending ICMP redirects is enabled globally and on all interfaces. Disabling sending ICMP redirects can reduce CPU usage in certain deployments.

## Commands

For information about...	Refer to page...
ip icmp redirect enable	<a href="#">19-18</a>
show ip icmp redirect	<a href="#">19-19</a>

## ip icmp redirect enable

Use this command to enable or disable sending ICMP redirects to the CPU for processing on a global level or on a specific interface. The **no** form of this command disables sending ICMP redirects to the CPU.



## Syntax

```
ip icmp redirect enable
no ip icmp redirect enable
```

## Parameters

None.

## Defaults

By default, sending ICMP redirects to the CPU is enabled globally and on all interfaces.

## Mode

Router global configuration mode: B5(su)->router(Config)#

Interface configuration mode: B5(su)->Router1(Config-if(Vlan 1))#

## Usage

You can use this command in router global configuration mode to enable or disable sending ICMP redirects globally on the switch.

You can use this command in router interface configuration mode to enable or disable sending ICMP redirects only on specific interfaces.

## Examples

This example disables sending ICMP redirects on the interface VLAN 5.

```
B5(su)->router#configure
B5(su)->router(Config)#interface vlan 5
B5(su)->Router1(Config-if(Vlan 5))# no ip icmp redirect enable
```

This example disables sending ICMP redirects globally.

```
B5(su)->router#configure
B5(su)->router(Config)#no ip icmp redirect enable
```

# show ip icmp redirect

Use this command to display the status of sending ICMP redirects at a global or interface level.

## Syntax

```
show ip icmp redirect {status | interface [vlan vlan-id]}
```

## Parameters

<b>status</b>	Display the global ICMP redirect status.
<b>interface</b>	Display ICMP redirect status for interfaces.
<b>vlan</b> <i>vlan-id</i>	(Optional) Display ICMP redirect status for the specified VLAN.

## Defaults

If no VLAN is specified with the **interface** parameter, information for all VLAN interfaces is displayed.

## Mode

Privileged EXEC mode: B5(su)->router#

Router global configuration mode: B5(su)->router(Config)#

## Examples

This example displays the global ICMP redirect status.

```
B5(su)->router#show ip icmp redirect status
Global ICMP Redirect status - Enabled
```

This example displays the ICMP redirect status for VLAN 5.

```
B5(su)->router#show ip icmp redirect interface vlan 5
Vlan Id          Admin Status
-----          -
5                Enabled
```

## IPv4 Routing Protocol Configuration

This chapter describes the IPv4 Routing Protocol Configuration set of commands and how to use them.



**Router:** The commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to [“Enabling Router Configuration Modes”](#) on page 18-2.

For information about...	Refer to page...
<a href="#">Configuring RIP</a>	20-1
<a href="#">Configuring IRDP</a>	20-11

## Configuring RIP

### RIP Configuration Task List and Commands

[Table 20-1](#) lists the tasks and commands associated with RIP configuration. Commands are described in the associated section as shown.

**Table 20-1 RIP Configuration Task List and Commands**

To do this...	Use these commands...
Enable RIP configuration mode.	<a href="#">“router rip”</a> on page 20-2
Enable RIP on an interface.	<a href="#">“ip rip enable”</a> on page 20-7
Configure an administrative distance.	<a href="#">“distance”</a> on page 20-3
Allow reception of a RIP version.	<a href="#">“ip rip send version”</a> on page 20-8
Allow transmission of a RIP version.	<a href="#">“ip rip receive version”</a> on page 20-8
Configure RIP simple authentication.	<a href="#">“ip rip authentication-key”</a> on page 20-9
Configure RIP encrypted authentication.	<a href="#">“ip rip message-digest-key”</a> on page 20-9
Disable automatic route summarization (necessary for enabling CIDR)	<a href="#">“no auto-summary”</a> on page 20-4
Activate split horizon or poison-reverse.	<a href="#">“split-horizon poison”</a> on page 20-4
Suppress sending routing updates.	<a href="#">“passive-interface”</a> on page 20-5

**Table 20-1 RIP Configuration Task List and Commands (Continued)**

To do this...	Use these commands...
Control reception of routing updates	<a href="#">“receive-interface”</a> on page 20-6
Control advertising non-RIP routes.	<a href="#">“redistribute”</a> on page 20-6

## Router Configuration Commands

The following commands are used to enter RIP router configuration mode and to configure RIP routing.

For information about...	Refer to page...
router rip	<a href="#">20-2</a>
distance	<a href="#">20-3</a>
no auto-summary	<a href="#">20-4</a>
split-horizon poison	<a href="#">20-4</a>
passive-interface	<a href="#">20-5</a>
receive-interface	<a href="#">20-6</a>
redistribute	<a href="#">20-6</a>

## router rip

Use this command to enable or disable RIP configuration mode. The **no** form of this command disables RIP.

### Syntax

```
router rip
no router rip
```

### Parameters

None.

### Defaults

None.

### Mode

Global configuration: B5(su)->router(Config)#

### Usage

You must execute the **router rip** command to enable the protocol before completing many RIP-specific configuration tasks. For details on enabling configuration modes, refer to [Table 18-2](#) in [“Enabling Router Configuration Modes”](#) on page 18-2.

## Example

This example shows how to enable RIP:

```
B5(su)->router#configure
B5(su)->router(Config)#router rip
B5(su)->router(Config-router)#
```

## distance

Use this command to configure the administrative distance for RIP routes. The **no** form of this command resets RIP administrative distance to the default value of 120.

### Syntax

```
distance weight
no distance [weight]
```

### Parameters

<i>weight</i>	Specifies an administrative distance for RIP routes. Valid values are <b>1 - 255</b> .
---------------	--

### Defaults

None.

### Mode

Router configuration: B5(su)->router(Config-router)#

### Usage

If several routes (coming from different protocols) are presented to the Enterasys B5, the protocol with the lowest administrative distance will be chosen for route installation. By default, RIP administrative distance is set to 120. The **distance** command can be used to change this value, resetting RIP's route preference in relation to other routes as shown in the table below.

Route Source	Default Distance
Connected	0
Static	1
OSPF	110
RIP	120

## Example

This example shows how to change the default administrative distance for RIP to 1001:

```
B5(su)->router(Config)#router rip
B5(su)->router(Config-router)#distance 100
```

## no auto-summary

Use this command to disable automatic route summarization.

### Syntax

```
no auto-summary  
auto-summary
```

### Parameters

None.

### Defaults

None.

### Mode

Router configuration: B5(su)->router(Config-router)#

### Usage

By default, RIP version 2 supports automatic route summarization, which summarizes subprefixes to the classful network boundary when crossing network boundaries. Disabling automatic route summarization enables CIDR, allowing RIP to advertise all subnets and host routing information on the Enterasys B5 device. To verify which routes are summarized for an interface, use the **show ip route** command as described in “[show ip route](#)” on page 19-15. The reverse of the command re-enables automatic route summarization. By default, RIP auto-summarization affects both RIPv1 and RIPv2 routes.



**Note:** This command is necessary for enabling CIDR for RIP on the Enterasys B5 device.

### Example

This example shows how to disable RIP automatic route summarization:

```
B5(su)->router(Config)#router rip  
B5(su)->router(Config-router)#no auto-summary
```

## split-horizon poison

Use this command to enable or disable split horizon poison-reverse mode for RIP packets. The **no** form of this command disables split horizon poison reverse.

### Syntax

```
split-horizon poison  
no split-horizon poison
```

### Parameters

None.

### Defaults

None.

## Mode

Router configuration: B5(su)->router(Config-router)#

## Usage

Split horizon prevents a network from being advertised out the same interface it was received on. This function is disabled by default.

## Example

This example shows how to disable split horizon poison reverse for RIP packets transmitted on the VLAN 1 interface:

```
B5(su)->router(Config)#router rip
B5(su)->router(Config-router)#no split-horizon poison
```

# passive-interface

Use this command to prevent RIP from transmitting update packets on an interface. The **no** form of this command disables passive interface.

## Syntax

```
passive-interface vlan vlan-id
no passive-interface vlan vlan-id
```

## Parameters

<b>vlan</b> <i>vlan-id</i>	Specifies the number of the VLAN to make a passive interface. This VLAN must be configured for IP routing as described in <a href="#">“Pre-Routing Configuration Tasks”</a> on page 18-1.
----------------------------	---

## Defaults

None.

## Mode

Router configuration: B5(su)->router(Config-router)#

## Usage

This command does not prevent RIP from monitoring updates on the interface.

## Example

This example shows how to set VLAN 2 as a passive interface. No RIP updates will be transmitted on VLAN 2:

```
B5(su)->router(Config)#router rip
B5(su)->router(Config-router)#passive-interface vlan 2
```

## receive-interface

Use this command to allow RIP to receive update packets on an interface. The **no** form of this command denies the reception of RIP updates. By default, receiving is enabled on all routing interfaces.

### Syntax

```
receive-interface vlan vlan-id
no receive-interface vlan vlan-id
```

### Parameters

<b>vlan</b> <i>vlan-id</i>	Specifies the number of the VLAN to make a receive interface. This VLAN must be configured for IP routing as described in <a href="#">“Pre-Routing Configuration Tasks”</a> on page 18-1.
----------------------------	---

### Defaults

None.

### Mode

Router configuration: B5(su)->router(Config-router)#

### Usage

This command does not affect the sending of RIP updates on the specified interface.

### Example

This example shows how to deny the reception of RIP updates on VLAN 2:

```
B5(su)->router(Config)#router rip
B5(su)->router(Config-router)#no receive-interface vlan 2
```

## redistribute

Use this command to allow routing information discovered through non-RIP protocols to be distributed in RIP update messages. The **no** form of this command clears redistribution parameters.

### Syntax

```
redistribute {connected | static} [metric metric value]
no redistribute {connected | stat
```

<b>connected</b>	Specifies that non-RIP routing information discovered via directly connected interfaces will be redistributed.
<b>static</b>	Specifies that non-RIP routing information discovered via static routes will be redistributed. Static routes are those created using the <b>ip route</b> command detailed in <a href="#">“ip route”</a> on page 19-16.
<b>metric</b> <i>metric value</i>	(Optional) Specifies a metric for the connected or static redistribution route. This value should be consistent with the designation protocol.



## Mode

Router configuration: B5(su)->router(Config-router)#

## Defaults

If *metric value* is not specified, 1 will be applied.

## Example

This example shows how to redistribute routing information discovered through static routes will be redistributed into RIP update messages:

```
B5(su)->router(Config)#router rip
B5(su)->router(Config-router)#redistribute static
```

## Interface Configuration Commands

The following commands are used to configure RIP on specific interfaces.

For information about...	Refer to page...
ip rip enable	<a href="#">20-7</a>
ip rip send version	<a href="#">20-8</a>
ip rip receive version	<a href="#">20-8</a>
ip rip authentication-key	<a href="#">20-9</a>
ip rip message-digest-key	<a href="#">20-9</a>

## ip rip enable

Use this command to enable RIP on an interface. The **no** form of this command disables RIP on an interface: By default, RIP is disabled on all interfaces.

### Syntax

```
ip rip enable
no ip rip enable
```

### Parameters

None.

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Example

This example shows how to enable RIP on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip rip enable
```

## ip rip send version

Use this command to set the RIP version for RIP update packets transmitted out an interface. The **no** version of this command sets the version of the RIP update packets to RIPv1.

### Syntax

```
ip rip send version {1 | 2 | r1compatible}  
no ip rip send version
```

### Parameters

<b>1</b>	Specifies RIP version 1. This is the default setting.
<b>2</b>	Specifies RIP version 2.
<b>r1compatible</b>	Specifies that packets be sent as version 2 packets, but transmits these as broadcast packets rather than multicast packets so that systems which only understand RIP version 1 can receive them.

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Example

This example shows how to set the RIP send version to 2 for packets transmitted on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1  
B5(su)->router(Config-if(Vlan 1))#ip rip send version 2
```

## ip rip receive version

Use this command to set the RIP version(s) for RIP update packets accepted on an interface. The **no** version of this command sets the acceptable receive version of the RIP update packets to RIPv1.

### Syntax

```
ip rip receive version {1 | 2 | 1 2 | none}  
no ip rip receive version
```

### Parameters

<b>1</b>	Specifies RIP version 1. This is the default setting.
<b>2</b>	Specifies RIP version 2.
<b>1 2</b>	Specifies RIP versions 1 and 2.
<b>none</b>	Specifies that no RIP routes will be processed on this interface.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Defaults

None.

## Example

This example shows how to set the RIP receive version to 2 for update packets received on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip rip receive version 2
```

## ip rip authentication-key

Use this command to enable or disable a RIP authentication key (password) for use on an interface. The **no** form of this command prevents RIP from using authentication.

### Syntax

```
ip rip authentication-key name
no ip rip authentication-key
```

### Parameters

<i>name</i>	Specifies the password to enable or disable for RIP authentication.
-------------	---

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Example

This example shows how to set the RIP authentication key chain to “**password**” on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip rip authentication-key password
```

## ip rip message-digest-key

Use this command to enable or disable a RIP MD5 authentication key (password) for use on an interface. The **no** form of this command prevents RIP from using authentication.

### Syntax

```
ip rip message-digest-key keyid md5 key
no ip rip message-digest-key keyid
```

## Parameters

<i>keyid</i>	Specifies the key ID to enable or disable for RIP authentication. Valid values are <b>1</b> to <b>255</b> .
<b>md5</b>	Specifies use of the MD5 algorithm.
<i>key</i>	Specifies the RIP authentication password.

## Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Defaults

None.

## Examples

This example shows how to set the MD5 authentication ID to 5 for the RIP authentication key set on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip rip message-digest-key 5 md5 password
```

# Configuring IRDP

## Purpose

To enable and configure the ICMP Router Discovery Protocol (IRDP) on an interface. This protocol enables a host to determine the address of a router it can use as a default gateway. It is disabled by default.

## Commands

For information about...	Refer to page...
<code>ip irdp enable</code>	<a href="#">20-11</a>
<code>ip irdp maxadvertinterval</code>	<a href="#">20-12</a>
<code>ip irdp minadvertinterval</code>	<a href="#">20-12</a>
<code>ip irdp holdtime</code>	<a href="#">20-13</a>
<code>ip irdp preference</code>	<a href="#">20-13</a>
<code>ip irdp broadcast</code>	<a href="#">20-14</a>
<code>show ip irdp</code>	<a href="#">20-14</a>

## ip irdp enable

Use this command to enable IRDP on an interface. The **no** form of this command disables IRDP on an interface.

### Syntax

```
ip irdp enable
no ip irdp enable
```

### Parameters

None.

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Example

This example shows how to enable IRDP on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip irdp enable
```

## ip irdp maxadvertinterval

Use this command to set the maximum interval in seconds between IRDP advertisements. The **no** form of this command resets the maximum advertisement interval to the default value of **600** seconds.

### Syntax

```
ip irdp maxadvertinterval interval
no irdp maxadvertinterval
```

### Parameters

---

<i>interval</i>	Specifies a maximum advertisement interval in seconds. Valid values are <b>4</b> to <b>1800</b> .
-----------------	---

---

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Example

This example shows how to set the maximum IRDP advertisement interval to 1000 seconds on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip irdp maxadvertinterval 1000
```

## ip irdp minadvertinterval

Use this command to set the minimum interval in seconds between IRDP advertisements. The **no** form of this command deletes the custom holdtime setting, and resets the minimum advertisement interval to the default value of three-fourths of the **maxadvertinterval** value, which is equal to 450 seconds.

### Syntax

```
ip irdp minadvertinterval interval
no irdp minadvertinterval
```

### Parameters

---

<i>interval</i>	Specifies a minimum advertisement interval in seconds. Valid values are <b>3</b> to <b>1800</b> .
-----------------	---

---

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Example

This example shows how to set the minimum IRDP advertisement interval to 500 seconds on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip irdp minadvertinterval 500
```

## ip irdp holdtime

Use this command to set the length of time in seconds IRDP advertisements are held valid. The **no** form of this command resets the hold time to the default value of three times the **maxadvertinterval** value, which is equal to 1800 seconds.

### Syntax

```
ip irdp holdtime holdtime
no irdp holdtime
```

### Parameters

<i>holdtime</i>	Specifies the hold time in seconds. Valid values are 0 to 9000.
-----------------	---

### Defaults

None.

### Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

### Example

This example shows how to set the IRDP hold time to 4000 seconds on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip irdp holdtime 4000
```

## ip irdp preference

Use this command to set the IRDP preference value for an interface. This value is used by IRDP to determine the interface's selection as a default gateway address. The **no** form of this command resets the interface's IRDP preference value to the default of 0.

### Syntax

```
ip irdp preference preference
no irdp preference
```

### Parameters

<i>preference</i>	Specifies the value to indicate the interface's use as a default router address. Valid values are -2147483648 to 2147483647.  The minimum value indicates that the address, even though it may be advertised, is not to be used by neighboring hosts as a default router address.
-------------------	---

## Defaults

None.

## Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Example

This example shows how to set IRDP preference on the VLAN 1 interface so that the interface's address may still be advertised, but cannot be used by neighboring hosts as a default router address:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip irdp preference -2147483648
```

# ip irdp broadcast

Use this command to configure IRDP to use the limited broadcast address of 255.255.255.255. The default is multicast with address 224.0.0.1. The **no** form of this command resets IRDP to use multicast on IP address 224.0.0.1.

## Syntax

```
ip irdp broadcast
no ip irdp broadcast
```

## Parameters

None.

## Defaults

None.

## Mode

Interface configuration: B5(su)->router(Config-if(Vlan 1))#

## Example

This example shows how to enable broadcast for IRDP on the VLAN 1 interface:

```
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip irdp broadcast
```

# show ip irdp

Use this command to display IRDP information.

## Syntax

```
show ip irdp [vlan vlan-id]
```



---

## Parameters

---

<b>vlan</b> <i>vlan-id</i>	(Optional) Displays IRDP information for a specific VLAN. This VLAN must be configured for IP routing as described in <a href="#">“Pre-Routing Configuration Tasks”</a> on page 18-1.
----------------------------	---

---

## Defaults

If **vlan** *vlan-id* is not specified, IRDP information for all interfaces will be displayed.

## Mode

Global configuration: B5(su)->router(Config)#

Exec mode: B5(su)->router#

## Example

This example shows how to display IRDP information for the VLAN 1 interface:

```
B5(su)->router#show ip irdp vlan 1
Interface vlan 1 has router discovery enabled
Advertisements will occur between 450 and 600 seconds
Advertisements are sent with broadcasts
Advertisements are valid for 1800 seconds
Default preference will be 0
```

show ip irdp

---

## IPv6 Management

This chapter describes the switch mode set of commands used to manage IPv6.

### Purpose

To enable or disable the IPv6 management function, to configure and display the IPv6 host address and IPv6 gateway for the switch, and to display IPv6 status information.

### Commands

For information about...	Refer to page...
show ipv6 status	<a href="#">21-1</a>
set ipv6	<a href="#">21-2</a>
set ipv6 address	<a href="#">21-3</a>
show ipv6 address	<a href="#">21-4</a>
clear ipv6 address	<a href="#">21-4</a>
set ipv6 gateway	<a href="#">21-5</a>
clear ipv6 gateway	<a href="#">21-6</a>
show ipv6 neighbors	<a href="#">21-7</a>
show ipv6 netstat	<a href="#">21-7</a>
ping ipv6	<a href="#">21-8</a>
traceroute ipv6	<a href="#">21-9</a>

### show ipv6 status

Use this command to display the status of the IPv6 management function.

#### Syntax

```
show ipv6 status
```

#### Parameters

None.

## Defaults

None.

## Mode

Switch mode, read-only.

## Example

This example shows how to display IPv6 management function status.

```
B5(ro)->show ipv6 status
IPv6 Administrative Mode: Disabled
```

# set ipv6

Use this command to globally enable or disable the IPv6 management function.

## Syntax

```
set ipv6 {enable | disable}
```

## Parameters

---

<b>enable   disable</b>	Enable or disable the IPv6 management function.
-------------------------	---

---

## Defaults

By default, IPv6 management is disabled.

## Mode

Switch mode, read-write.

## Usage

When you enable IPv6 management on the switch, the system automatically generates a link-local host address for the switch from the host MAC address. You can set a different host IPv6 address with the **set ipv6 address** command.

## Example

This example shows how to enable IPv6 management.

```
B5(su)-> set ipv6 enable
```

```
B5(su)->show ipv6 status
IPv6 Administrative Mode: Enabled
```

```
B5(su)->show ipv6 address
Name                IPv6 Address
-----
host                 FE80::201:F4FF:FE5C:2880/64
```

## set ipv6 address

Use this command to configure IPv6 global addressing information.

### Syntax

```
set ipv6 address ipv6-addr/prefix-length [eui64]
```

### Parameters

<i>ipv6-addr</i>	The IPv6 address or prefix to be configured. This parameter must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
<i>prefix-length</i>	The length of the IPv6 prefix for this address. The value of <i>prefix-length</i> is a decimal number indicating the number of high-order contiguous bits of the address that comprise the network portion of the address.
<b>eui64</b>	(Optional) Formulate the IPv6 address using an EUI-64 ID in the lower order 64 bits of the address.

### Defaults

No global unicast IPv6 address is defined by default.

### Mode

Switch mode, read-write.

### Usage

Use this command to manually configure a global unicast IPv6 address for IPv6 management. You can specify the address completely, or you can use the optional **eui64** parameter to allow the switch to generate the lower order 64 bits of the address.

When using the **eui64** parameter, you specify only the network prefix and length.

### Examples

This example shows how to completely specify an IPv6 address by entering all 128 bits and the prefix:

```
B5(su)->set ipv6 address 2001:0db8:1234:5555::9876:2/64
```

```
B5(su)->show ipv6 address
```

```
Name          IPv6 Address
-----
host          FE80::201:F4FF:FE5C:2880/64
host          2001:DB8:1234:5555::9876:2/64
```

This example shows how to use the **eui64** parameter to configure the lower order 64 bits:

```
B5(su)->set ipv6 address 2001:0db8:1234:5555::/64 eui64
```

```
B5(su)->show ipv6 address
```

```
Name          IPv6 Address
-----
host          FE80::201:F4FF:FE5C:2880/64
host          2001:DB8:1234:5555:201:F4FF:FE5C:2880/64
```

## show ipv6 address

Use this command to display the system IPv6 address(es) and IPv6 gateway address (default router), if configured.

### Syntax

```
show ipv6 address
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Usage

This command displays the IPv6 addresses configured automatically and with the **set ipv6 address** and **set ipv6 gateway** commands.

### Example

This example displays two IPv6 management (host) addresses configured for the switch. The first listed is the link local address that was automatically created when IPv6 was enabled for the host. The second address is a global address that was manually configured. The gateway address was also automatically created for the link local address.

```
B5(su)->show ipv6 address
Name                IPv6 Address
-----
host                FE80::201:F4FF:FE5C:2880/64
host                2001:DB8:1234:5555:201:F4FF:FE5C:2880/64
gateway            FE80::201:F4FF:FE5D:1234
```

## clear ipv6 address

Use this command to clear IPv6 global addresses.

### Syntax

```
clear ipv6 [address {all | ipv6-addr/prefix-length}]
```

### Parameters

<i>ipv6-addr</i>	The IPv6 address to be cleared. This parameter must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
<i>prefix-length</i>	The length of the IPv6 prefix for this address. The value of <i>prefix-length</i> is a decimal number indicating the number of high-order contiguous bits of the address that comprise the network portion of the address.
<b>all</b>	Deletes all IPv6 global addresses.

## Defaults

If **address** is not entered, all manually configured global IPv6 addresses are cleared.

## Mode

Switch mode, read-write.

## Usage

This command clears addresses manually configured with the **set ipv6 address** command. Use the **clear ipv6 gateway** command to clear the IPv6 gateway address.

## Example

This example illustrates that this command clears only those IPv6 addresses configured with the **set ipv6 address** command. The link-local address for the host interface and the gateway address are not removed with this command.

```
B5(su)->show ipv6 address
Name                IPv6 Address
-----
host                FE80::201:F4FF:FE5C:2880/64
host                2001:DB8:1234:5555:201:F4FF:FE5C:2880/64
host                2001:DB8:1234:5555::9876:2/64
gateway             FE80::201:F4FF:FE5D:1234
```

```
B5(su)->clear ipv6 address all
```

```
B5(su)->show ipv6 address
Name                IPv6 Address
-----
host                FE80::201:F4FF:FE5C:2880/64
gateway             FE80::201:F4FF:FE5D:1234
```

# set ipv6 gateway

Use this command to configure the IPv6 gateway (default router) address.

## Syntax

```
set ipv6 gateway ipv6-addr
```

## Parameters

<i>ipv6-addr</i>	The IPv6 address to be configured. The address can be a global unicast or link-local IPv6 address, in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
------------------	--

## Defaults

None.

## Mode

Switch mode, read-write.

## Usage

This command configures the IPv6 gateway address. Only one IPv6 gateway address can be configured for the switch, so executing this command when a gateway address has already been configured will overwrite the previously configured address.

Use the **show ipv6 address** command to display a configured IPv6 gateway address.

## Example

This example shows how to configure an IPv6 gateway address using a link-local address.

```
B5(su)->set ipv6 gateway fe80::201:f4ff:fe5d:1234
B5(su)->show ipv6 address
Name                IPv6 Address
-----
host                FE80::201:F4FF:FE5C:2880/64
gateway            FE80::201:F4FF:FE5D:1234
```

## clear ipv6 gateway

Use this command to clear an IPv6 gateway address.

## Syntax

```
clear ipv6 gateway
```

## Parameters

None.

## Defaults

None.

## Mode

Switch mode, read-write.

## Example

This example shows how to remove a configured IPv6 gateway address.

```
B5(su)->show ipv6 address
Name                IPv6 Address
-----
host                FE80::201:F4FF:FE5C:2880/64
gateway            FE80::201:F4FF:FE5D:1234

B5(su)->clear ipv6 gateway

B5(su)->show ipv6 address
Name                IPv6 Address
-----
host                FE80::201:F4FF:FE5C:2880/64
```



## show ipv6 neighbors

Use this command to display the system IPv6 Neighbor Discovery Protocol cache.

### Syntax

```
show ipv6 neighbors
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows example output of this command.

```
B5(su)->show ipv6 neighbors
```

IPv6 Address	MAC Address	isRtr	State	Last Updated
2001:db8:1234:6666::2310:3	00:04:76:73:42:31	True	Reachable	00:01:16

## show ipv6 netstat

Use this command to display IPv6 netstat information.

### Syntax

```
show ipv6 netstat
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows the output of this command.

```
B5(su)->show ipv6 netstat
```

Prot	Local Address	Foreign Address	State
TCP	3333::211:88FF:FE59:4424.22	2020::D480:1384:F58C:B114.1049	ESTABLISHED
TCP	3333::211:88FF:FE59:4424.443		TIME_WAIT

```
2020::D480:1384:F58C:B114.1056
TCP  ::.23          LISTEN
    ::.*
TCP  3333::211:88FF:FE59:4424.22    ESTABLISHED
    2020::D480:1384:F58C:B114.1050
TCP  3333::211:88FF:FE59:4424.22    ESTABLISHED
    3333::2117:F1C0:90B:910D.1045
TCP  ::.80          LISTEN
    ::.*
TCP  ::.22          LISTEN
    ::.*

TCP  3333::211:88FF:FE59:4424.80    ESTABLISHED
    2020::D480:1384:F58C:B114.1053
TCP  3333::211:88FF:FE59:4424.80    ESTABLISHED
    2020::D480:1384:F58C:B114.1054
TCP  ::.443        LISTEN
    ::.*
TCP  3333::211:88FF:FE59:4424.22    ESTABLISHED
    2020::D480:1384:F58C:B114.1048
TCP  3333::211:88FF:FE59:4424.443    TIME_WAIT
    2020::D480:1384:F58C:B114.1055
```

## ping ipv6

Use this command to test routing network connectivity by sending IP ping requests.

### Syntax

```
ping ipv6-addr [size num]
```

### Parameters

<i>ipv6-addr</i>	Specifies the IPv6 address of the system to ping. Enter the address in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
<i>size num</i>	(Optional) Specifies the size of the datagram packet. The value of <i>num</i> can range from 48 to 2048 bytes.

### Defaults

None.

### Mode

Switch mode, read-write.

### Usage

This command is also available in router mode.

### Examples

This example shows output from a successful ping to IPv6 address 2001:0db8:1234:5555::1234:1.

```
B5(su)->ping ipv6 2001:0db8:1234:5555::1234:1
2001:DB8:1234:5555::1234:1 is alive
```

This example shows output from an unsuccessful ping to IPv6 address 2001:0db8:1234:5555::1234:1.

```
B5(su)->ping ipv6 2001:0db8:1234:5555::1234:1
no answer from 2001:DB8:1234:5555::1234:1
```

## tracertoute ipv6

Use this command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.

### Syntax

```
tracertoute ipv6 ipv6-addr
```

### Parameters

<i>ipv6-addr</i>	Specifies a host to which the route of an IPv6 packet will be traced. Enter the address in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
------------------	---

### Defaults

None.

### Mode

Switch mode, read-write.

### Usage

This command is also available in router mode.

### Example

This example shows how to use tracertoute to display a round trip path to host 2001:0db8:1234:5555

```
B5(su)->router#tracertoute ipv6 2001:0db8:1234:5555::1
Tracertoute to 2001:0db8:1234:5555, 30 hops max, 40 byte packets
 1 2001:0db8:1234:5555          1.000000e+00 ms  1.000000e+00 ms  1.000000e+00 ms
```



## Authentication and Authorization Configuration

This chapter describes the following authentication and authorization commands and how to use them. For information about using the TACACS+ authentication method for management, see [Chapter 23, TACACS+ Configuration](#).

For information about...	Refer to page...
<a href="#">Overview of Authentication and Authorization Methods</a>	22-1
<a href="#">Setting the Authentication Login Method</a>	22-4
<a href="#">Configuring RADIUS</a>	22-6
<a href="#">Configuring 802.1X Authentication</a>	22-15
<a href="#">Configuring MAC Authentication</a>	22-25
<a href="#">Configuring Multiple Authentication Methods</a>	22-37
<a href="#">Configuring User + IP Phone Authentication</a>	22-48
<a href="#">Configuring VLAN Authorization (RFC 3580)</a>	22-49
<a href="#">Configuring Policy Mappable Response</a>	22-52
<a href="#">Configuring MAC Locking</a>	22-57
<a href="#">Configuring Port Web Authentication (PWA)</a>	22-68
<a href="#">Configuring Secure Shell (SSH)</a>	22-80
<a href="#">Configuring Access Lists</a>	22-82



**Note:** An Enterasys Networks Feature Guide document containing an in-depth discussion of authentication and authorization configuration is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads/>

### Overview of Authentication and Authorization Methods

The following methods are available for controlling which users are allowed to access, monitor, and manage the switch.

- Login user accounts and passwords – used to log in to the CLI via a Telnet connection or local COM port connection. For details, refer to “[Setting User Accounts and Passwords](#)” on page 3-2.
- Host Access Control Authentication (HACA) – authenticates user access of Telnet management, console local management and WebView via a central RADIUS Client/Server or

TACACS+ application. When RADIUS or TACACS+ is enabled, this essentially overrides login user accounts. When HACA is active per a valid RADIUS or TACACS+ configuration, the user names and passwords used to access the switch via Telnet, SSH, WebView, and COM ports will be validated against the configured RADIUS server. Only in the case of a RADIUS timeout will those credentials be compared against credentials locally configured on the switch. For details, refer to [“Configuring RADIUS”](#) on page 22-6.

- SNMP user or community names – allows access to the Enterasys B5 switch via a network SNMP management application. To access the switch, you must enter an SNMP user or community name string. The level of management access is dependent on the associated access policy. For details, refer to [Chapter 8](#).
- 802.1X Port Based Network Access Control using EAPOL (Extensible Authentication Protocol) – provides a mechanism via a RADIUS server for administrators to securely authenticate and grant appropriate access to end user devices communicating with Enterasys B5 ports. For details on using CLI commands to configure 802.1X, refer to [“Configuring 802.1X Authentication”](#) on page 22-15.



**Note:** To configure EAP pass-through, which allows client authentication packets to be forwarded through the switch to an upstream device, 802.1X authentication must be globally disabled with the **set dot1x** command.

- MAC Authentication – provides a mechanism for administrators to securely authenticate source MAC addresses and grant appropriate access to end user devices communicating with Enterasys B5 ports. For details, refer to [“Configuring MAC Authentication”](#) on page 22-25.
- Multiple Authentication Methods – allows users to authenticate using multiple methods of authentication on the same port. For details, refer to [“Configuring Multiple Authentication Methods”](#) on page 22-37.
- Multi-User Authentication – allows multiple users and devices on the same port to authenticate using any supported authentication method. Each user or device can be mapped to the same or different roles using Enterasys policy for access control, VLAN authorization, traffic rate limiting, and quality of service. This is the most flexible and preferred method to use for VoIP (PC daisy chained to a phone). For details, refer to [“About Multi-User Authentication”](#) on page 22-37. Refer to [Appendix A, Policy and Authentication Capacities](#), for a listing of the number of users per port supported by the Enterasys B5.
- User + IP Phone (Legacy feature) – The User + IP Phone authentication feature provides legacy support for authentication and authorization of two devices, specifically a PC cascaded with a VLAN-tagging IP phone, on a single port on the `switch`. The IP phone must authenticate using MAC or 802.1X authentication, but the user may authenticate by any method. This feature allows both the user’s PC and IP phone to simultaneously authenticate on a single port and each receive a unique level of network access. For details, refer to [“Configuring User + IP Phone Authentication”](#) on page 22-48.



**Note:** User + IP Phone authentication is a legacy feature that should only be used if you have already implemented User + IP Phone in your network with switches that do not support true multi-user authentication.

- RFC 3580 tunnel attributes provide a mechanism to contain an 802.1X, MAC, or PWA authenticated user to a VLAN regardless of the PVID. This feature dynamically assigns a VLAN based on the RFC 3580 tunnel attributes returned in the RADIUS accept message. Refer to [“Configuring VLAN Authorization \(RFC 3580\)”](#) on page 22-49.
- Configuring Policy Mappable Response – allows you to define how the system should handle allowing an authenticated user onto a port based on the contents of the RADIUS server Access-Accept reply. There are three possible response settings: tunnel mode, policy mode, or

both tunnel and policy, also known as hybrid authentication mode. Refer to “[Configuring Policy Mappable Response](#)” on page 22-52.

- MAC Locking – locks a port to one or more MAC addresses, preventing the use of unauthorized devices and MAC spoofing on the port. For details, refer to “[Configuring MAC Locking](#)” on page 22-57.
- Port Web Authentication (PWA) – passes all login information from the end station to a RADIUS server for authentication before allowing a user to access the network. PWA is an alternative to 802.1X and MAC authentication. For details, refer to “[Configuring Port Web Authentication \(PWA\)](#)” on page 22-68.
- Secure Shell (SSH) – provides secure Telnet. For details, refer to “[Configuring Secure Shell \(SSH\)](#)” on page 22-80.
- IP Access Lists (ACLs) – permits or denies access to routing interfaces based on protocol and inbound and/or outbound IP address restrictions configured in access lists. For details, refer to “[Configuring Access Lists](#)” on page 22-82.
- TACACS+ (Terminal Access Controller Access-Control System Plus) – a security protocol developed by Cisco Systems that can be used as an alternative to the standard RADIUS security protocol (RFC 2865). TACACS+ runs over TCP and encrypts the body of each packet. Refer to [Chapter 23, TACACS+ Configuration](#), for information about the commands used to configure TACACS+.

## RADIUS Filter-ID Attribute and Dynamic Policy Profile Assignment

If you configure an authentication method that requires communication with a RADIUS server, you can use the RADIUS Filter-ID attribute to dynamically assign a policy profile and/or management level to authenticating users and/or devices.

The RADIUS Filter-ID attribute is simply a string that is formatted in the RADIUS Access-Accept packet sent back from the RADIUS server to the switch during the authentication process.

Each user can be configured in the RADIUS server database with a RADIUS Filter-ID attribute that specifies the name of the policy profile and/or management level the user should be assigned upon successful authentication. During the authentication process, when the RADIUS server returns a RADIUS Access-Accept message that includes a Filter-ID matching a policy profile name configured on the switch, the switch then dynamically applies the policy profile to the physical port the user/device is authenticating on.

### Filter-ID Attribute Formats

Enterasys Networkssupports two Filter-ID formats — “decorated” and “undecorated.” The decorated format has three forms:

- To specify the policy profile to assign to the authenticating user (network access authentication):

```
Enterasys:version=1:policy=string
```

where *string* specifies the policy profile name. Policy profile names are case-sensitive.

- To specify a management level (management access authentication):

```
Enterasys:version=1:mgmt=level
```

where *level* indicates the management level, either **ro**, **rw**, or **su**.

- To specify both management level and policy profile:

```
Enterasys:version=1:mgmt=level:policy=string
```

The undecorated format is simply a string that specifies a policy profile name. The undecorated format cannot be used for management access authentication.

Decorated Filter-IDs are processed first by the switch. If no decorated Filter-IDs are found, then undecorated Filter-IDs are processed. If multiple Filter-IDs are found that contain conflicting values, a Syslog message is generated.

## Setting the Authentication Login Method

### Purpose

To configure the authentication login method to be used for management.

### Commands

The commands used to configure the authentication login method are listed below.

For information about...	Refer to page...
<a href="#">show authentication login</a>	22-4
<a href="#">set authentication login</a>	22-5
<a href="#">clear authentication login</a>	22-5

## show authentication login

Use this command to display the current authentication login method for management.

### Syntax

```
show authentication login
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, Read-Only.

### Example

This example shows how to display the current authentication login method.

```
B5(rw)->show authentication login
```

```
Authentication Login List  Method 1      Method 2      Method 3
-----
any                       tacacs        radius        local
```



## set authentication login

Use this command to set the authentication login method.

### Syntax

```
set authentication login {any | local | radius | tacacs}
```

### Parameters

<b>any</b>	Specifies that the authentication protocol will be selected using the following precedence order: <ul style="list-style-type: none"> <li>• TACACS+</li> <li>• RADIUS</li> <li>• Local</li> </ul>
<b>local</b>	Specifies that the local network password settings will be used for authentication login.
<b>radius</b>	Specifies that RADIUS will be used for authentication login.
<b>tacacs</b>	Specifies that TACACS+ will be used for authentication login.

### Defaults

If this command is not executed, the default login method is “**any**.”

### Mode

Switch command, Read-Write.

### Example

This example shows how to set the authentication login method to use the local password settings:

```
B5(rw)->set authentication login local
```

## clear authentication login

Use this command to reset the authentication login method to the default setting of “any”.

### Syntax

```
clear authentication login
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, Read-Write.

## Example

This example shows how to reset the authentication login method.

```
B5(rw)->clear authentication login
```

# Configuring RADIUS

## Purpose

To perform the following:

- Review the RADIUS client/server configuration on the switch.
- Enable or disable the RADIUS client.
- Set local and remote login options.
- Set primary and secondary server parameters, including IP address, timeout period, authentication realm, and number of user login attempts allowed.
- Reset RADIUS server settings to default values.
- Configure a RADIUS accounting server.
- Configure the interface used for the source IP address of the RADIUS application when generating RADIUS packets.

## Commands

For information about...	Refer to page...
show radius	<a href="#">22-6</a>
set radius	<a href="#">22-8</a>
clear radius	<a href="#">22-9</a>
show radius accounting	<a href="#">22-10</a>
set radius accounting	<a href="#">22-11</a>
clear radius accounting	<a href="#">22-12</a>
show radius interface	<a href="#">22-12</a>
set radius interface	<a href="#">22-13</a>
clear radius interface	<a href="#">22-14</a>

## show radius

Use this command to display the current RADIUS client/server configuration.

### Syntax

```
show radius [status | retries | timeout | server [index | all]]
```

## Parameters

<b>status</b>	(Optional) Displays the RADIUS server's enable status.
<b>retries</b>	(Optional) Displays the number of retry attempts before the RADIUS server times out.
<b>timeout</b>	(Optional) Displays the maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin.
<b>server</b>	(Optional) Displays RADIUS server configuration information.
<i>index</i>   <b>all</b>	For use with the <b>server</b> parameter to show server configuration for all servers or a specific RADIUS server as defined by an index.

## Defaults

If no parameters are specified, all RADIUS configuration information will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display RADIUS configuration information:

```
B5(rw)->show radius
RADIUS status:      Enabled
RADIUS retries:     3
RADIUS timeout:     20 seconds
RADIUS Server      IP Address      Auth-Port  Realm-Type
-----
10                 172.16.20.10    1812      management-access
```

[Table 22-1](#) provides an explanation of the command output.

**Table 22-1 show radius Output Details**

Output Field	What It Displays...
RADIUS status	Whether RADIUS is <b>enabled</b> or <b>disabled</b> .
RADIUS retries	Number of retry attempts before the RADIUS server times out. The default value of <b>3</b> can be reset using the <b>set radius</b> command as described in " <a href="#">set radius</a> " on page 22-8.
RADIUS timeout	Maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin. The default value of <b>20</b> can be reset using the <b>set radius</b> command as described in " <a href="#">set radius</a> " on page 22-8.
RADIUS Server	RADIUS server's index number, IP address, and UDP authentication port.
Realm-Type	Realm defines who has to go through the RADIUS server for authentication. <ul style="list-style-type: none"> <li>• Management-access: This means that anyone trying to access the switch (Telnet, SSH, Local Management) has to authenticate through the RADIUS server.</li> <li>• Network-access: This means that all the users have to authenticate to a RADIUS server before they are allowed access to the network.</li> <li>• Any-access: Means that both Management-access and Network-access have been enabled.</li> </ul>

## set radius

Use this command to enable, disable, or configure RADIUS authentication.

### Syntax

```
set radius {enable | disable} | {retries number-of-retries} | {timeout timeout} |
{server index ip-address port [secret-value] [realm {management-access | any |
network-access}]} | {realm {management-access | any | network-access} {index| all}}
```

### Parameters

<b>enable   disable</b>	Enables or disables the RADIUS client.
<b>retries</b> <i>number-of-retries</i>	Specifies the number of retry attempts before the RADIUS server times out. Valid values are from <b>0</b> to <b>10</b> . Default is <b>3</b> .
<b>timeout</b> <i>timeout</i>	Specifies the maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin. Valid values are from <b>1</b> to <b>30</b> . Default is <b>20</b> seconds.
<b>server</b> <i>index ip_address port</i>	Specifies the index number, IP address and the UDP authentication port for the RADIUS server.
<i>secret-value</i>	(Optional) Specifies an encryption key to be used for authentication between the RADIUS client and server.
<b>realm</b> <b>management-access   any   network-access</b>	<p>Realm allows you to define who has to go through the RADIUS server for authentication.</p> <ul style="list-style-type: none"> <li><b>management-access</b>: This means that anyone trying to access the switch (Telnet, SSH, Local Management) has to authenticate through the RADIUS server.</li> <li><b>network-access</b>: This means that all the users have to authenticate to a RADIUS server before they are allowed access to the network.</li> <li><b>any</b>: Means that both management-access and network-access have been enabled.</li> </ul> <p><b>Note:</b> If the <b>management-access</b> or <b>any</b> access realm has been configured, the local “admin” account is disabled for access to the switch using the console, Telnet, or Local Management. Only the <b>network-access</b> realm allows access to the local “admin” account.</p>
<i>index</i>   <b>all</b>	Applies the realm setting to a specific server or to all servers.

### Defaults

If *secret-value* is not specified, none will be applied.

If **realm** is not specified, the **any** access realm will be used.

### Mode

Switch command, read-write.

### Usage

The Enterasys B5 device allows up to 10 RADIUS servers to be configured, with up to two servers active at any given time.

The RADIUS client can only be enabled on the switch once a RADIUS server is online, and its IP address(es) has been configured with the same password the RADIUS client will use.

## Examples

This example shows how to enable the RADIUS client for authenticating with RADIUS server 1 at IP address 192.168.6.203, UDP authentication port 1812, and an authentication password of "pwsecret." As previously noted, the "server secret" password entered here must match that already configured as the Read-Write (rw) password on the RADIUS server:

```
B5(su)->set radius server 1 192.168.6.203 1812 pwsecret
```

This example shows how to set the RADIUS timeout to 5 seconds:

```
B5(su)->set radius timeout 5
```

This example shows how to set RADIUS retries to 10:

```
B5(su)->set radius retries 10
```

This example shows how to force any management-access to the switch (Telnet, web, SSH) to authenticate through a RADIUS server. The **all** parameter at the end of the command means that any of the defined RADIUS servers can be used for this Authentication.

```
B5(rw)->set radius realm management-access all
```

## clear radius

Use this command to clear RADIUS server settings.

### Syntax

```
clear radius [retries] | [timeout] | [server {index | all | realm {index / all}}]
```

### Parameters

<b>retries</b>	Resets the maximum number of attempts a user can contact the RADIUS server before timing out to <b>3</b> .
<b>timeout</b>	Resets the maximum amount of time to establish contact with the RADIUS server before timing out to <b>20</b> seconds.
<b>server</b>	Deletes server settings.
<i>index</i>   <b>all</b>	For use with the <b>server</b> parameter to clear the server configuration for all servers or a specific RADIUS server as defined by an index.
<b>realm</b>	Resets the realm setting for all servers or a specific RADIUS server as defined by an index.

### Mode

Switch command, read-write.

### Defaults

None.

## Examples

This example shows how to clear all settings on all RADIUS servers:

```
B5(su)->clear radius server all
```

This example shows how to reset the RADIUS timeout to the default value of 20 seconds:

```
B5(su)->clear radius timeout
```

## show radius accounting

Use this command to display the RADIUS accounting configuration. This transmits accounting information between a network access server and a shared accounting server.

### Syntax

```
show radius accounting [server] | [counter ip-address] | [retries] | [timeout]
```

### Parameters

<b>server</b>	(Optional) Displays one or all RADIUS accounting server configurations.
<b>counter ip-address</b>	(Optional) Displays counters for a RADIUS accounting server.
<b>retries</b>	(Optional) Displays the maximum number of attempts to contact the RADIUS accounting server before timing out.
<b>timeout</b>	(Optional) Displays the maximum amount of time before timing out.

### Mode

Switch command, read-only.

### Defaults

If no parameters are specified, all RADIUS accounting configuration information will be displayed.

### Example

This example shows how to display RADIUS accounting configuration information. In this case, RADIUS accounting is not currently enabled and global default settings have not been changed. One server has been configured.

For details on enabling and configuring RADIUS accounting, refer to “[set radius accounting](#)” on page 22-11:

```
B5(ro)->show radius accounting
```

```
RADIUS accounting status:      Disabled
RADIUS Acct Server  IP Address  Acct-Port  Retries  Timeout  Status
-----
1                   172.16.2.10  1856       3        20       Disabled
```

# set radius accounting

Use this command to configure RADIUS accounting.

## Syntax

```
set radius accounting {[enable | disable] [retries retries] [timeout timeout]
[server ip_address port [server-secret]]
```

## Parameters

<b>enable   disable</b>	Enables or disables the RADIUS accounting client.
<b>retries</b> <i>retries</i>	Sets the maximum number of attempts to contact a specified RADIUS accounting server before timing out. Valid retry values are <b>0 - 10</b> .
<b>timeout</b> <i>timeout</i>	Sets the maximum amount of time (in seconds) to establish contact with a specified RADIUS accounting server before timing out. Valid timeout values are <b>1 - 30</b> .
<b>server</b> <i>ip_address</i> <i>port server-secret</i>	Specifies the accounting server's: <ul style="list-style-type: none"> <li>• IP address</li> <li>• UDP authentication port (<b>0 - 65535</b>)</li> <li>• <i>server-secret</i> (Read-Write password to access this accounting server. Device will prompt for this entry upon creating a server instance, as shown in the example below.)</li> </ul>

## Mode

Switch command, read-write.

## Defaults

None.

## Examples

This example shows how to enable the RADIUS accounting client for authenticating with the accounting server at IP address 10.2.4.12, UDP authentication port 1800. As previously noted, the "server secret" password entered here must match that already configured as the Read-Write (rw) password on the RADIUS accounting server:

```
B5(su)->set radius accounting server 10.2.4.12 1800
Enter secret:
Re-enter secret:
```

This example shows how to set the RADIUS accounting timeout to 30 seconds:

```
B5(su)->set radius accounting timeout 30
```

This example shows how to set RADIUS accounting retries to 10:

```
B5(su)->set radius accounting retries 10
```

## clear radius accounting

Use this command to clear RADIUS accounting configuration settings.

### Syntax

```
clear radius accounting {server ip-address | retries | timeout | counter}
```

### Parameters

<b>server</b> <i>ip-address</i>	Clears the configuration on one or more accounting servers.
<b>retries</b>	Resets the retries to the default value of 3.
<b>timeout</b>	Resets the timeout to 5 seconds.
<b>counter</b>	Clears counters.

### Mode

Switch command, read-write.

### Defaults

None.

### Example

This example shows how to reset the RADIUS accounting timeout to 5 seconds.

```
B5(su)->clear radius accounting timeout
```

## show radius interface

Use this command to display the interface used for the source IP address of the RADIUS application when generating RADIUS packets.

### Syntax

```
show radius interface
```

### Parameters

None.

### Defaults

None.

### Mode

Switch mode, read-only.

### Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the RADIUS application.

```
B5(rw)->show radius interface
loopback 1 192.168.10.1
```



## set radius interface

Use this command to specify the interface used for the source IP address of the RADIUS application when generating RADIUS packets.

### Syntax

```
set radius interface {loopback loop-ID | vlan vlan-ID}
```

### Parameters

<b>loopback</b> <i>loop-ID</i>	Specifies the loopback interface to be used. The value of <i>loop-ID</i> can range from 0 to 7.
<b>vlan</b> <i>vlan-ID</i>	Specifies the VLAN interface to be used. The value of <i>vlan-ID</i> can range from 1 to 4093.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

This command allows you to configure the source IP address used for the source IP address of the RADIUS application when generating RADIUS packets. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the RADIUS application.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface, if configured, will be used for both the source IP address and NAS-IP. If no interface is specified and no Host address is configured, the source IP address will be the address of the routed interface on which the packet egresses. If loopback 0 has been configured, the NAS-IP will be set to the IP address of loopback 0. Otherwise, the NAS-IP will be zero.

### Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the RADIUS application source IP address.

```
B5(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
B5(rw)->router(Config-if(Vlan 100))#exit
B5(rw)->router(Config)#exit
B5(rw)->router#exit
B5(rw)->router>exit
B5(rw)->set radius interface vlan 100

B5(rw)->show radius interface
vlan 100 192.168.10.1
```

## clear radius interface

Use this command to clear the interface used for the source IP address of the RADIUS application back to the default of the Host interface, if configured. If no Host address is configured, the source IP address will be the address of the routed interface on which the packet egresses.

### Syntax

```
clear radius interface
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This command returns the interface used for the source IP address of the RADIUS application back to the default of the Host interface.

```
B5(rw)->show radius interface
vlan 100 192.168.10.1
B5(rw)->clear radius interface
B5(rw)->
```

# Configuring 802.1X Authentication

## Purpose

To review and configure 802.1X authentication for one or more ports using EAPOL (Extensible Authentication Protocol). 802.1X controls network access by enforcing user authorization on selected ports, which results in allowing or denying network access according to RADIUS server configuration.



**Note:** To configure EAP pass-through, which allows client authentication packets to be forwarded through the switch to an upstream device, 802.1X authentication must be globally disabled with the **set dot1x** command (“[set dot1x](#)” on page 22-18).

## Commands

For information about...	Refer to page...
show dot1x	<a href="#">22-15</a>
show dot1x auth-config	<a href="#">22-17</a>
set dot1x	<a href="#">22-18</a>
set dot1x auth-config	<a href="#">22-19</a>
clear dot1x auth-config	<a href="#">22-20</a>
show eapol	<a href="#">22-21</a>
set eapol	<a href="#">22-23</a>
clear eapol	<a href="#">22-23</a>

## show dot1x

Use this command to display 802.1X status, diagnostics, statistics, and reauthentication or initialization control information for one or more ports.

### Syntax

```
show dot1x [auth-diag] [auth-stats] [port [init | reauth]] [port-string]
```

### Parameters

<b>auth-diag</b>	(Optional) Displays authentication diagnostics information.
<b>auth-stats</b>	(Optional) Displays authentication statistics.
<b>port init   reauth</b>	(Optional) Displays the status of port initialization and reauthentication control for the port.
<i>port-string</i>	(Optional) Displays information for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

### Defaults

If no parameters are specified, 802.1X status will be displayed.

If *port-string* is not specified, information for all ports will be displayed.

## Mode

Switch command, read-only.

## Examples

This example shows how to display 802.1X status:

```
B5(su)->show dot1x
DOT1X is disabled.
```

This example shows how to display authentication diagnostics information for ge.1.1:

```
B5(su)->show dot1x auth-diag ge.1.1

Port : 1   Auth-Diag
Enter Connecting:                0
EAP Logoffs While Connecting:   0
Enter Authenticating:           0
Success While Authenticating    0
Timeouts While Authenticating:  0
Fails While Authenticating:     0
ReAuths While Authenticating:   0
EAP Starts While Authenticating: 0
EAP logoff While Authenticating: 0
Backend Responses:              0
Backend Access Challenges:      0
Backend Others Requests To Supp: 0
Backend NonNak Responses From:  0
Backend Auth Successes:         0
Backend Auth Fails:             0
```

This example shows how to display authentication statistics for ge.1.1:

```
B5(su)->show dot1x auth-stats ge.1.1
Port: 1   Auth-Stats
EAPOL Frames Rx:                 0
EAPOL Frames Tx:                 0
EAPOL Start Frames Rx:           0
EAPOL Logoff Frames Rx:          0
EAPOL RespId Frames Rx:          0
EAPOL Resp Frames Rx:            0
EAPOL Req Frames Tx:             0
EAP Length Error Frames Rx:      0
Last EAPOL Frame Version:        0
Last EAPOL Frame Source:         00:00:00:00:00:00
```

This example shows how to display the status of port reauthentication control for ge.1.1 through ge.1.6:

```
B5(su)->show dot1x port reauth ge.1.1-6
Port 1: Port reauthenticate:     FALSE
Port 2: Port reauthenticate:     FALSE
Port 3: Port reauthenticate:     FALSE
Port 4: Port reauthenticate:     FALSE
Port 5: Port reauthenticate:     FALSE
Port 6: Port reauthenticate:     FALSE
```

## show dot1x auth-config

Use this command to display 802.1X authentication configuration settings for one or more ports.

### Syntax

```
show dot1x auth-config [authcontrolled-portcontrol] [maxreq] [quietperiod]
[reauthenabled] [reauthperiod] [servertimeout] [supptimeout] [txperiod]
[port-string]
```

### Parameters

<b>authcontrolled-portcontrol</b>	(Optional) Displays the current value of the controlled Port control parameter for the port.
<b>maxreq</b>	(Optional) Displays the value set for maximum requests currently in use by the backend authentication state machine.
<b>quietperiod</b>	(Optional) Displays the value set for quiet period currently in use by the authenticator PAE state machine.
<b>reauthenabled</b>	(Optional) Displays the state of reauthentication control used by the Reauthentication Timer state machine.
<b>reauthperiod</b>	(Optional) Displays the value, in seconds, set for the reauthentication period used by the reauthentication timer state machine.
<b>servertimeout</b>	(Optional) Displays the server timeout value, in seconds, currently in use by the backend authentication state machine.
<b>supptimeout</b>	(Optional) Displays the authentication supplicant timeout value, in seconds, currently in use by the backend authentication state machine.
<b>txperiod</b>	(Optional) Displays the transmission period value, in seconds, currently in use by the authenticator PAE state machine.
<i>port-string</i>	(Optional) Limits the display of desired information information to specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

### Defaults

If no parameters are specified, all 802.1X settings will be displayed.

If *port-string* is not specified, information for all ports will be displayed.

### Mode

Switch command, read-only.

### Examples

This example shows how to display the EAPOL port control mode for ge.1.1:

```
B5(su)->show dot1x auth-config authcontrolled-portcontrol ge.1.1
Port 1: Auth controlled port control: Auto
```

This example shows how to display the 802.1X quiet period settings for ge.1.1:

```
B5(su)->show dot1x auth-config quietperiod ge.1.1
Port 1: Quiet period: 30
```

This example shows how to display all 802.1X authentication configuration settings for ge.1.1:

```
B5(ro)->show dot1x auth-config ge.1.1
```

```
Port : 1      Auth-Config
PAE state:                    Initialize
Backend auth state:          Initialize
Admin controlled directions: Both
Oper controlled directions:  Both
Auth controlled port status: Authorized
Auth controlled port control: Auto
Quiet period:                 60
Transmission period:         30
Supplicant timeout:          30
Server timeout:               30
Maximum requests:            2
Reauthentication period:     3600
Reauthentication control:     Disabled
```

## set dot1x

Use this command to enable or disable 802.1X authentication, to reauthenticate one or more access entities, or to reinitialize one or more supplicants.

### Syntax

```
set dot1x {enable | disable | port {init / reauth} {true | false} [port-string]}
```

### Parameters

<b>enable   disable</b>	Enables or disables 802.1X.
<b>port</b>	Enable or disable 802.1X reauthentication or initialization control on one or more ports.
<b>init   reauth</b>	Configure initialization or reauthentication control.
<b>true   false</b>	Enable (true) or disable (false) reinitialization/reauthentication.
<i>port-string</i>	(Optional) Specifies the port(s) to reinitialize or reauthenticate.

### Defaults

If no ports are specified, the reinitialization or reauthentication setting will be applied to all ports.

### Mode

Switch command, read-write.

### Usage

Disabling 802.1X authentication globally, by not entering a specific *port-string* value, will enable the EAP pass-through feature. EAP pass-through allows client authentication packets to be forwarded unmodified through the switch to an upstream device.

### Examples

This example shows how to enable 802.1X:

```
B5(su)->set dot1x enable
```

This example shows how to reinitialize ge.1.2:

```
B5(rw)->set dot1x port init true ge.1.2
```

## set dot1x auth-config

Use this command to configure 802.1X authentication.

### Syntax

```
set dot1x auth-config {[authcontrolled-portcontrol {auto | forced-auth |
forced-unauth}} [maxreq value] [quietperiod value] [reauthenabled {false | true}]
[reauthperiod value] [servertimeout timeout] [supptimeout timeout] [txperiod
value]} [port-string]
```

### Parameters

<b>authcontrolled-portcontrol</b> <b>auto   forced-auth   forced-unauth</b>	Specifies the 802.1X port control mode. <ul style="list-style-type: none"> <li><b>auto</b> – Set port control mode to auto controlled port control. This is the default value.</li> <li><b>forced-auth</b> – Set port control mode to ForcedAuthorized controlled port control.</li> <li><b>forced-unauth</b> – Set port control mode to ForcedUnauthorized controlled port control.</li> </ul>
<b>maxreq</b> <i>value</i>	Specifies the maximum number of authentication requests allowed by the backend authentication state machine. Valid values are <b>1 – 10</b> . Default value is 2.
<b>quietperiod</b> <i>value</i>	Specifies the time (in seconds) following a failed authentication before another attempt can be made by the authenticator PAE state machine. Valid values are <b>0 – 65535</b> . Default value is 60 seconds.
<b>reauthenabled</b> <b>false   true</b>	Enables ( <b>true</b> ) or disables ( <b>false</b> ) reauthentication control of the reauthentication timer state machine. Default value is false.
<b>reauthperiod</b> <i>value</i>	Specifies the time lapse (in seconds) between attempts by the reauthentication timer state machine to reauthenticate a port. Valid values are <b>0 – 65535</b> . Default value is 3600 seconds.
<b>servertimeout</b> <i>timeout</i>	Specifies a timeout period (in seconds) for the authentication server, used by the backend authentication state machine. Valid values are <b>1 – 300</b> . Default value is 30 seconds.
<b>supptimeout</b> <i>timeout</i>	Specifies a timeout period (in seconds) for the authentication supplicant used by the backend authentication state machine. Valid values are <b>1 – 300</b> . Default value is 30 seconds.
<b>txperiod</b> <i>value</i>	Specifies the period (in seconds) which passes between authenticator PAE state machine EAP transmissions. Valid values are <b>0 – 65535</b> . Default value is 30 seconds.
<i>port-string</i>	(Optional) Limits the configuration of desired settings to specified port(s). For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

### Defaults

If *port-string* is not specified, authentication parameters will be set on all ports.

### Mode

Switch command, read-write.

## Examples

This example shows how to enable reauthentication control on ports ge.1.1-3:

```
B5(su)->set dot1x auth-config reauthenabled true ge.1.1-3
```

This example shows how to set the 802.1X quiet period to 120 seconds on ports ge.1.1-3:

```
B5(su)->set dot1x auth-config quietperiod 120 ge.1.1-3
```

## clear dot1x auth-config

Use this command to reset 802.1X authentication parameters to default values on one or more ports.

### Syntax

```
clear dot1x auth-config [authcontrolled-portcontrol] [maxreq] [quietperiod]
[reauthenabled] [reauthperiod] [servertimeout] [supptimeout] [txperiod] [port-
string]
```

### Parameters

<b>authcontrolled-portcontrol</b>	(Optional) Resets the 802.1X port control mode to <b>auto</b> .
<b>maxreq</b>	(Optional) Resets the maximum requests value to <b>2</b> .
<b>quietperiod</b>	(Optional) Resets the quiet period value to <b>60</b> seconds.
<b>reauthenabled</b>	(Optional) Resets the reauthentication control state to disabled ( <b>false</b> ).
<b>reauthperiod</b>	(Optional) Resets the reauthentication period value to <b>3600</b> seconds.
<b>servertimeout</b>	(Optional) Resets the server timeout value to <b>30</b> seconds.
<b>supptimeout</b>	(Optional) Resets the authentication supplicant timeout value to <b>30</b> seconds.
<b>txperiod</b>	(Optional) Resets the transmission period value to <b>30</b> seconds.
<i>port-string</i>	(Optional) Resets settings on specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

### Defaults

If no parameters are specified, all authentication parameters will be reset.

If *port-string* is not specified, parameters will be set on all ports.

### Mode

Switch command, read-write.

### Examples

This example shows how to reset the 802.1X port control mode to auto on all ports:

```
B5(su)->clear dot1x auth-config authcontrolled-portcontrol
```

This example shows how to reset reauthentication control to disabled on ports ge.1.1-3:

```
B5(su)->clear dot1x auth-config reauthenabled ge.1.1-3
```



This example shows how to reset the 802.1X quiet period to 60 seconds on ports ge.1.1-3:

```
B5(su)->clear dot1x auth-config quietperiod ge.1.1-3
```

## show eapol

Use this command to display EAPOL status or settings for one or more ports.

### Syntax

```
show eapol [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays EAPOL status for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

### Defaults

If *port-string* is not specified, only EAPOL enable status will be displayed.

### Mode

Switch command, read-only.

### Example

This example shows how to display EAPOL status for ports ge.1.1-3:

```
B5(su)->show eapol ge.1.1-3
EAPOL is disabled.
```

Port	Authentication State	Authentication Mode
-----	-----	-----
ge.1.1	Initialize	Auto
ge.1.2	Initialize	Auto
ge.1.3	Initialize	Auto

[Table 22-2](#) provides an explanation of the command output. For details on using the **set eapol** command to enable the protocol and assign an authentication mode, refer to [“set eapol”](#) on page 22-23.

**Table 22-2 show eapol Output Details**

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible <i>port-string</i> values, refer to “Port String Syntax Used in the CLI” on page 7-1.
Authentication State	<p>Current EAPOL authentication state for each port. Possible internal states for the authenticator (switch) are:</p> <ul style="list-style-type: none"> <li>• <b>initialize</b>: A port is in the initialize state when: <ul style="list-style-type: none"> <li>– authentication is disabled,</li> <li>– authentication is enabled and the port is not linked, or</li> <li>– authentication is enabled and the port is linked. (In this case very little time is spent in this state, it immediately transitions to the connecting state, via disconnected).</li> </ul> </li> <li>• <b>disconnected</b>: The port passes through this state on its way to connected whenever the port is reinitialized, via link state change, reauthentication failure, or management intervention.</li> <li>• <b>connecting</b>: While in this state, the authenticator sends request/ID messages to the end user.</li> <li>• <b>authenticating</b>: The port enters this state from connecting after receiving a response/ID from the end user. It remains in this state until the entire authentication exchange between the end user and the authentication server completes.</li> <li>• <b>authenticated</b>: The port enters this state from authenticating state after the exchange completes with a favorable result. It remains in this state until linkdown, logoff, or until a reauthentication begins.</li> <li>• <b>aborting</b>: The port enters this state from authenticating when any event occurs that interrupts the login exchange.</li> <li>• <b>held</b>: After any login failure the port remains in this state for the number of seconds equal to quietPeriod (can be set using MIB).</li> <li>• <b>forceAuth</b>: Management is allowing normal, unsecured switching on this port.</li> <li>• <b>forceUnauth</b>: Management is preventing any frames from being forwarded to or from this port.</li> </ul>
Authentication Mode	<p>Mode enabling network access for each port. Modes include:</p> <ul style="list-style-type: none"> <li>• <b>Auto</b>: Frames are forwarded according to the authentication state of each port.</li> <li>• <b>Forced Authorized Mode</b>: Meant to disable authentication on a port. It is intended for ports that support ISLs and devices that cannot authenticate, such as printers and file servers. If a default policy is applied to the port via the policy profile MIB, then frames are forwarded according to the configuration set by that policy, otherwise frames are forwarded according to the current configuration for that port. Authentication using 802.1X is not possible on a port in this mode.</li> <li>• <b>Forced Unauthorized Mode</b>: All frames received on the port are discarded by a filter. Authentication using 802.1X is not possible on a port in this mode.</li> </ul>

## set eapol

Use this command to enable or disable EAPOL port-based user authentication with the RADIUS server and to set the authentication mode for one or more ports.

### Syntax

```
set eapol [enable | disable] [auth-mode {auto | forced-auth | forced-unauth}]
port-string
```

### Parameters

<b>enable   disable</b>	Enables or disables EAPOL.
<b>auth-mode</b>	Specifies the authentication mode as:
<b>auto   forced-auth   forced-unauth</b>	<ul style="list-style-type: none"> <li><b>auto</b> - Auto authorization mode. This is the default mode and will forward frames according to the authentication state of the port. For details on this mode, refer to <a href="#">Table 22-2</a>.</li> <li><b>forced-auth</b> - Forced authorized mode, which disables authentication on the port.</li> <li><b>forced-unauth</b> - Forced unauthorized mode, which filters and discards all frames received on the port.</li> </ul>
<i>port-string</i>	Specifies the port(s) on which to set EAPOL parameters. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

### Defaults

None.

### Mode

Switch command, read-write.

### Examples

This example shows how to enable EAPOL:

```
B5(su)->set eapol enable
```

This example shows how to enable EAPOL with forced authorized mode on port ge.1.1:

```
B5(su)->set eapol auth-mode forced-auth ge.1.1
```

## clear eapol

Use this command to globally clear the EAPOL authentication mode, or to clear settings for one or more ports.

### Syntax

```
clear eapol [auth-mode] [port-string]
```

## Parameters

---

<b>auth-mode</b>	(Optional) Globally clears the EAPOL authentication mode.
<i>port-string</i>	Specifies the port(s) on which to clear EAPOL parameters. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

---

## Defaults

If **auth-mode** is not specified, all EAPOL settings will be cleared.

If *port-string* is not specified, settings will be cleared for all ports.

## Mode

Switch command, read-write.

## Example

This example shows how to clear the EAPOL authentication mode for port ge.1.3:

```
B5(su)->clear eapol auth-mode ge.1.3
```

# Configuring MAC Authentication

## Purpose

To review, disable, enable and configure MAC authentication. This authentication method allows the device to authenticate source MAC addresses in an exchange with an authentication server. The authenticator (switch) selects a source MAC seen on a MAC-authentication enabled port and submits it to a backend client for authentication. The backend client uses the MAC address stored password, if required, as credentials for an authentication attempt. If accepted, a string representing an access policy and/or VLAN authorization may be returned. If present, the switch applies the associated policy rules and VLAN segmentation.

You can specify a mask to apply to MAC addresses when authenticating users through a RADIUS server (see “[set macauthentication significant-bits](#)” on page 22-35). The most common use of significant bit masks is for authentication of all MAC addresses for a specific vendor.

## Commands

For information about...	Refer to page...
show macauthentication	<a href="#">22-25</a>
show macauthentication session	<a href="#">22-27</a>
set macauthentication	<a href="#">22-28</a>
set macauthentication password	<a href="#">22-28</a>
clear macauthentication password	<a href="#">22-29</a>
set macauthentication port	<a href="#">22-29</a>
set macauthentication portinitialize	<a href="#">22-30</a>
set macauthentication portquietperiod	<a href="#">22-30</a>
clear macauthentication portquietperiod	<a href="#">22-31</a>
set macauthentication macinitialize	<a href="#">22-31</a>
set macauthentication reauthentication	<a href="#">22-32</a>
set macauthentication portreauthenticate	<a href="#">22-32</a>
set macauthentication macreauthenticate	<a href="#">22-33</a>
set macauthentication reauthperiod	<a href="#">22-33</a>
clear macauthentication reauthperiod	<a href="#">22-34</a>
set macauthentication significant-bits	<a href="#">22-35</a>
clear macauthentication significant-bits	<a href="#">22-35</a>

## show macauthentication

Use this command to display MAC authentication information for one or more ports.

### Syntax

```
show macauthentication [port-string]
```

## Parameters

<i>port-string</i>	(Optional) Displays MAC authentication information for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
--------------------	---

## Defaults

If *port-string* is not specified, MAC authentication information will be displayed for all ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display MAC authentication information for ge.2.1 through 8:

```
B5(su)->show macauthentication ge.2.1-8
MAC authentication:           - enabled
MAC user password:           - NOPASSWORD
Port username significant bits - 48
```

Port	Port State	Reauth Period	Auth Allowed	Auth Allocated	Reauthentications
ge.2.1	disabled	3600	1	1	disabled
ge.2.2	disabled	3600	1	1	disabled
ge.2.3	disabled	3600	1	1	disabled
ge.2.4	disabled	3600	1	1	disabled
ge.2.5	disabled	3600	1	1	disabled
ge.2.6	disabled	3600	1	1	disabled
ge.2.7	disabled	3600	1	1	disabled
ge.2.8	disabled	3600	1	1	disabled

[Table 22-3](#) provides an explanation of the command output.

**Table 22-3 show macauthentication Output Details**

Output Field	What It Displays...
MAC authentication	Whether MAC authentication is globally enabled or disabled. Set using the <b>set macauthentication</b> command as described in “ <a href="#">set macauthentication</a> ” on page 22-28.
MAC user password	User password associated with MAC authentication on the device. Set using the <b>set macauthentication password</b> command as described in “ <a href="#">set macauthentication password</a> ” on page 22-28.
Port username significant bits	Number of significant bits in the MAC addresses to be used starting with the left-most bit of the vendor portion of the MAC address. The significant portion of the MAC address is sent as a user-name credential when the primary attempt to authenticate the full MAC address fails. Any other failure to authenticate the full address, (i.e., authentication server timeout) causes the next attempt to start once again with a full MAC authentication. Default value of 48 can be changed with the <b>set macauthentication significant-bits</b> command.
Port	Port designation. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
Port State	Whether or not MAC authentication is enabled or disabled on this port.

**Table 22-3 show macauthentication Output Details (Continued)**

Output Field	What It Displays...
Reauth Period	Reauthentication period for this port. Default value of <b>30</b> can be changed using the <b>set macauthentication reauthperiod</b> command (page 22-33).
Auth Allowed	Number of concurrent authentications supported on this port.
Auth Allocated	Maximum number of MAC authentications permitted on this port.
Reauthentications	Whether or not reauthentication is enabled or disabled on this port. Set using the <b>set macauthentication reauthentication</b> command (page 22-32).

## show macauthentication session

Use this command to display the active MAC authenticated sessions.

### Syntax

```
show macauthentication session
```

### Parameters

None.

### Defaults

If *port-string* is not specified, MAC session information will be displayed for all MAC authentication ports.

### Mode

Switch command, read-only.

### Usage

Changing the Reauth Period with the [set macauthentication reauthperiod](#) command does not affect current sessions. New sessions display the correct period.

### Example

This example shows how to display MAC session information:

```
B5(su)->show macauthentication session
Port          MAC Address          Duration  Reauth Period  Reauthentications
-----          -
ge.1.2       00:60:97:b5:4c:07   0,00:52:31  3600           disabled
```

[Table 22-4](#) provides an explanation of the command output.

**Table 22-4 show macauthentication session Output Details**

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
MAC Address	MAC address associated with the session.
Duration	Time this session has been active.

**Table 22-4 show macauthentication session Output Details (Continued)**

Output Field	What It Displays...
Reauth Period	Reauthentication period for this port, set using the <b>set macauthentication reauthperiod</b> command described in “ <a href="#">set macauthentication reauthperiod</a> ” on page 22-33.
Reauthentications	Whether or not reauthentication is enabled or disabled on this port. Set using the <b>set macauthentication reauthentication</b> command described in “ <a href="#">set macauthentication reauthentication</a> ” on page 22-32.

## set macauthentication

Use this command to globally enable or disable MAC authentication.

### Syntax

```
set macauthentication {enable | disable}
```

### Parameters

---

<b>enable   disable</b>	Globally enables or disables MAC authentication.
-------------------------	--

---

### Mode

Switch command, read-write.

### Defaults

None.

### Example

This example shows how to globally enable MAC authentication:

```
B5(su)->set macauthentication enable
```

## set macauthentication password

Use this command to set a MAC authentication password.

### Syntax

```
set macauthentication password password
```

### Parameters

---

<i>password</i>	Specifies a text string MAC authentication password.
-----------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.



## Example

This example shows how to set the MAC authentication password to “macauth”:

```
B5(su)->set macauthentication password macauth
```

## clear macauthentication password

Use this command to clear the MAC authentication password.

### Syntax

```
clear macauthentication password
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the MAC authentication password:

```
B5(su)->clear macauthentication password
```

## set macauthentication port

Use this command to enable or disable one or more ports for MAC authentication.

### Syntax

```
set macauthentication port {enable | disable} port-string
```

### Parameters

<b>enable   disable</b>	Enables or disables MAC authentication.
<i>port-string</i>	Specifies port(s) on which to enable or disable MAC authentication. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

### Defaults

None.

### Mode

Switch command, read-write.

## Usage

Enabling port(s) for MAC authentication requires globally enabling MAC authentication on the switch as described in “[set macauthentication](#)” on page 22-28, and then enabling it on a port-by-port basis. By default, MAC authentication is globally disabled and disabled on all ports.

## Example

This example shows how to enable MAC authentication on ge.2.1 through 5:

```
B5(su)->set macauthentication port enable ge.2.1-5
```

## set macauthentication portinitialize

Use this command to force one or more MAC authentication ports to re-initialize and remove any currently active sessions on those ports.

### Syntax

```
set macauthentication portinitialize port-string
```

### Parameters

<i>port-string</i>	Specifies the MAC authentication port(s) to re-initialize. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
--------------------	---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to force ge.2.1 through 5 to initialize:

```
B5(su)->set macauthentication portinitialize ge.2.1-5
```

## set macauthentication portquietperiod

This sets the number of seconds following a failed authentication before another attempt may be made on the port.

### Syntax

```
set macauthentication portquietperiod time port-string
```

### Parameters

<i>time</i>	Period in seconds to wait after a failed authentication. By default, this is 30 seconds.
<i>port-string</i>	Specifies the ports for which the quit period is to be applied. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example sets port 1 to wait 5 seconds after a failed authentication attempt before a new attempt can be made:

```
B5(su)->set macauthentication portquietperiod 5 ge.1.1
```

# clear macauthentication portquietperiod

This sets the quiet period back to the default value of 30 seconds.

## Syntax

```
clear macauthentication portquietperiod [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Specifies the ports for which the quiet period is to be reset. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
--------------------	--

---

## Defaults

If a *port-string* is not specified then all ports will be set to the default port quiet period.

## Mode

Switch command, read-write.

## Example

This example resets the default quiet period on port 1:

```
B5(su)->clear macauthentication portquietperiod ge.1.1
```

# set macauthentication macinitialize

Use this command to force a current MAC authentication session to re-initialize and remove the session.

## Syntax

```
set macauthentication macinitialize mac-addr
```

## Parameters

---

<i>mac-addr</i>	Specifies the MAC address of the session to re-initialize.
-----------------	--

---

## Mode

Switch command, read-write.

## Defaults

None.

## Example

This example shows how to force the MAC authentication session for address 00-60-97-b5-4c-07 to re-initialize:

```
B5(su)->set macauthentication macinitialize 00-60-97-b5-4c-07
```

# set macauthentication reauthentication

Use this command to enable or disable reauthentication of all currently authenticated MAC addresses on one or more ports.

## Syntax

```
set macauthentication reauthentication {enable | disable} port-string
```

## Parameters

---

<b>enable   disable</b>	Enables or disables MAC reauthentication.
<i>port-string</i>	Specifies port(s) on which to enable or disable MAC reauthentication. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to enable MAC reauthentication on ge.4.1 through 5:

```
B5(su)->set macauthentication reauthentication enable ge.4.1-5
```

# set macauthentication portreauthenticate

Use this command to force an immediate reauthentication of the currently active sessions on one or more MAC authentication ports.

## Syntax

```
set macauthentication portreauthenticate port-string
```

## Parameters

---

<i>port-string</i>	Specifies MAC authentication port(s) to be reauthenticated. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
--------------------	--

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to force ge.2.1 though 5 to reauthenticate:

```
B5(su)->set macauthentication portreauthentication ge.2.1-5
```

# set macauthentication macreauthenticate

Use this command to force an immediate reauthentication of a MAC address.

## Syntax

```
set macauthentication macreauthenticate mac-addr
```

## Parameters

---

<i>mac-addr</i>	Specifies the MAC address of the session to reauthenticate.
-----------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to force the MAC authentication session for address 00-60-97-b5-4c-07 to reauthenticate:

```
B5(su)->set macauthentication macreauthenticate 00-60-97-b5-4c-07
```

# set macauthentication reauthperiod

Use this command to set the MAC reauthentication period (in seconds). This is the time lapse between attempts to reauthenticate any current MAC address authenticated to a port.

## Syntax

```
set macauthentication reauthperiod time port-string
```

## Parameters

---

<i>time</i>	Specifies the number of seconds between reauthentication attempts. Valid values are 1 - 4294967295.
<i>port-string</i>	Specifies the port(s) on which to set the MAC reauthentication period. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

Changing the Reauth Period with the **set macauthentication reauthperiod** command does not affect current sessions. New sessions will use the correct period.

## Example

This example shows how to set the MAC reauthentication period to 7200 seconds (2 hours) on ge.2.1 through 5:

```
B5(su)->set macauthentication reauthperiod 7200 ge.2.1-5
```

# clear macauthentication reauthperiod

Use this command to clear the MAC reauthentication period on one or more ports.

## Syntax

```
clear macauthentication reauthperiod [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Clears the MAC reauthentication period on specific port(s). For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
--------------------	---

---

## Defaults

If *port-string* is not specified, the reauthentication period will be cleared on all ports.

## Mode

Switch command, read-write.

## Example

This example shows how to globally clear the MAC reauthentication period:

```
B5(su)->clear macauthentication reauthperiod
```

## set macauthentication significant-bits

Use this command to set the number of significant bits of the MAC address to use for authentication.

### Syntax

```
set macauthentication significant-bits number
```

### Parameters

---

<i>number</i>	Specifies the number of significant bits to be used for authentication.
---------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

This command allows you to specify a mask to apply to MAC addresses when authenticating users through a RADIUS server. The most common use of significant bit masks is for authentication of all MAC addresses for a specific vendor.

On switches using MAC authentication, the MAC address of a user attempting to log in is sent to the RADIUS server as the user name. If access is denied, and if a significant bit mask has been configured (other than 48) with this command, the switch will apply the mask and resend the masked address to the RADIUS server. For example, if a user with MAC address of 00-16-CF-12-34-56 is denied access, and a 32 bit mask has been configured, the switch will apply the mask and resend a MAC address of 00-16-CF-12-00-00 to the RADIUS server.

To use a significant bits mask for authentication of devices by a particular vendor, specify a 24-bit mask, to mask out everything except the vendor portion of the MAC address.

### Example

This example sets the MAC authentication significant bits mask to 24.

```
B5(su)->set macauthentication significant-bits 24
```

## clear macauthentication significant-bits

Use this command to reset the number of significant bits of the MAC address to use for authentication to the default of 48.

### Syntax

```
clear macauthentication significant-bits
```

### Parameters

None.

### Defaults

None.

## Mode

Switch command, read-write.

## Example

This example resets the MAC authentication significant bits to 48.

```
B5(su)->clear macauthentication significant-bits
```



# Configuring Multiple Authentication Methods

## About Multiple Authentication Types

When enabled, multiple authentication types allows a user to authenticate using more than one method on the same port. In order for multiple authentication to function on the device, each possible method of authentication (MAC authentication, 802.1X, PWA) must be enabled globally and configured appropriately on the desired ports with its corresponding command set described in this chapter. The precedence configured for the authentication methods determines which authentication method is actually applied to the user, device, or port.

Multiple authentication mode must be globally enabled on the device using the [set multiauth mode](#) command. Authentication precedence can be configured with the [set multiauth precedence](#) command.

## About Multi-User Authentication

Multi-user authentication refers to the ability to authenticate more than one user or device on the same port, with each user or device being provided the appropriate level of network resources based on policy.

When a single supplicant connected to an access layer port authenticates, a policy profile can be dynamically applied to all traffic on the port. When multi-user authentication is **not** implemented, and more than one supplicant is connected to a port, the firmware does not provision network resources on a per-user or per-device basis, even though different users or devices may require a different set of network resources.

In order to support provisioning network resources on a per-user basis, by applying the policy configured in the RADIUS filter-ID or RFC 3580 tunnel attributes for a given user or device, the switch must be the point of authentication for the attached devices. The RADIUS filter-ID and tunnel attributes are part of the RADIUS user account and are included in the RADIUS access-accept message response received by the switch from the authentication server.

The maximum number of multiple users supported per port depends on your platform. Refer to [Appendix A, Policy and Authentication Capacities](#) for a description of the multi-user capacities for your device. By default, the number of allowed users per port is set to 1. To configure the number of allowed users per port, use the **set multiauth port numusers** command. Use the **show multiauth port** command to display the current values of “Max users” and “Allowed users” per port.

## Commands

For information about...	Refer to page...
show multiauth	<a href="#">22-38</a>
set multiauth mode	<a href="#">22-39</a>
clear multiauth mode	<a href="#">22-39</a>
set multiauth precedence	<a href="#">22-40</a>
clear multiauth precedence	<a href="#">22-40</a>
show multiauth port	<a href="#">22-41</a>
set multiauth port	<a href="#">22-41</a>

For information about...	Refer to page...
clear multiauth port	<a href="#">22-42</a>
show multiauth station	<a href="#">22-43</a>
show multiauth session	<a href="#">22-43</a>
show multiauth idle-timeout	<a href="#">22-44</a>
set multiauth idle-timeout	<a href="#">22-45</a>
clear multiauth idle-timeout	<a href="#">22-46</a>
show multiauth session-timeout	<a href="#">22-46</a>
set multiauth session-timeout	<a href="#">22-47</a>
clear multiauth session-timeout	<a href="#">22-48</a>

## show multiauth

Use this command to display multiple authentication system configuration.

### Syntax

```
show multiauth
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display multiple authentication system configuration:

```
B5(rw)->show multiauth

Multiple authentication system configuration
-----
Supported types           : dot1x, pwa, mac
Maximum number of users  : 768
Current number of users  : 2
System mode               : multi
Default precedence       : dot1x, pwa, mac
Admin precedence         : dot1x, pwa, mac
Operational precedence   : dot1x, pwa, mac
```

## set multiauth mode

Use this command to set the system authentication mode to allow multiple authenticators simultaneously (802.1x, PWA, and MAC Authentication) on a single port, or to strictly adhere to 802.1x authentication.

### Syntax

```
set multiauth mode {multi | strict}
```

### Parameters

<b>multi</b>	Allows the system to use multiple authenticators simultaneously (802.1x, PWA, and MAC Authentication) on a port. This is the default mode.
<b>strict</b>	User must authenticate using 802.1x authentication before normal traffic (anything other than authentication traffic) can be forwarded.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

Multiauth **multi** mode requires that MAC, PWA, and 802.1X authentication be enabled globally, and configured appropriately on the desired ports according to their corresponding command sets described in this chapter. Refer to “[Configuring 802.1X Authentication](#)” on page 22-15 and “[Configuring MAC Authentication](#)” on page 22-25 and “[Configuring Port Web Authentication \(PWA\)](#)” on page 22-68.

### Example

This example shows how to enable simultaneous multiple authentications:

```
B5(rw)->set multiauth mode multi
```

## clear multiauth mode

Use this command to clear the system authentication mode.

### Syntax

```
clear multiauth mode
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

## Example

This example shows how to clear the system authentication mode:

```
B5(rw)->clear multiauth mode
```

## set multiauth precedence

Use this command to set the system's multiple authentication administrative precedence.

### Syntax

```
set multiauth precedence {[dot1x] [mac] [pwa]}
```

### Parameters

<b>dot1x</b>	Sets precedence for 802.1X authentication.
<b>mac</b>	Sets precedence for MAC authentication.
<b>pwa</b>	Sets precedence for port web authentication.

### Defaults

Default precedence order is dot1x, pwa, mac.

### Mode

Switch command, read-write.

### Usage

When a user is successfully authenticated by more than one method at the same time, the precedence of the authentication methods will determine which RADIUS-returned filter ID will be processed and result in an applied traffic policy profile.

## Example

This example shows how to set precedence for MAC authentication:

```
B5(rw)->set multiauth precedence mac dot1x
```

## clear multiauth precedence

Use this command to clear the system's multiple authentication administrative precedence to the default precedence order.

### Syntax

```
clear multiauth precedence
```

### Parameters

None.

### Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to clear the multiple authentication precedence:

```
B5(rw)->clear multiauth precedence
```

# show multiauth port

Use this command to display multiple authentication properties for one or more ports.

## Syntax

```
show multiauth port [port-string]
```

## Parameters

---

<i>port-string</i>	(Optional) Displays multiple authentication information for specific port(s).
--------------------	---

---

## Defaults

If *port-string* is not specified, multiple authentication information will be displayed for all ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display multiple authentication information for ports *ge.3.1-4*. The number of “Max users” shown by this command varies depending on the platform.

```
B5(rw)->show multiauth port ge.3.1-4
```

Port	Mode	Max users	Allowed users	Current users
ge.3.1	auth-opt	<i>n</i>	1	0
ge.3.2	auth-opt	<i>n</i>	1	0
ge.3.3	auth-opt	<i>n</i>	1	0
ge.3.4	auth-opt	<i>n</i>	1	0

# set multiauth port

Use this command to set multiple authentication properties for one or more ports.

## Syntax

```
set multiauth port mode {auth-opt | auth-reqd | force-auth | force-unauth} |  
numusers numusers port-string
```

## Parameters

<b>mode</b> <b>auth-opt</b>   <b>auth-reqd</b>   <b>force-auth</b>   <b>force-unauth</b>	Specifies the port(s)' multiple authentication mode as: <ul style="list-style-type: none"> <li>• <b>auth-opt</b> — Authentication optional (“non-strict” behavior). If a user does not attempt to authenticate using 802.1x, or if 802.1x authentication fails, the port will allow traffic to be forwarded according to the defined default VLAN.</li> <li>• <b>auth-reqd</b> — Authentication is required.</li> <li>• <b>force-auth</b> — Authentication considered.</li> <li>• <b>force-unauth</b> — Authentication disabled.</li> </ul>
<b>numusers</b> <i>numusers</i>	Specifies the number of users allowed authentication on port(s). Valid values depend on your specific platform. Refer to <a href="#">Appendix A, Policy and Authentication Capacities</a> for information about multi-user capacities.
<i>port-string</i>	Specifies the port(s) on which to set multiple authentication properties.

## Defaults

Default value for the number of users allowed to authenticate on a port is 1.

## Mode

Switch command, read-write.

## Examples

This example shows how to set the port multiple authentication mode to required on ge.3.14:

```
B5(rw)->set multiauth port mode auth-reqd ge.3.14
```

This example shows how to set the number of users allowed to authenticate on port ge.3.14 to 2:

```
B5(rw)->set multiauth port numusers 2 ge.3.14
```

# clear multiauth port

Use this command to clear multiple authentication properties for one or more ports.

## Syntax

```
clear multiauth port {mode | numusers} port-string
```

## Parameters

<b>mode</b>	Clears the specified port's multiple authentication mode.
<b>numusers</b>	Clears the value set for the number of users allowed authentication on the specified port.
<i>port-string</i>	Specifies the port or ports on which to clear multiple authentication properties.

## Defaults

None.

## Mode

Switch command, read-write.

## Examples

This example shows how to clear the port multiple authentication mode on port `ge.3.14`:

```
B5(rw)->clear multiauth port mode ge.3.14
```

This example shows how to clear the number of users on port `ge.3.14`:

```
B5(rw)->clear multiauth port numusers ge.3.14
```

## show multiauth station

Use this command to display multiple authentication station (end user) entries.

### Syntax

```
show multiauth station [mac address] [port port-string]
```

### Parameters

<b>mac</b> address	(Optional) Displays multiple authentication station entries for a specific MAC address.
<b>port</b> port-string	(Optional) Displays multiple authentication station entries for one or more ports.

### Mode

Switch command, read-only.

### Defaults

If no options are specified, multiple authentication station entries will be displayed for all MAC addresses and ports.

### Example

This example shows how to display multiple authentication station entries. In this case, two end user MAC addresses are shown:

```
B5(rw)->show multiauth station
Port          Address type  Address
-----
ge.1.20      mac          00-10-a4-9e-24-87
ge.2.16      mac          00-b0-d0-e5-0c-d0
```

## show multiauth session

Use this command to display multiple authentication session entries.

### Syntax

```
show multiauth session [all] [agent {dot1x | mac | pwa}] [mac address]
[port port-string]
```

## Parameters

<b>all</b>	(Optional) Displays information about all sessions, including those with terminated status.
<b>agent dot1x   mac   pwa</b>	(Optional) Displays 802.1X, or MAC, or port web authentication session information.
<b>mac address</b>	(Optional) Displays multiple authentication session entries for specific MAC address(es).
<b>port port-string</b>	(Optional) Displays multiple authentication session entries for the specified port or ports.

## Defaults

If no options are specified, multiple authentication session entries will be displayed for all sessions, authentication types, MAC addresses, and ports.

## Mode

Switch command, read-only.

## Example

This example shows how to display multiple authentication session information for port ge.1.1.

```
B5(su)->show multiauth session port ge.1.1
```

Port	ge.1.1	Station address	00-01-03-86-0A-87
Auth status	success	Last attempt	FRI MAY 18 11:16:36 2007
Agent type	dot1x	Session applied	true
Server type	radius	VLAN-Tunnel-Attr	none
Policy index	0	Policy name	Administrator
Session timeout	0	Session duration	0,00:00:25
Idle timeout	5	Idle time	0,00:00:00
Termination time	Not Terminated		

## show multiauth idle-timeout

Use this command to display the timeout value, in seconds, for an idle session for all authentication methods.

## Syntax

```
show multiauth idle-timeout
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.



## Example

This example shows how to display timeout values for an idle session for all authentication types.

```
B5(su)->show multiauth idle-timeout
Authentication type  Timeout (sec)
-----
dot1x                0
pwa                  0
mac                  0
```

## set multiauth idle-timeout

Use this command to set the maximum number of consecutive seconds an authenticated session may be idle before termination of the session.

### Syntax

```
set multiauth idle-timeout [dot1x | mac | pwa] timeout
```

### Parameters

<b>dot1x</b>	(Optional) Specifies the IEEE 802.1X port-based network access control authentication method for which to set the timeout value.
<b>mac</b>	(Optional) Specifies the Enterasys MAC authentication method for which to set the timeout value.
<b>pwa</b>	(Optional) Specifies the Enterasys Port Web Authentication method for which to set the timeout value.
<i>timeout</i>	Specifies the timeout value in seconds. The value can range from 0 to 65535. A value of 0 means that no idle timeout will be applied unless an idle timeout value is provided by the authenticating server.

### Defaults

If no authentication method is specified, the idle timeout value is set for all authentication methods.

### Mode

Switch mode, read-write.

### Usage

If you set an idle timeout value, a MAC user whose MAC address has aged out of the forwarding database will be unauthenticated if no traffic has been seen from that address for the specified idle timeout period.

A value of zero indicates that no idle timeout will be applied unless an idle timeout value is provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may encode a Idle-Timeout Attribute in its authentication response.

## Example

This example sets the idle timeout value for all authentication methods to 300 seconds.

```
B5(su)->set multiauth idle-timeout 300
```

## clear multiauth idle-timeout

Use this command to reset the maximum number of consecutive seconds an authenticated session may be idle before termination of the session to its default value of 0.

### Syntax

```
clear multiauth idle-timeout [dot1x | mac | pwa]
```

### Parameters

<b>dot1x</b>	(Optional) Specifies the IEEE 802.1X port-based network access control authentication method for which to reset the timeout value to its default.
<b>mac</b>	(Optional) Specifies the Enterasys MAC authentication method for which to reset the timeout value to its default.
<b>pwa</b>	(Optional) Specifies the Enterasys Port Web Authentication method for which to reset the timeout value to its default.

### Defaults

If no authentication method is specified, the idle timeout value is reset to its default value of 0 for all authentication methods.

### Mode

Switch mode, read-write.

### Example

This example resets the idle timeout value for all authentication methods to 0 seconds.

```
B5(su)->clear multiauth idle-timeout
```

## show multiauth session-timeout

Use this command to display the session timeout value, in seconds, for all authentication methods.

### Syntax

```
show multiauth session-timeout
```

### Parameters

None.

### Defaults

None.

### Mode

Switch mode, read-only.

## Example

This example displays the session timeout values for all authentication methods.

```
B5(su)->show multiauth session-timeout
Authentication type  Timeout (sec)
-----
dot1x                0
pwa                  0
mac                  0
```

## set multiauth session-timeout

Use this command to set the maximum number of seconds an authenticated session may last before termination of the session.

### Syntax

```
set multiauth session-timeout [dot1x | mac | pwa] timeout
```

### Parameters

<b>dot1x</b>	(Optional) Specifies the IEEE 802.1X port-based network access control authentication method for which to set the session timeout value.
<b>mac</b>	(Optional) Specifies the Enterasys MAC authentication method for which to set the session timeout value.
<b>pwa</b>	(Optional) Specifies the Enterasys Port Web Authentication method for which to set the session timeout value.
<i>timeout</i>	Specifies the timeout value in seconds. The value can range from 0 to 65535. A value of 0 means that no session timeout will be applied unless a session timeout value is provided by the authenticating server.

### Defaults

If no authentication method is specified, the session timeout value is set for all authentication methods.

### Mode

Switch mode, read-write.

### Usage

A value of zero may be superseded by a session timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may encode a Session-Timeout Attribute in its authentication response.

## Example

This example sets the session timeout value for the IEEE 802.1X authentication method to 300 seconds.

```
B5(su)->set multiauth session-timeout dot1x 300
```

## clear multiauth session-timeout

Use this command to reset the maximum number of consecutive seconds an authenticated session may last before termination of the session to its default value of 0.

### Syntax

```
clear multiauth session-timeout [dot1x | mac | pwa]
```

### Parameters

<b>dot1x</b>	(Optional) Specifies the IEEE 802.1X port-based network access control authentication method for which to reset the timeout value to its default.
<b>mac</b>	(Optional) Specifies the Enterasys MAC authentication method for which to reset the timeout value to its default.
<b>pwa</b>	(Optional) Specifies the Enterasys Port Web Authentication method for which to reset the timeout value to its default.

### Defaults

If no authentication method is specified, the session timeout value is reset to its default value of 0 for all authentication methods.

### Mode

Switch mode, read-write.

### Example

This example resets the session timeout value for the IEEE 802.1X authentication method to 0 seconds.

```
B5(su)->clear multiauth session-timeout dot1x
```

## Configuring User + IP Phone Authentication

User + IP phone authentication is a legacy feature that allows a user and their IP phone to both use a single port on the `switch` but to have separate policy roles. The user's PC and their IP phone are daisy-chained together with a single connection to the network.

This special application of multi-user authentication was inherited from legacy platforms (such as the B2 and C2) that could not natively support multiple users per port. The Enterasys B5 can support multiple users per port so the User + IP phone application should only be used if you are integrating Enterasys B5s into a legacy deployment.

With "User + IP Phone" authentication, the policy role for the IP phone is statically mapped using a policy admin rule which assigns any packets received with a VLAN tag set to a specific VID (for example, Voice VLAN) to an specified policy role (for example, IP Phone policy role). Therefore, it is required that the IP phone be configured to send VLAN-tagged packets tagged for the "Voice" VLAN. Refer to the **Usage** section for the command "[set policy rule](#)" on page 11-10 for additional information about configuring a policy admin rule that maps a VLAN tag to a policy role.

Note that if the IP phone authenticates to the network, the RADIUS accept message must return null values for RFC 3580 tunnel attributes and the Filter-ID.

The second policy role, for the user, can either be statically configured with the default policy role on the port or dynamically assigned through authentication to the network (using a RADIUS Filter-ID). When the default policy role is assigned on a port, the VLAN set as the port's PVID is mapped to the default policy role. When a policy role is dynamically applied to a user as the result of a successfully authenticated session, the “authenticated VLAN” is mapped to the policy role set in the Filter-ID returned from the RADIUS server. The “authenticated VLAN” may either be the PVID of the port, if the PVID Override for the policy profile is disabled, or the VLAN specified in the PVID Override if the PVID Override is enabled.

## Configuring VLAN Authorization (RFC 3580)

### Purpose

RFC 3580 Tunnel Attributes provide a mechanism to contain an 802.1X, MAC, or PWA authenticated user to a VLAN regardless of the PVID. This is referred to as dynamic VLAN assignment.

Please see section 3-31 of RFC 3580 for details on configuring a RADIUS server to return the desired tunnel attributes. As stated in RFC 3580, “... it may be desirable to allow a port to be placed into a particular Virtual LAN (VLAN), defined in [IEEE8021Q], based on the result of the authentication.”

The RADIUS server typically indicates the desired VLAN by including tunnel attributes within its Access-Accept parameters. However, the IEEE 802.1X or MAC authenticator can also be configured to instruct the VLAN to be assigned to the supplicant by including tunnel attributes within Access-Request parameters.

The following tunnel attributes are used in VLAN authorization assignment:

- Tunnel-Type - VLAN (13)
- Tunnel-Medium-Type - 802
- Tunnel-Private-Group-ID - VLANID

In order to authenticate RFC 3580 users, policy mappable response must be set to **tunnel** as described in “[Configuring Policy Mappable Response](#)” on page 22-52.



**Note:** A policy license, if applicable, is not required to deploy RFC 3580 dynamic VLAN assignment.

### Commands

For information about...	Refer to page...
set vlanauthorization	<a href="#">22-50</a>
set vlanauthorization egress	<a href="#">22-50</a>
clear vlanauthorization	<a href="#">22-51</a>
show vlanauthorization	<a href="#">22-51</a>

## set vlanauthorization

Enable or disable the use of the RADIUS VLAN tunnel attribute to put a port into a particular VLAN based on the result of authentication.

### Syntax

```
set vlanauthorization {enable | disable} [port-string]
```

### Parameters

<b>enable   disable</b>	Enables or disables vlan authorization/tunnel attributes.
<i>port-string</i>	(Optional) Specifies which ports to enable or disable the use of VLAN tunnel attributes/authorization. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

### Defaults

VLAN authentication is disabled by default.

### Mode

Switch command, read-write.

### Examples

This example shows how to enable VLAN authentication for all Gigabit Ethernet ports:

```
B5(rw)-> set vlanauthorization enable ge.*.*
```

This example shows how to disable VLAN authentication for all Gigabit Ethernet ports on switch unit/module 3:

```
B5(rw)-> set vlanauthorization disable ge.3.*
```

## set vlanauthorization egress

Controls the modification of the current VLAN egress list of 802.1x authenticated ports for the VLANs returned in the RADIUS authorization filter id string.

### Syntax

```
set vlanauthorization egress {none | tagged | untagged} port-string
```

### Parameters

<b>none</b>	Specifies that no egress manipulation will be made.
<b>tagged</b>	Specifies that the authenticating port will be added to the current tagged egress for the VLAN-ID returned.
<b>untagged</b>	Specifies that the authenticating port will be added to the current untagged egress for the VLAN-ID returned (default).
<i>port-string</i>	Specifies that the port or list of ports, to which this command will apply. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

## Defaults

By default, administrative egress is set to untagged.

## Mode

Switch command, read-write.

## Example

This example shows how to enable the insertion of the RADIUS assigned VLAN to an 802.1q tag for all outbound frames for ports 10 through 15 on unit/module number 3.

```
B5(rw)->set vlanauthorization egress tagged ge.3.10-15
```

# clear vlanauthorization

Use this command to return port(s) to the default configuration of VLAN authorization disabled, egress untagged.

## Syntax

```
clear vlanauthorization [port-string]
```

## Parameters

<i>port-string</i>	(Optional) Specifies which ports are to be restored to default configuration. If no port string is entered, the action will be a global setting. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

## Defaults

If no port string is entered, all ports will be reset to default configuration with VLAN authorization disabled and egress frames untagged.

## Mode

Switch command, read-write.

## Example

This example shows how to clear VLAN authorization for all ports on slots 3, 4, and 5:

```
B5(rw)->clear vlanauthorization ge.3-5.*
```

# show vlanauthorization

Displays the VLAN authentication status and configuration information for the specified ports.

## Syntax

```
show vlanauthorization [port-string]
```

## Parameters

<i>port-string</i>	(Optional) Displays VLAN authentication status for the specified ports. If no port string is entered, then the global status of the setting is displayed. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

## Defaults

If no port string is entered, the status for all ports will be displayed.

## Mode

Switch command, read-only.

## Example

This command shows how to display VLAN authorization status for ge.1.1:

```
B5(su)->show vlanauthorization ge.1.1
Vlan Authorization: - enabled
port      status  administrative  operational  authenticated  vlan id
           status  egress         egress      mac address
-----  -----  -----
ge.1.1   enabled  untagged
```

[Table 22-5](#) provides an explanation of command output. For details on enabling and assigning protocol and egress attributes, refer to [“set vlanauthorization”](#) on page 22-50 and [“set vlanauthorization egress”](#) on page 22-50.

**Table 22-5 show vlanauthorization Output Details**

Output Field	What It Displays...
port	Port identification
status	Port status as assigned by set vlanauthorization command
administrative egress	Port status as assigned by the set vlanauthorization egress command
operational egress	Port operational status of vlanauthorization egress.
authenticated mac address	If authentication has succeeded, displays the MAC address assigned for egress.
vlan id	If authentication has succeeded, displays the assigned VLAN id for ingress.

## Configuring Policy Mappable Response

The policy mappable response feature allows you to define how the system should handle allowing an authenticated user onto a port based on the contents of the RADIUS server Access-Accept reply. There are three possible response settings: tunnel mode, policy mode, or both tunnel and policy, also known as hybrid authentication mode.

When the mappable response is set to **tunnel mode**, the system will use the tunnel attributes in the RADIUS reply to apply a VLAN to the authenticating user and will ignore any Filter-ID attributes in the RADIUS reply. On this platform, when tunnel mode is configured, no VLAN-to-policy mapping will occur. When using VLAN authorization, the policy mappable response should be set to tunnel (see [“Configuring VLAN Authorization \(RFC 3580\)”](#) on page 22-49).



When the mappable response is set to **policy mode**, the system will use the Filter-ID attributes in the RADIUS reply to apply a policy to the authenticating user and will ignore any tunnel attributes in the RADIUS reply. On this platform, when policy mode is configured, no VLAN-to-policy mapping will occur.

When the mappable response is set to **both**, or hybrid authentication mode, both Filter-ID attributes (dynamic policy assignment) and tunnel attributes (dynamic VLAN assignment) sent in RADIUS server Access-Accept replies are used to determine how the switch should handle authenticating users. On this platform, when hybrid authentication mode is configured, VLAN-to-policy mapping can occur, as described below in [“When Policy Mappable Response is “Both”](#)” on page 22-53.

Using hybrid authentication mode eliminates the dependency on having to assign VLANs through policy roles — VLANs can be assigned by means of the tunnel attributes while policy roles can be assigned by means of the Filter-ID attributes. Alternatively, VLAN-to-policy mapping can be used to map policies to users using the VLAN specified by the tunnel attributes, without having to configure Filter-ID attributes on the RADIUS server. This separation gives administrators more flexibility in segmenting their networks beyond the platform’s hardware policy role limits.

Refer to [“RADIUS Filter-ID Attribute and Dynamic Policy Profile Assignment”](#) on page 22-3 for more information about Filter-ID attributes and [“Configuring VLAN Authorization \(RFC 3580\)”](#) on page 22-49 for more information about tunnel attributes.

## Operational Description

### When Policy Mappable Response is “Both”

Hybrid authentication mode uses both Filter-ID attributes and tunnel attributes. To enable hybrid authentication mode, use the [set policy mappable](#) command and set the **response** parameter to **both**. When configured to use both sets of attributes:

- If both the Filter-ID and tunnel attributes are present in the RADIUS reply, then the policy profile specified by the Filter-ID is applied to the authenticating user, and if VLAN authorization is enabled globally and on the authenticating user’s port, the VLAN specified by the tunnel attributes is applied to the authenticating user.

If VLAN authorization is not enabled, the VLAN specified by the policy profile is applied. See [“Configuring VLAN Authorization \(RFC 3580\)”](#) on page 22-49 for information about enabling VLAN authorization globally and on specific ports.

- If the Filter-ID attributes are present but the tunnel attributes are not present, the policy profile specified by the Filter-ID is applied, along with the VLAN specified by the policy profile.
- If the tunnel attributes are present but the Filter-ID attributes are not present or are invalid, and if VLAN authorization is enabled globally and on the authenticating user’s port, then the switch will check the VLAN-to-policy mapping table (configured with the **set policy mappable** command):
  - If an entry mapping the received VLAN ID to a valid policy profile is found, then that policy profile, along with the VLAN specified by the policy profile, will be applied to the authenticating user.
  - If no matching mapping table entry is found, the VLAN specified by the tunnel attributes will be applied to the authenticating user.
  - If the VLAN-to-policy mapping table is invalid, then the `etsysPolicyRFC3580MapInvalidMapping` MIB is incremented and the VLAN specified by the tunnel attributes will be applied to the authenticating user.

If VLAN authorization is not enabled, the tunnel attributes are ignored.

### When Policy Mactable Response is “Policy”

When the switch is configured to use only Filter-ID attributes, by setting the **set policy mactable** command **response** parameter to **policy**:

- If the Filter-ID attributes are present, the specified policy profile will be applied to the authenticating user. If no Filter-ID attributes are present, or if the policy ID is unknown or invalid, the default policy (if it exists) will be applied.
- If the tunnel attributes are present, they are ignored. No VLAN-to-policy mapping will occur.

On switches that support policy, the default mactable response mode is **policy**. On switches that do not support policy, the default mactable response mode is **tunnel**.

### When Policy Mactable Response is “Tunnel”

When the switch is configured to use only tunnel attributes, by setting the **set policy mactable** command **response** parameter to **tunnel**, and if VLAN authorization is enabled both globally and on the authenticating user’s port:

- If the tunnel attributes are present, the specified VLAN will be applied to the authenticating user. No VLAN-to-policy mapping will occur.
- If the tunnel attributes are not present, the default policy VLAN will be applied if it exists. Otherwise, the port VLAN will be applied.
- If the Filter-ID attributes are present, they are ignored.

If VLAN authorization is not enabled, the user will be allowed onto the port with the default policy, if it exists. If no default policy exists, the port VLAN will be applied.

On switches that support policy, the default mactable response mode is **policy**. On switches that do not support policy, the default mactable response mode is **tunnel**.

## Commands

For information about...	Refer to page...
show policy mactable	<a href="#">22-54</a>
set policy mactable	<a href="#">22-55</a>
clear policy mactable	<a href="#">22-56</a>

## show policy mactable

Use this command to display information about the current VLAN-to-policy mapping table and the switch’s policy mactable response setting.

### Syntax

```
show policy mactable [vlan-list]
```

### Parameters

<i>vlan-list</i>	(Optional) Specifies the VLAN or list of VLANs for which to display the VLAN-to-policy settings.
------------------	--

## Defaults

If no VLAN list is specified, all entries in the VLAN-to-policy mapping table are displayed.

## Mode

Switch command, read-only.

## Usage

This command displays both the policy mactable response setting, and the entries in the VLAN-to-policy mapping table for one or multiple VLANs. Refer to “[Operational Description](#)” on page 22-53 for information about how the VLAN-to-policy mapping table is used.

## Example

This example shows how to display the policy mactable response and all the entries in the VLAN-to-policy mapping table. In this example, hybrid authentication mode is enabled (because the policy mactable response is **both**).

```
B5(rw)->show policy mactable
Policy map response      :  both
Policy map last change  :  1 days 00:23:57
```

VLAN ID	Policy Profile
144	4 (Students)
160	7 (Faculty)

# set policy mactable

Use this command to configure the VLAN-to-policy mapping table and also the switch’s mactable response setting— that is, whether the switch is in tunnel mode, policy mode, or hybrid authentication mode.

## Syntax

```
set policy mactable {vlan-list policy-index | response {both | policy | tunnel}}
```

## Parameters

<i>vlan-list policy-index</i>	Specifies an entry in the VLAN-to-policy mapping table, which relates a policy profile with a VLAN ID or range of IDs. <i>vlan-list</i> can range from 1 to 4093. <i>policy-index</i> can range from 1 to 1023.
<b>response</b>	Indicates that this command is configuring the policy mactable response.
<b>both</b>	Sets the mactable response to look at both the Filter-ID and tunnel attributes in a RADIUS Access-Accept reply to determine how to handle an authenticating user. This is equivalent to enabling hybrid authentication mode.
<b>policy</b>	Sets the mactable response to policy mode. The system will look at only the Filter-ID attributes in a RADIUS Access-Accept reply to determine how to handle an authenticating user.
<b>tunnel</b>	Sets the mactable response to tunnel mode. The system will look at only the tunnel attributes in a RADIUS Access-Accept reply to determine how to handle an authenticating user.

## Defaults

No mapping table entries are configured.

The default policy mactable response setting is **policy** mode.

## Mode

Switch command, read-write.

## Usage

This command can be used to create entries in the VLAN-to-policy mapping table and also to set the switch's mactable response. Refer to "[Operational Description](#)" on page 22-53 for more information about the switch's operations for all mactable response parameters.

When you are using VLAN authorization for dynamic VLAN assignment, you should set the policy mactable response to **tunnel**. See "[Configuring VLAN Authorization \(RFC 3580\)](#)" on page 22-49.

## Examples

This example shows how to set the policy mactable response to both, or hybrid authentication mode:

```
B5(rw)->set policy mactable response both
```

This example shows how to configure a policy mapping entry that will map VLAN 144 to policy profile 4.

```
B5(rw)->set policy mactable 144 4
```

# clear policy mactable

Use this command to clear a VLAN-to-policy mapping table entry or to reset the mactable response to the default value of **policy** mode.

## Syntax

```
clear policy mactable {vlan-list | response}
```

## Parameters

<i>vlan-list</i>	Clears the policy profile mapping for the specified VLAN ID or range of VLANs.
<b>response</b>	Resets the mactable response to <b>policy</b> .

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command can be used to remove an entry in the VLAN-to-policy mapping table or to change the mactable response back to the default value of **policy** mode.

## Example

This example removes the entry in the mapping table for VLAN 144.

```
B5(rw)->show policy mactable
Policy map response      : both
Policy map last change  : 1 days 17:23:57

      VLAN ID      Policy Profile
      144           4             (Students)
      160           7             (Faculty)
```

```
B5(rw)->clear policy mactable 144
```

```
B5(rw)->show policy mactable
Policy map response      : both
Policy map last change  : 1 days 17:24:01

      VLAN ID      Policy Profile
      160           7             (Faculty)
```

## Configuring MAC Locking

This feature locks a MAC address to one or more ports, preventing connection of unauthorized devices through the port(s). When source MAC addresses are received on specified ports, the switch discards all subsequent frames not containing the configured source addresses. The only frames forwarded on a “locked” port are those with the “locked” MAC address(es) for that port.

There are two methods of locking a MAC to a port: first arrival and static. The first arrival method is defined to be locking the first  $n$  number of MACs which arrive on a port configured with MAC locking enabled. The value  $n$  is configured with the **set maclock firstarrival** command.

The static method is defined to be statically provisioning a MAC-port lock using the **set maclock** command. The maximum number of static MAC addresses allowed for MAC locking on a port can be configured with the **set maclock static** command.

You can configure the switch to issue a violation trap if a packet arrives with a source MAC address different from any of the currently locked MAC addresses for that port.

MACs are unlocked as a result of:

- A link down event
- When MAC locking is disabled on a port
- When a MAC is aged out of the forwarding database when FirstArrival aging is enabled

When properly configured, MAC locking is an excellent security tool as it prevents MAC spoofing on configured ports. Also if a MAC were to be secured by something like Dragon Dynamic Intrusion Detection, MAC locking would make it more difficult for a hacker to send packets into the network because the hacker would have to change their MAC address and move to another port. In the meantime the system administrator would be receiving a maclock trap notification.

## Purpose

To review, disable, enable, and configure MAC locking.

## Commands

For information about...	Refer to page...
show maclock	<a href="#">22-58</a>
show maclock stations	<a href="#">22-59</a>
set maclock enable	<a href="#">22-60</a>
set maclock disable	<a href="#">22-61</a>
set maclock	<a href="#">22-61</a>
clear maclock	<a href="#">22-62</a>
set maclock static	<a href="#">22-63</a>
clear maclock static	<a href="#">22-63</a>
set maclock firstarrival	<a href="#">22-64</a>
clear maclock firstarrival	<a href="#">22-65</a>
set maclock agefirstarrival	<a href="#">22-65</a>
clear maclock agefirstarrival	<a href="#">22-66</a>
set maclock move	<a href="#">22-66</a>
set maclock trap	<a href="#">22-67</a>

## show maclock

Use this command to display the status of MAC locking on one or more ports.

### Syntax

```
show maclock [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Displays MAC locking status for specified port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">"Port String Syntax Used in the CLI"</a> on page 7-1.
--------------------	--

### Defaults

If *port-string* is not specified, MAC locking status will be displayed for all ports.

### Mode

Switch command, read-only.

### Example

This example shows how to display MAC locking information for ge.1.1.

```
B5(su)->show maclock ge.1.1
MAC locking is globally enabled
```

```
Port      Port      Trap      Aging      Max Static  Max FirstArrival  Last Violating
Number    Status    Status    Status     Allocated    Allocated         MAC Address
```

```
-----
ge.1.1  enabled  disabled  enabled  20          1          00:a0:c9:39:5c:b4
```

Table 22-6 provides an explanation of the command output.

**Table 22-6 show maclock Output Details**

Output Field	What It Displays...
Port Number	Port designation. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.
Port Status	Whether MAC locking is <b>enabled</b> or <b>disabled</b> on the port. MAC locking is globally disabled by default. For details on enabling MAC locking on the switch and on one or more ports, refer to “ <a href="#">set maclock enable</a> ” on page 22-60 and “ <a href="#">set maclock</a> ” on page 22-61.
Trap Status	Whether MAC lock trap messaging is <b>enabled</b> or <b>disabled</b> on the port. For details on setting this status, refer to “ <a href="#">set maclock trap</a> ” on page 22-67.
Aging Status	Whether aging of FirstArrival MAC addresses is <b>enabled</b> or <b>disabled</b> on the port. Refer to “ <a href="#">set maclock agefirstarrival</a> ” on page 22-65.
Max Static Allocated	The maximum static MAC addresses allowed locked to the port. For details on setting this value, refer to “ <a href="#">set maclock static</a> ” on page 22-63.
Max FirstArrival Allocated	The maximum end station MAC addresses allowed locked to the port. For details on setting this value, refer to “ <a href="#">set maclock firstarrival</a> ” on page 22-64.
Last Violating MAC Address	Most recent MAC address(es) violating the maximum static and first arrival value(s) set for the port.

## show maclock stations

Use this command to display MAC locking information about end stations connected to the switch.

### Syntax

```
show maclock stations [firstarrival | static] [port-string]
```

### Parameters

<b>firstarrival</b>	(Optional) Displays MAC locking information about end stations first connected to MAC locked ports.
<b>static</b>	(Optional) Displays MAC locking information about static (management defined) end stations connected to MAC locked ports.
<i>port-string</i>	(Optional) Displays end station information for specified port(s). For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

### Defaults

If no parameters are specified, MAC locking information will be displayed for all end stations.

### Mode

Switch command, read-only.

## Example

This example shows how to display MAC locking information for the end stations connected to all Gigabit Ethernet ports in unit/module 2:

```
B5(su)->show maclock stations ge.2.*
Port Number  MAC Address          Status      State      Aging
-----
ge.2.1      00:a0:c9:39:5c:b4    active     first arrival  true
ge.2.7      00:a0:c9:39:1f:11    active     static        false
```

Table 22-7 provides an explanation of the command output.

**Table 22-7 show maclock stations Output Details**

Output Field	What It Displays...
Port Number	Port designation. For a detailed description of possible <i>port-string</i> values, refer to “Port String Syntax Used in the CLI” on page 7-1.
MAC address	MAC address of the end station(s) locked to the port.
Status	Whether the end stations are <b>active</b> or <b>inactive</b> .
State	Whether the end station locked to the port is a <b>first arrival</b> or <b>static</b> connection.
Aging	When true, FirstArrival MACs that have aged out of the forwarding database will be removed for the associated port lock.

## set maclock enable

Use this command to enable MAC locking globally or on one or more ports.



**Note:** MAC locking needs to be enabled globally and on appropriate ports for it to function.

### Syntax

```
set maclock enable [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Enables MAC locking on specific port(s). For a detailed description of possible <i>port-string</i> values, refer to “Port String Syntax Used in the CLI” on page 7-1.
--------------------	--

### Defaults

If *port-string* is not specified, MAC locking will be enabled globally.

### Mode

Switch command, read-write.

### Usage

When enabled and configured, MAC locking defines which MAC addresses, as well as how many MAC addresses are permitted to use specific port(s).



MAC locking is disabled by default at device startup. Configuring one or more ports for MAC locking requires globally enabling it on the device and then enabling it on the desired ports.

### Example

This example shows how to enable MAC locking on `ge.2.3`:

```
B5(su)->set maclock enable ge.2.3
```

## set maclock disable

Use this command to disable MAC locking globally or on one or more ports.

### Syntax

```
set maclock disable [port-string]
```

### Parameters

<i>port-string</i>	(Optional) Disables MAC locking on specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

### Defaults

If *port-string* is not specified, MAC locking will be disabled globally on the switch.

### Mode

Switch command, read-write.

### Example

This example shows how to disable MAC locking on `ge.2.3`:

```
B5(su)->set maclock disable ge.2.3
```

## set maclock

Use this command to create a static MAC address-to-port locking, and to enable or disable MAC locking for the specified MAC address and port.

### Syntax

```
set maclock mac-address port-string {create | enable | disable}
```

### Parameters

<i>mac-address</i>	Specifies the MAC address for which MAC locking will be created, enabled or disabled.
<i>port-string</i>	Specifies the port on which to create, enable or disable MAC locking for the specified MAC. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

<b>create</b>	Establishes a MAC locking association between the specified MAC address and port. Create automatically enables MAC locking between the specified MAC address and port.
<b>enable   disable</b>	Enables or disables MAC locking between the specified MAC address and port.

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

Configuring a port for MAC locking requires globally enabling it on the switch first using the **set maclock enable** command as described in “[set maclock enable](#)” on page 22-60.

Static MAC locking a user on multiple ports is not supported.

Statically MAC locked addresses will display in the **show mac** output (as described on page 14-22) as address type “other” and will not remove them on link down.

## Example

This example shows how to create a MAC locking association between MAC address 0e-03-ef-d8-44-55 and port ge.3.2:

```
B5(rw)->set maclock 0e-03-ef-d8-44-55 ge.3.2 create
```

# clear maclock

Use this command to remove a static MAC address to port locking entry.

## Syntax

```
clear maclock mac-address port-string
```

## Parameters

<i>mac-address</i>	Specifies the MAC address that will be removed from the list of static MACs allowed to communicate on the port.
<i>port-string</i>	Specifies the port on which to clear the MAC address. For a detailed description of possible <i>port-string</i> values, refer to “ <a href="#">Port String Syntax Used in the CLI</a> ” on page 7-1.

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The MAC address that is cleared will no longer be able to communicate on the port unless the first arrival limit has been set to a value greater than 0 and this limit has not yet been met.

For example, if user B's MAC is removed from the static MAC address list and the first arrival limit has been set to 0, then user B will not be able to communicate on the port. If user A's MAC is removed from the static MAC address list and the first arrival limit has been set to 10, but only has 7 entries, user A will become the 8th entry and allowed to communicate on the port.

## Example

This example shows how to remove a MAC from the list of static MACs allowed to communicate on port `ge.3.2`:

```
B5(rw)->clear maclock 0e-03-ef-d8-44-55 ge.3.2
```

## set maclock static

Use this command to set the maximum number of static MAC addresses allowed per port. Static MACs are administratively defined.

### Syntax

```
set maclock static port-string value
```

### Parameters

<i>port-string</i>	Specifies the port on which to set the maximum number of static MACs allowed. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<i>value</i>	Specifies the maximum number of static MAC addresses allowed per port. Valid values are 0 to 20.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the maximum number of allowable static MACs to 2 on `ge.3.1`:

```
B5(rw)->set maclock static ge.3.1 2
```

## clear maclock static

Use this command to reset the number of static MAC addresses allowed per port to the default value of 20.

### Syntax

```
clear maclock static port-string
```

## Parameters

<i>port-string</i>	Specifies the port on which to reset number of static MAC addresses allowed. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to reset the number of allowable static MACs on ge.2.3:

```
B5(rw)->clear maclock static ge.2.3
```

# set maclock firstarrival

Use this command to restrict MAC locking on a port to a maximum number of end station addresses first connected to that port.

## Syntax

```
set maclock firstarrival port-string value
```

## Parameters

<i>port-string</i>	Specifies the port on which to limit MAC locking. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<i>value</i>	Specifies the number of first arrival end station MAC addresses to be allowed connections to the port. Valid values are <b>0</b> to <b>600</b> .

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

The maclock first arrival count resets when the link goes down. This feature is beneficial if you have roaming users—the first arrival count will be reset every time a user moves to another port, but will still protect against connecting multiple devices on a single port and will protect against MAC address spoofing.



**Note:** Setting a port's first arrival limit to 0 does not deny the first MAC address learned on the port from passing traffic.

## Example

This example shows how to restrict MAC locking to 6 MAC addresses on ge.2.3:

```
B5(su)->set maclock firstarrival ge.2.3 6
```

## clear maclock firstarrival

Use this command to reset the number of first arrival MAC addresses allowed per port to the default value of 600.

### Syntax

```
clear maclock firstarrival port-string
```

### Parameters

<i>port-string</i>	Specifies the port on which to reset the first arrival value. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to reset MAC first arrivals on ge.2.3:

```
B5(su)->clear maclock firstarrival ge.2.3
```

## set maclock agefirstarrival

Use this command to enable or disable the aging of first arrival MAC addresses. When enabled, first arrival MAC addresses that are aged out of the forwarding database will be removed from the associated port MAC lock.

### Syntax

```
set maclock agefirstarrival port-string {enable | disable}
```

### Parameters

<i>port-string</i>	Specifies the port(s) on which to enable or disable first arrival aging. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>enable</b>   <b>disable</b>	Enable or disable first arrival aging. By default, first arrival aging is disabled.

### Defaults

None.

## Mode

Switch mode, read-write.

## Example

This example enables first arrival aging on port ge.1.1.

```
B5(su)-> set maclock agefirstarrival ge.1.1 enable
```

# clear maclock agefirstarrival

Use this command to reset first arrival aging on one or more ports to its default state of disabled.

## Syntax

```
clear maclock agefirstarrival port-string
```

## Parameters

---

<i>port-string</i>	Specifies the port(s) on which to disable first arrival aging. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

## Defaults

None.

## Mode

Switch mode, read-write.

## Example

This example disables first arrival aging on port ge.1.1.

```
B5(su)-> clear maclock agefirstarrival ge.1.1 enable
```

# set maclock move

Use this command to move all current first arrival MACs to static entries.

## Syntax

```
set maclock move port-string
```

## Parameters

---

<i>port-string</i>	Specifies the port on which MAC will be moved from first arrival MACs to static entries. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

If there are more first arrival MACs than the allowed maximum static MACs, then only the latest first arrival MACs will be moved to static entries. For example, if you set the maximum number of static MACs to 2 with the **set maclock static** command, and then executed the **set maclock move** command, even though there were five MACs in the first arrival table, only the two most recent MAC entries would be moved to static entries.

## Example

This example shows how to move all current first arrival MACs to static entries on ports ge.3.1-40:

```
B5(rw)->set maclock move ge.3.1-40
```

# set maclock trap

Use this command to enable or disable MAC lock trap messaging.

## Syntax

```
set maclock trap port-string {enable | disable}
```

## Parameters

<i>port-string</i>	Specifies the port on which MAC lock trap messaging will be enabled or disabled. For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
<b>enable</b>   <b>disable</b>	Enables or disables MAC lock trap messaging.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

When enabled, this feature authorizes the switch to send an SNMP trap message if an end station is connected that exceeds the maximum values configured using the **set maclock firstarrival** and **set maclock static** commands. Violating MAC addresses are dropped from the device's (or stack's) filtering database.

## Example

This example shows how to enable MAC lock trap messaging on ge.2.3:

```
B5(su)->set maclock trap ge.2.3 enable
```

# Configuring Port Web Authentication (PWA)

## About PWA

PWA provides a way of authenticating users through a Web portal before allowing general access to the network.

To log on using PWA, the user makes a request through a web browser for the PWA web page or is automatically redirected to this login page after requesting a URL in a browser.

Depending upon the authenticated state of the user, a login page or a logout page will display. When a user submits username and password, the switch then authenticates the user via a preconfigured RADIUS server. If the login is successful, then the user will be granted full network access according to the user's policy configuration on the switch.

## Purpose

To review, enable, disable, and configure Port Web Authentication (PWA).

## Commands

For information about...	Refer to page...
show pwa	<a href="#">22-69</a>
set pwa	<a href="#">22-70</a>
show pwa banner	<a href="#">22-71</a>
set pwa banner	<a href="#">22-71</a>
clear pwa banner	<a href="#">22-72</a>
set pwa displaylogo	<a href="#">22-72</a>
set pwa ipaddress	<a href="#">22-73</a>
set pwa guestname	<a href="#">22-74</a>
clear pwa guestname	<a href="#">22-74</a>
set pwa guestpassword	<a href="#">22-75</a>
set pwa gueststatus	<a href="#">22-75</a>
set pwa initialize	<a href="#">22-76</a>
set pwa quietperiod	<a href="#">22-76</a>
set pwa maxrequest	<a href="#">22-77</a>
set pwa portcontrol	<a href="#">22-77</a>
show pwa session	<a href="#">22-78</a>
set pwa enhancedmode	<a href="#">22-79</a>



## show pwa

Use this command to display port web authentication information for one or more ports.

### Syntax

```
show pwa [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Displays PWA information for specific port(s).
--------------------	---

---

### Defaults

If *port-string* is not specified, PWA information will be displayed for all ports.

### Mode

Switch command, read-only.

### Example

This example shows how to display PWA information for *ge.2.1*:

```
B5(su)->show pwa ge.2.1
PWA Status                - enabled
PWA IP Address            - 192.168.62.99
PWA Protocol              - PAP
PWA Enhanced Mode        - N/A
PWA Logo                  - enabled
PWA Guest Networking Status - disabled
PWA Guest Name            - guest
PWA Redirect Time        - N/A
```

Port	Mode	AuthStatus	QuietPeriod	MaxReq
-----	-----	-----	-----	-----
ge.2.1	disabled	disconnected	60	16

[Table 22-8](#) provides an explanation of the command output.

**Table 22-8 show pwa Output Details**

Output Field	What It Displays...
PWA Status	Whether or not port web authentication is enabled or disabled. Default state of disabled can be changed using the <b>set pwa</b> command as described in “ <a href="#">set pwa</a> ” on page 22-70.
PWA IP Address	IP address of the end station from which PWA will prevent network access until the user is authenticated. Set using the <b>set pwa ipaddress</b> command as described in “ <a href="#">set pwa ipaddress</a> ” on page 22-73.
PWA Protocol	Whether PWA protocol is CHAP or PAP. .
PWA Enhanced Mode	Whether PWA enhanced mode is enabled or disabled. Default state of disabled can be changed using the <a href="#">set pwa enhancedmode</a> command as described in “ <a href="#">set pwa enhancedmode</a> ” on page 22-79.
PWA Logo	Whether the Enterasys logo will be displayed or hidden at user login. Default state of enabled (displayed) can be changed using the <b>set pwa displaylogo</b> command as described in “ <a href="#">set pwa displaylogo</a> ” on page 22-72.

**Table 22-8 show pwa Output Details (Continued)**

Output Field	What It Displays...
PWA Guest Networking Status	Whether PWA guest user status is disabled or enabled with RADIUS or no authentication. Default state of disabled can be changed using the <b>set pwa gueststatus</b> command as described in “ <a href="#">set pwa gueststatus</a> ” on page 22-75.
PWA Guest Name	Guest user name for PWA enhanced mode networking. Default value of “guest” can be changed using the <b>set pwa guestname</b> command as described in “ <a href="#">set pwa guestname</a> ” on page 22-74.
PWA Guest Password	Guest user’s password. Default value of an empty string can be changed using the <b>set pwa guestpassword</b> command as described in “ <a href="#">set pwa guestpassword</a> ” on page 22-75.
PWA Redirect Time	Time in seconds after login success before the user is redirected to the PWA home page.
Port	PWA port designation.
Mode	Whether PWA is enabled or disabled on his port.
Auth Status	Whether or not the port state is disconnected, authenticating, authenticated, or held (authentication has failed).
Quiet Period	Amount of time a port will be in the held state after a user unsuccessfully attempts to log on to the network. Default value of 60 can be changed using the <b>set pwa quietperiod</b> command as described in “ <a href="#">set pwa quietperiod</a> ” on page 22-76.
MaxReq	Maximum number of log on attempts allowed before transitioning the port to a held state. Default value of 2 can be changed using the <b>set pwa maxrequests</b> command as described in “ <a href="#">set pwa maxrequest</a> ” on page 22-77.

## set pwa

Use this command to enable or disable port web authentication.

### Syntax

```
set pwa {enable | disable}
```

### Parameters

<b>enable   disable</b>	Enables or disables port web authentication.
-------------------------	--

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to enable port web authentication:

```
B5(su)->set pwa enable
```

## show pwa banner

Use this command to display the port web authentication login banner string.

### Syntax

```
show pwa banner
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display the PWA login banner:

```
B5(su)->show pwa banner  
Welcome to Enterasys Networks
```

## set pwa banner

Use this command to configure a string to be displayed as the PWA login banner.

### Syntax

```
set pwa banner string
```

### Parameters

---

<i>string</i>	Specifies the PWA login banner.
---------------	---------------------------------

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the PWA login banner to “Welcome to Enterasys Networks”:

```
B5(su)->set pwa banner "Welcome to Enterasys Networks"
```

## clear pwa banner

Use this command to reset the PWA login banner to a blank string.

### Syntax

```
clear pwa banner
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to reset the PWA login banner to a blank string

```
B5(su)->clear pwa banner
```

## set pwa displaylogo

Use this command to set the display options for the Enterasys Networks logo.

### Syntax

```
set pwa displaylogo {display | hide}
```

### Parameters

---

<b>display   hide</b>	Displays or hides the Enterasys Networks logo when the PWA website displays.
-----------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to hide the Enterasys Networks logo:

```
B5(su)->set pwa displaylogo hide
```

## set pwa ipaddress

Use this command to set the PWA IP address. This is the IP address of the end station from which PWA will prevent network access until the user is authenticated.

### Syntax

```
set pwa ipaddress ip-address
```

### Parameters

---

<i>ip-address</i>	Specifies a globally unique IP address. This same value must be configured into every authenticating switch in the domain.
-------------------	--

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set a PWA IP address of 1.2.3.4:

```
B5(su)->set pwa ipaddress 1.2.3.4
```

## set pwa protocol

Use this command to set the port web authentication protocol.

### Syntax

```
set pwa protocol {chap | pap}
```

### Parameters

---

<b>chap   pap</b>	Sets the PWA protocol to: <ul style="list-style-type: none"> <li>• CHAP (PPP Challenge Handshake Protocol) - encrypts the username and password between the end-station and the switch port.</li> <li>• PAP (Password Authentication Protocol- does not provide any encryption between the end-station and the switch port. This is the default.</li> </ul>
-------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set a the PWA protocol to CHAP:

```
B5(su)->set pwa protocol chap
```

## set pwa guestname

Use this command to set a guest user name for PWA networking. PWA will use this name to grant network access to guests without established login names and passwords.

### Syntax

```
set pwa guestname name
```

### Parameters

---

<i>name</i>	Specifies a guest user name.
-------------	------------------------------

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to set the PWA guest user name to “guestuser”:

```
B5(su)->set pwa guestname guestuser
```

## clear pwa guestname

Use this command to clear the PWA guest user name.

### Syntax

```
clear pwa guestname
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to clear the PWA guest user name

```
B5(su)->clear pwa guestname
```

## set pwa guestpassword

Use this command to set the guest user password for PWA networking.

### Syntax

```
set pwa guestpassword
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

PWA will use this password and the guest user name to grant network access to guests without established login names and passwords.

### Example

This example shows how to set the PWA guest user password name:

```
B5(su)->set pwa guestpassword
Guest Password: *****
Retype Guest Password: *****
```

## set pwa gueststatus

Use this command to enable or disable guest networking for port web authentication.

### Syntax

```
set pwa gueststatus {authnone | authradius | disable}
```

### Parameters

<b>authnone</b>	Enables guest networking with no authentication method.
<b>authradius</b>	Enables guest networking with RADIUS authentication. Upon successful authentication from RADIUS, PWA will apply the policy returned from RADIUS to the PWA port.
<b>disable</b>	Disables guest networking.

### Defaults

None.

### Mode

Switch command, read-write.

## Usage

PWA will use a guest password and guest user name to grant network access with default policy privileges to users without established login names and passwords.

## Example

This example shows how to enable PWA guest networking with RADIUS authentication:

```
B5(su)->set pwa guestnetworking authradius
```

## set pwa initialize

Use this command to initialize a PWA port to its default unauthenticated state.

### Syntax

```
set pwa initialize [port-string]
```

### Parameters

---

<i>port-string</i>	(Optional) Initializes specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	---

---

### Defaults

If *port-string* is not specified, all ports will be initialized.

### Mode

Switch command, read-write.

### Example

This example shows how to initialize ports ge.1.5-7:

```
B5(su)->set pwa initialize ge.1.5-7
```

## set pwa quietperiod

Use this command to set the amount of time a port will remain in the held state after a user unsuccessfully attempts to log on to the network.

### Syntax

```
set pwa quietperiod time [port-string]
```

### Parameters

---

<i>time</i>	Specifies quiet time in seconds.
<i>port-string</i>	(Optional) Sets the quiet period for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

---



## Defaults

If *port-string* is not specified, quiet period will be set for all ports.

## Mode

Switch command, read-write.

## Example

This example shows how to set the PWA quiet period to 30 seconds for ports *ge.1.5-7*:

```
B5(su)->set pwa quietperiod 30 ge.1.5-7
```

# set pwa maxrequest

Use this command to set the maximum number of log on attempts allowed before transitioning the PWA port to a held state.

## Syntax

```
set pwa maxrequests requests [port-string]
```

## Parameters

<i>maxrequests</i>	Specifies the maximum number of log on attempts.
<i>port-string</i>	(Optional) Sets the maximum requests for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to " <a href="#">Port String Syntax Used in the CLI</a> " on page 7-1.

## Defaults

If *port-string* is not specified, maximum requests will be set for all ports.

## Mode

Switch command, read-write.

## Example

This example shows how to set the PWA maximum requests to 3 for all ports:

```
B5(su)->set pwa maxrequests 3
```

# set pwa portcontrol

This command enables or disables PWA authentication on select ports.

## Syntax

```
set pwa portcontrol {enable | disable} [port-string]
```

## Parameters

<b>enable   disable</b>	Enables or disables PWA on specified ports.
<i>port-string</i>	(Optional) Sets the control mode on specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.

## Defaults

If *port-string* is not specified, PWA will enabled on all ports.

## Mode

Switch command, read-write.

## Example

This example shows how to enable PWA on ports 1-22:

```
B5(su)->set pwa portcontrol enable ge.1.1-22
```

# show pwa session

Use this command to display information about current PWA sessions.

## Syntax

```
show pwa session [port-string]
```

## Parameters

<i>port-string</i>	(Optional) Displays PWA session information for specific port(s). For a detailed description of possible <i>port-string</i> values, refer to <a href="#">“Port String Syntax Used in the CLI”</a> on page 7-1.
--------------------	--

## Defaults

If *port-string* is not specified, session information for all ports will be displayed.

## Mode

Switch command, read-only.

## Example

This example shows how to display PWA session information:

```
B5(su)->show pwa session
```

Port	MAC	IP	User	Duration	Status
ge.2.19	00-c0-4f-20-05-4b	172.50.15.121	pwachap10	0,14:46:55	active
ge.2.19	00-c0-4f-24-51-70	172.50.15.120	pwachap1	0,15:43:30	active
ge.2.19	00-00-f8-78-9c-a7	172.50.15.61	pwachap11	0,14:47:58	active

---

## set pwa enhancedmode

This command enables PWA URL redirection. The switch intercepts all HTTP packets on port 80 from the end user, and sends the end user a refresh page destined for the PWA IP Address configured.

### Syntax

```
set pwa enhancedmode {enable | disable}
```

### Parameters

---

<b>enable   disable</b>	Enables or disables PWA <b>enhancedmode</b> .
-------------------------	---

---

### Defaults

None.

### Mode

Switch command, read-write.

### Example

This example shows how to enable PWA **enhancedmode**:

```
B5(su)->set pwa enhancedmode enable
```

# Configuring Secure Shell (SSH)

## Purpose

To review, enable, disable, and configure the Secure Shell (SSH) protocol, which provides secure Telnet. The switch can support up to two concurrent SSH sessions.

## Commands

For information about...	Refer to page...
show ssh status	<a href="#">22-80</a>
set ssh	<a href="#">22-80</a>
set ssh hostkey	<a href="#">22-81</a>

## show ssh status

Use this command to display the current status of SSH on the switch.

### Syntax

```
show ssh status
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example shows how to display SSH status on the switch:

```
B5(su)->show ssh status
SSH Server status: Disabled
```

## set ssh

Use this command to enable, disable or reinitialize SSH server on the switch. By default, the SSH server is disabled. The switch can support up to two concurrent SSH sessions.

### Syntax

```
set ssh {enable | disable | reinitialize}
```

## Parameters

<b>enable   disable</b>	Enables or disables SSH, or reinitializes the SSH server.
<b>reinitialize</b>	Reinitializes the SSH server.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This example shows how to disable SSH:

```
B5(su)->set ssh disable
```

# set ssh hostkey

Use this command to reinitialize new SSH authentication keys.

## Syntax

```
set ssh hostkey reinitialize
```

## Parameters

<b>reinitialize</b>	Reinitializes the server host authentication keys.
---------------------	--

## Defaults

None

## Mode

Switch command, read-write.

## Example

This example shows how to regenerate SSH keys:

```
B5(su)->set ssh hostkey reinitialize
```

# Configuring Access Lists



**Router:** These commands can be executed when the device is in **router mode** only. For details on how to enable router configuration modes, refer to “[Enabling Router Configuration Modes](#)” on page 18-2.



**Note:** Refer to the Release Notes for your product for any limitations that may apply to access control lists.

## Purpose

To review and configure security access control lists (ACLs), which permit or deny access to routing interfaces based on protocol and IP address restrictions.

## Commands

For information about...	Refer to page...
show access-lists	<a href="#">22-82</a>
access-list (standard)	<a href="#">22-83</a>
access-list (extended)	<a href="#">22-84</a>
ip access-group	<a href="#">22-86</a>

## show access-lists

Use this command to display configured IP access lists when operating in router mode.

### Syntax

```
show access-lists [number]
```

### Parameters

<i>access-list-number</i>	(Optional) Displays access list information for a specific access list number. Valid values are between <b>1</b> and <b>199</b> .
---------------------------	---

### Defaults

If *number* is not specified, the entire table of access lists will be displayed.

### Mode

Any router mode.

### Example

This example shows how to display IP access list number 145. This is an extended access list, which permits or denies ICMP, UDP and IP frames based on restrictions configured with one of the **access-list** commands. For details on configuring standard access lists, refer to “[access-list \(standard\)](#)” on page 22-83. For details on configuring extended access lists, refer to “[access-list \(extended\)](#)” on page 22-84.

```
B5(su)->router#show access-lists 145

Extended IP access list 145
 1: permit icmp host 88.255.255.254 any
 2: permit icmp any host 11.11.16.16
 3: deny icmp any any
 4: permit tcp host 88.255.255.254 any eq 22
 5: permit udp 88.255.128.0 0.0.127.255 eq 161 any
 6: permit tcp any host 230.10.230.10 eq 1234
 7: deny tcp any any eq 23
 8: permit ip 88.255.128.0 0.0.127.255 any
 9: deny ip any 224.0.0.0 31.0.0.0
```

## access-list (standard)

Use this command to define a standard IP access list by number when operating in router mode. The **no** form of this command removes the defined access list or entry.

### Syntax

#### To create an ACL entry:

```
access-list access-list-number {deny | permit} source [source-wildcard]
```

```
no access-list access-list-number [entryno [entryno]]
```

#### To insert or replace an ACL entry:

```
access-list access-list-number insert | replace entryno {deny | permit} source [source-wildcard]
```

#### To move entries within an ACL:

```
access-list access-list-number move destination source1 [source2]
```

### Parameters

<i>access-list-number</i> [ <i>entryno</i> [ <i>entryno</i> ]]	Specifies a standard access list number. Valid values are from <b>1</b> to <b>99</b> . When using the <b>no access-list</b> command, you can delete a whole access-list, or only specific entries in the list with the optional <i>entryno</i> parameter. Specify a range of entries by entering the start and end entry numbers.
<b>deny</b>   <b>permit</b>	Denies or permits access if specified conditions are met.
<i>source</i>	Specifies the network or host from which the packet will be sent. Valid options for expressing source are: <ul style="list-style-type: none"> <li>• IP address or range of addresses (A.B.C.D)</li> <li>• <b>any</b> - Any source host</li> <li>• <b>host source</b> - IP address of a single source host</li> </ul>
<i>source-wildcard</i>	(Optional) Specifies the bits to ignore in the <i>source</i> address.

<b>insert</b>   <b>replace</b> <i>entryno</i>	(Optional) Inserts this new entry before a specified entry in an existing ACL, or replaces a specified entry with this new entry.
<b>move</b> <i>destination</i> <i>source1 source2</i>	(Optional) Moves a sequence of access list entries before another entry. <i>Destination</i> is the number of the existing entry before which this new entry will be moved. <i>Source1</i> is a single entry number or the first entry number in the range to be moved. <i>Source2</i> (optional) is the last entry number in the range to be moved. If <i>source2</i> is not specified, only the <i>source1</i> entry will be moved.

## Defaults

If **insert**, **replace** or **move** are not specified, the new entry will be appended to the access list.

If *source2* is not specified with **move**, only one entry will be moved.

## Mode

Global configuration: B5(su)->router(Config)#

## Usage

Valid access list numbers for standard ACLs are **1** to **99**. For extended ACLs, valid values are **100** to **199**.

Access lists are applied to interfaces by using the **ip access-group** command (page 22-86).

All access lists have an implicit “deny any any” statement as their last entry.

## Examples

This example shows how to create access list 1 with three entries that allow access to only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list entries will be rejected:

```
B5(su)->router(Config)#access-list 1 permit 192.5.34.0 0.0.0.255
B5(su)->router(Config)#access-list 1 permit 128.88.0.0 0.0.255.255
B5(su)->router(Config)#access-list 1 permit 36.0.0.0 0.255.255.255
```

This example moves entry 16 to the beginning of ACL 22:

```
B5(su)->router(Config)#access-list 22 move 1 16
```

# access-list (extended)

Use this command to define an extended IP access list by number when operating in router mode. The **no** form of this command removes the defined access list or entry:

## Syntax

### To create an extended ACL entry:

```
access-list access-list-number {deny | permit} protocol source [source-wildcard]
[eq port] destination [destination-wildcard] [eq port]
```

```
no access-list access-list-number [entryno [entryno]]
```

### To insert or replace an ACL entry:

```
access-list access-list-number insert | replace entryno {deny | permit} protocol
source [source-wildcard] [eq port] destination [destination-wildcard] [eq port]
```



## To move entries within an ACL:

```
access-list access-list-number move destination source1 [source2]
```

### Parameters

<i>access-list-number</i> [ <i>entryno</i> [ <i>entryno</i> ]]	Specifies an extended access list number. Valid values are from <b>100</b> to <b>199</b> . When using the <b>no access-list</b> command, you can delete a whole access-list, or only specific entries in the list with the optional <i>entryno</i> parameter. Specify a range of entries by entering the start and end entry numbers.
<b>deny</b>   <b>permit</b>	Denies or permits access if specified conditions are met.
<i>protocol</i>	Specifies an IP protocol for which to deny or permit access. Valid values and their corresponding protocols are: <ul style="list-style-type: none"> <li>• <b>ip</b> - Any Internet protocol</li> <li>• <b>udp</b> - User Datagram Protocol</li> <li>• <b>tcp</b> - Transmission Control Protocol</li> <li>• <b>icmp</b> - Internet Control Message Protocol</li> </ul>
<i>source</i>	Specifies the network or host from which the packet will be sent. Valid options for expressing source are: <ul style="list-style-type: none"> <li>• IP address or range of addresses (A.B.C.D)</li> <li>• <b>any</b> - Any source host</li> <li>• <b>host source</b> - IP address of a single source host</li> </ul>
<i>source-wildcard</i>	(Optional) Specifies the bits to ignore in the <i>source</i> address.
<b>eq port</b>	(Optional) Applies access rules to TCP or UDP source and/or destination port numbers equal to the specified port number. Port numbers can range from 0 to 65535. <b>Note:</b> This parameter is not available when you specify the <b>icmp</b> protocol.
<i>destination</i>	Specifies the network or host to which the packet will be sent. Valid options for expressing destination are: <ul style="list-style-type: none"> <li>• IP address (A.B.C.D)</li> <li>• <b>any</b> - Any destination host</li> <li>• <b>host source</b> - IP address of a single destination host</li> </ul>
<i>destination-wildcard</i>	(Optional) Specifies the bits to ignore in the <i>destination</i> address.
<b>insert</b>   <b>replace</b> <i>entryno</i>	(Optional) Inserts this new entry before a specified entry in an existing ACL, or replaces a specified entry with this new entry.
<b>move</b> <i>destination</i> <i>source1 source2</i>	(Optional) Moves a sequence of access list entries before another entry. <i>Destination</i> is the number of the existing entry before which this new entry will be moved. <i>Source1</i> is a single entry number or the first entry number in the range to be moved. <i>Source2</i> (optional) is the last entry number in the range to be moved. If <i>source2</i> is not specified, only the <i>source1</i> entry will be moved.

### Defaults

If **insert**, **replace**, or **move** are not specified, the new entry will be appended to the access list.

If *source2* is not specified with **move**, only one entry will be moved.

If **eq port** is not specified, TCP/UDP ports are not used for filtering. Only the protocol, source, and destination are used for applying the rule.

## Mode

Global configuration: B5(su)->router(Config)#

## Usage

Access lists are applied to interfaces by using the **ip access-group** command as described in “[ip access-group](#)” on page 22-86.

Valid *access-list-numbers* for extended ACLs are **100 to 199**. For standard ACLs, valid values are **1 to 99**.

All access lists have an implicit “deny any any” statement as their last entry.

## Examples

This example shows how to define access list 145 to deny ICMP transmissions from any source and for any destination:

```
B5(su)->router(Config)#access-list 145 deny ICMP any any
```

This example appends to access list 145 a permit statement that allows the host with IP address 88.255.255.254 to do an SSH remote login to any destination on TCP port 22.

```
B5(su)->router(Config)#access-list 145 permit tcp host 88.255.255.254 any eq 22
```

This example appends to access list 145 a permit statement that allows SNMP control traffic (from UDP port 161) to be sent from IP addresses within the range defined by 88.255.128.0 0.0.127.255 to any destination.

```
B5(su)->router(Config)#access-list 145 permit udp 88.255.128.0 0.0.127.255 eq 161 any
```

# ip access-group

Use this command to apply access restrictions to inbound frames on an interface when operating in router mode. The **no** form of this command removes the specified access list.

## Syntax

```
ip access-group access-list-number in  
no ip access-group access-list-number in
```

## Parameters

<i>access-list-number</i>	Specifies the number of the access list to be applied to the access list. This is a decimal number from <b>1</b> to <b>199</b> .
<b>in</b>	Filters inbound frames.

## Defaults

None.

## Mode

Interface configuration: B5(su)->router(Config-if(Vlan <vlan\_id>))#

## Usage

ACLs must be applied per routing interface. An access list can be applied to inbound traffic only. Access lists can now be applied to routed VLANs which incorporate LAGs.

## Example

This example shows how to apply access list 1 for all inbound frames on the VLAN 1 interface. Through the definition of access list 1, only frames with a source address on the 192.5.34.0/24 network will be routed. All the frames with other source addresses received on the VLAN 1 interface are dropped:

```
B5(su)->router(Config)#access-list 1 permit 192.5.34.0 0.0.0.255
B5(su)->router(Config)#interface vlan 1
B5(su)->router(Config-if(Vlan 1))#ip access-group 1 in
```



## TACACS+ Configuration

This chapter provides information about the commands used to configure and monitor TACACS+ (Terminal Access Controller Access-Control System Plus).

TACACS+ is a security protocol that provides services for secure authentication, CLI command authorization, and CLI auditing for administrative access. It can be used as an alternative to the standard RADIUS security protocol (RFC 2865). TACACS+ runs over TCP and encrypts the body of each management packet.

Based on the now obsolete TACACS protocol (defined in RFC 1492), TACACS+ is defined in an un-published and expired Internet Draft draft-grant-tacacs-02.txt, "The TACACS+ Protocol Version 1.78," January, 1997.

For detailed information about using TACACS+ in your network, refer to the Enterasys Feature Guide "TACACS+ Configuration" located on the Enterasys web site:

<https://extranet.enterasys.com/downloads/>

For information about...	Refer to page...
<a href="#">show tacacs</a>	<a href="#">23-2</a>
<a href="#">set tacacs</a>	<a href="#">23-3</a>
<a href="#">show tacacs server</a>	<a href="#">23-3</a>
<a href="#">set tacacs server</a>	<a href="#">23-4</a>
<a href="#">clear tacacs server</a>	<a href="#">23-5</a>
<a href="#">show tacacs session</a>	<a href="#">23-6</a>
<a href="#">set tacacs session</a>	<a href="#">23-7</a>
<a href="#">clear tacacs session</a>	<a href="#">23-8</a>
<a href="#">show tacacs command</a>	<a href="#">23-9</a>
<a href="#">set tacacs command</a>	<a href="#">23-9</a>
<a href="#">show tacacs singleconnect</a>	<a href="#">23-10</a>
<a href="#">set tacacs singleconnect</a>	<a href="#">23-10</a>
<a href="#">show tacacs interface</a>	<a href="#">23-11</a>
<a href="#">set tacacs interface</a>	<a href="#">23-11</a>
<a href="#">clear tacacs interface</a>	<a href="#">23-12</a>

## show tacacs

Use this command to display the current TACACS+ configuration information and status.

### Syntax

```
show tacacs [state]
```

### Parameters

<b>state</b>	(Optional) Displays only the TACACS+ client status.
--------------	---

### Defaults

If **state** is not specified, all TACACS+ configuration information will be displayed.

### Mode

Switch command, Read-Only.

### Example

This example shows how to display all TACACS configuration information.

```
B5(ro)->show tacacs
TACACS+ status:Disabled
TACACS+ session accounting state:disable
TACACS+ command authorization state:disable
TACACS+ command aaccounting state:disable
TACACS+ single connect state:Disabled
TACACS+ service: exec
TACACS+ session authorization A-V pairs:
      access-level   attribute   value
      read-only     priv-lvl   0
      read-write     priv-lvl   1
      super-user     priv-lvl   15
TACACS+ Server  IP address      Port    Timeout
-----
1              192.168.10.1   49      10
```

[Table 23-1](#) provides an explanation of the command output.

**Table 23-1 show tacacs Output Details**

Output...	What it displays...
TACACS+ status	Whether the TACACS+ client is <b>enabled</b> or <b>disabled</b> .
TACACS+ session accounting state	Whether TACACS+ session accounting is <b>enabled</b> or <b>disabled</b> .
TACACS+ command authorization state	Whether TACACS+ command authorization is <b>enabled</b> or <b>disabled</b> .
TACACS+ command accounting state	Whether TACACS+ command accounting is <b>enabled</b> or <b>disabled</b> .

**Table 23-1 show tacacs Output Details (Continued)**

Output...	What it displays...
TACACS+ singleconnect state	Whether TACACS+ singleconnect is <b>enabled</b> or <b>disabled</b> . When enabled, the TACACS+ client sends multiple requests over a single TCP connection.
TACACS+ service	The name of the service that is requested by the TACACS+ client for session authorization. "exec" is the default service name.
TACACS+ session authorization A-V pairs	Displays the attribute – value pairs that are mapped to the <b>read-only</b> , <b>read-write</b> , and <b>super-user</b> access privilege levels for the service requested for session authorization.  The attribute names and values shown in the example above are the default values.
TACACS+ Server	Displays the TACACS+ server information used by the TACACS+ client.

## set tacacs

Use this command to enable or disable the TACACS+ client.

### Syntax

```
set tacacs {enable | disable}
```

### Parameters

<b>enable   disable</b>	Enables or disables the TACACS client.
-------------------------	--

### Defaults

None.

### Mode

Switch command, Read-Write.

### Usage

The TACACS+ client can be enabled on the switch anytime, with or without a TACACS+ server online. If the TACACS+ server is offline and TACACS+ is enabled, the login authentication is switched to RADIUS or local, if enabled.

### Examples

This example shows how to enable the TACACS+ client.

```
B5(rw)->set tacacs enable
```

## show tacacs server

Use this command to display the current TACACS+ server configuration.

### Syntax

```
show tacacs server {index | all}
```

## Parameters

<i>index</i>	Display the configuration of the TACACS+ server identified by <i>index</i> . The value of <i>index</i> can range from 1 to 2,147,483,647.
<b>all</b>	Display the configuration for all configured TACACS+ servers.

## Defaults

None.

## Mode

Switch command, Read-Only.

## Example

This example displays configuration information for TACACS+ server 1.

```
B5(ro)->show tacacs server 1
TACACS+ Server  IP address      Port      Timeout
-----
1                192.168.10.1  49        10
```

## set tacacs server

Use this command to configure the TACACS+ server(s) to be used by the TACACS+ client. You can configure the timeout value for all configured servers or a single server, or you can configure the IP address, TCP port, and secret for a single server. For simplicity, two syntax statements are shown.

## Syntax

```
set tacacs server {all | index} timeout seconds
set tacacs server index address port secret
```

## Parameters

<b>all</b>	Specify the timeout value for all configured TACACS+ servers.
<i>index</i>	Configure the TACACS+ server identified by <i>index</i> . The value of <i>index</i> can range from 1 to 2,147,483,647.
<b>timeout</b> <i>seconds</i>	Set the timeout value for the specified server(s) in seconds. The value of <i>seconds</i> can range from 1 to 180 seconds. The default timeout value is 10 seconds.
<i>address</i>	Specify the IP address of the TACACS+ server.
<i>port</i>	Specify the TCP port for the TACACS+ server. The value of <i>port</i> can range from 0 to 65535, but typically, port 49 is specified.
<i>secret</i>	Specify the secret (shared password) for the TACACS+ server.

## Defaults

No TACACS+ servers are configured by default.

When you do configure a TACACS+ server, the default timeout value is 10 seconds.



## Mode

Switch command, Read-Write.

## Usage

Up to 5 TACACS+ servers can be configured, with the index value of 1 having the highest priority. If you want to change the default timeout value for a specific server or all servers, you must enter the command using the **timeout** parameter.

When at least one backup server has been configured and the switch loses contact with the primary server, the switch will contact the next server in priority. If the switch was trying to authenticate a user when the connection was lost, or if the default login access (read-only permissions) had been received, the switch will try to authenticate again.

If a user had already been authenticated and authorized, then the backup server is contacted without requiring any authentication. The backup server will just authorize or account for the packets coming in for that user. Since a task ID is associated with each accounting session, if there is a failover to a backup server, the accounting information will still be associated with the correct session using the task ID.

When a failover to a backup server occurs, syslog messages are generated containing the reason for the failure.

## Example

This example configures TACACS+ server 1. Then, the default timeout value of 10 seconds is changed to 20 seconds.

```
B5(rw)->set tacacs server 1 192.168.10.10 49 mysecret
B5(rw)->set tacacs server 1 timeout 20
```

## clear tacacs server

Use this command to remove one or all configured TACACS+ servers, or to return the timeout value to its default value for one or all configured TACACS+ servers.

## Syntax

```
clear tacacs server {all | index} [timeout]
```

## Parameters

<b>all</b>	Specifies that all configured TACACS+ servers should be affected.
<i>index</i>	Specifies one TACACS+ server to be affected.
<b>timeout</b>	(Optional) Return the timeout value to its default value of 10 seconds.

## Defaults

If **timeout** is not specified, the affected TACACS+ servers will be removed.

## Mode

Switch command, Read-Write.

## Examples

This example removes TACACS+ server 1.

```
B5(rw)->clear tacacs server 1
```

This example resets the timeout value to its default value of 10 seconds for all configured TACACS+ servers.

```
B5(rw)->clear tacacs server all timeout
```

## show tacacs session

Use this command to display the current TACACS+ client session settings.

### Syntax

```
show tacacs session {authorization | accounting}
```

### Parameters

<b>authorization</b>	Display client session authorization settings.
<b>accounting</b>	Display client session accounting settings.

### Defaults

None.

### Mode

Switch command, Read-Only.

### Examples

This example shows how to display client session authorization information:

```
B5(ro)->show tacacs session authorization
TACACS+ service: exec
TACACS+ session authorization A-V pairs:
      access-level  attribute  value
      read-only    priv-lvl  0
      read-write    priv-lvl  1
      super-user    priv-lvl  15
```

This example shows how to display client session accounting state.

```
B5(ro)->show tacacs session accounting
TACACS+ session accounting state:  enabled
```

## set tacacs session

Use this command to enable or disable TACACS+ session accounting, or to configure TACACS+ session authorization parameters. For simplicity, separate syntax formats are shown for configuring session accounting and session authorization.

### Syntax

```
set tacacs session accounting {enable | disable}
set tacacs session authorization {service name | read-only attribute value |
read-write attribute value | super-user attribute value}
```

### Parameters

<b>accounting</b>	Specifies that TACACS+ session accounting is being configured.
<b>enable   disable</b>	Enables or disables TACACS+ session accounting.
<b>authorization</b>	Specifies that TACACS+ session authorization is being configured.
<b>service name</b>	Specifies the name of the service that the TACACS+ client will request from the TACACS+ server. The <i>name</i> specified here must match the name of a service configured on the server. The default service name is <code>exec</code> .
<b>read-only attribute value</b>	Specifies that the <b>read-only</b> access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by <i>attribute</i> and <i>value</i> .  By default, <i>attribute</i> is "priv-lvl" and <i>value</i> is 0.
<b>read-write attribute value</b>	Specifies that the <b>read-write</b> access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by <i>attribute</i> and <i>value</i> .  By default, <i>attribute</i> is "priv-lvl" and <i>value</i> is 1.
<b>super-user attribute value</b>	Specifies that the <b>super-user</b> access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by <i>attribute</i> and <i>value</i> .  By default, <i>attribute</i> is "priv-lvl" and <i>value</i> is 15.

### Defaults

None.

### Mode

Switch command, Read-Write.

### Usage

When session accounting is enabled, the TACACS+ server will log accounting information, such as start and stop times, IP address of the client, and so forth, for each authorized client session.

When the TACACS+ client is enabled on the switch (with the **set tacacs enable** command), the session authorization parameters configured with this command are sent by the client to the TACACS+ server when a session is initiated on the switch. The parameter values must match a service and access level attribute-value pairs configured on the server for the session to be authorized. If the parameter values do not match, the session will not be allowed.

The service name and attribute-value pairs can be any character string, and are determined by your TACACS+ server configuration.

Since a task ID is associated with each accounting session, if there is a failover to a backup server, the accounting information will still be associated with the correct session using the task ID.

## Examples

This example configures the service requested by the TACACS+ client as the service name “basic.”

```
B5(rw)->set tacacs session authorization service basic
```

This example maps the **read-write** access privilege level to an attribute named “priv-lvl” with the value of 5 configured on the TACACS+ server.

```
B5(rw)->set tacacs session authorization read-write priv-lvl 5
```

This example enables TACACS+ session accounting.

```
B5(rw)->set tacacs session accounting enable
```

## clear tacacs session

Use this command to return the TACACS+ session authorization settings to their default values.

### Syntax

```
clear tacacs session authorization {[service] |[read-only] |[read-write] |
[super-user]}
```

### Parameters

<b>authorization</b>	Clears the TACACS+ session authorization parameters.
<b>service</b>	Clears the TACACS+ session authorization service name to the default value of “exec.”
<b>read-only</b>	Clears the TACACS+ session authorization read-only attribute-value pair to their default values of “priv-lvl” and 0.
<b>read-write</b>	Clears the TACACS+ session authorization read-write attribute-value pair to their default values of “priv-lvl” and 1.
<b>super-user</b>	Clears the TACACS+ session authorization super-user attribute-value pair to their default values of “priv-lvl” and 15.

### Defaults

At least one of the session authorization parameters must be specified.

### Mode

Switch command, Read-Write.

### Examples

This example shows how to return the service name to the default of “exec.”

```
B5(rw)->clear tacacs session authorization service
```

This example shows how to return all the session authorization parameters to their default values.

```
B5(rw)->clear tacacs session authorization service read-only read-write super-
user
```

## show tacacs command

Use this command to display the status (enabled or disabled) of TACACS+ accounting or authorization on a per-command basis.

### Syntax

```
show tacacs command {accounting | authorization}
```

### Parameters

<b>accounting</b>	Display the status of TACACS+ accounting on a per-command basis.
<b>authorization</b>	Display the status of TACACS+ authorization on a per-command basis.

### Defaults

None.

### Mode

Switch command, Read-Write.

### Example

This example shows how to display the state of the TACACS+ client's command authorization.

```
B5(rw)->show tacacs command authorization
TACACS+ command authorization state:  enabled
```

## set tacacs command

Use this command to enable or disable TACACS+ accounting or authorization on a per-command basis.

### Syntax

```
set tacacs command {accounting | authorization} {enable | disable}
```

### Parameters

<b>accounting   authorization</b>	Specifies either TACACS+ accounting or authorization to be enabled or disabled.
<b>enable   disable</b>	Enable or disable accounting or authorization on a per-command basis.

### Defaults

None.

### Mode

Switch command, Read-Write.

### Usage

In order for per-command accounting or authorization by a TACACS+ server to take place, the command must be executed within an authorized session.

When per-command accounting is enabled, the TACACS+ server will log accounting information, such as start and stop times, IP address of the client, and so forth, for each command executed during the session.

When per-command authorization is enabled, the TACACS+ server will check whether each command is permitted for that authorized session and return a success or fail. If the authorization fails, the command is not executed.

### Example

This example shows how to enable TACACS+ authorization on a command basis.

```
B5(rw)->set tacacs command authorization enable
```

## show tacacs singleconnect

Use this command to display the current status of the TACACS+ client's ability to send multiple requests over a single TCP connection.

### Syntax

```
show tacacs singleconnect
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, Read-Write.

### Example

This example shows how to display the state of the TACACS+ client's ability to send multiple requests over a single connection.

```
B5(rw)->show tacacs singleconnect
TACACS+ single-connect state: enabled
```

## set tacacs singleconnect

Use this command to enable or disable the ability of the TACACS+ client to send multiple requests over a single TCP connection. When enabled, the TACACS+ client will use a single TCP connection for all requests to a given TACACS+ server.

### Syntax

```
set tacacs singleconnect {enable | disable}
```

### Parameters

---

<b>enable   disable</b>	Enable or disable the ability to send multiple requests over a single TCP connection.
-------------------------	---

---

## Defaults

None.

## Mode

Switch command, Read-Write.

## Examples

This example shows how to disable sending multiple requests over a single connection.

```
B5(rw)->set tacacs singleconnect disable
```

## show tacacs interface

Use this command to display the interface used for the source IP address of the TACACS+ packets generated by the switch.

### Syntax

```
show tacacs interface
```

### Parameters

None.

### Defaults

None.

### Mode

Switch mode, read-only.

### Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the TACACS+ packets generated by the switch.

```
B5(rw)->show tacacs interface
loopback 1 192.168.10.1
```

## set tacacs interface

Use this command to specify the interface used for the source IP address of the TACACS+ packets generated by the switch.

### Syntax

```
set tacacs interface {loopback loop-ID | vlan vlan-ID}
```

### Parameters

<b>loopback</b> <i>loop-ID</i>	Specifies the loopback interface to be used. The value of <i>loop-ID</i> can range from 0 to 7.
--------------------------------	---

---

<b>vlan</b> <i>vlan-ID</i>	Specifies the VLAN interface to be used. The value of vlan-ID can range from 1 to 4093.
----------------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command allows you to configure the source IP address used by the TACACS+ application on the switch when generating packets for management purposes. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the TACACS+ client.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface will be used.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

## Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the TACACS+ client source IP address.

```
B5(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
B5(rw)->router(Config-if(Vlan 100))#exit
B5(rw)->router(Config)#exit
B5(rw)->router#exit
B5(rw)->router>exit
B5(rw)->set tacacs interface vlan 100

B5(rw)->show tacacs interface
vlan 100 192.168.10.1
```

## clear tacacs interface

Use this command to clear the interface used for the source IP address of the TACACS+ client back to the default of the Host interface.

### Syntax

```
clear tacacs interface
```

### Parameters



None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This command returns the interface used for the source IP address of the TACACS+ client back to the default of the Host interface.

```
B5(rw)->show tacacs interface
vlan 100 192.168.10.1
B5(rw)->clear tacacs interface
B5(rw)->
```

clear tacacs interface

---

## sFlow Configuration

This chapter provides information about the commands used to configure and monitor the sFlow system.

For information about...	Refer to page...
<a href="#">Overview</a>	24-1
<a href="#">Commands</a>	24-4

### Overview

sFlow is a method for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives visibility into network activity, enabling effective management and control of network resources.

An sFlow solution consists of an sFlow Agent, embedded in the network device such as a switch or router, and an sFlow Collector. The sFlow Agent uses sampling technology to capture traffic statistics from the device it is monitoring and immediately forwards the sampled traffic statistics to an sFlow Collector for analysis in sFlow datagrams.

The sFlow Agent uses two forms of sampling — statistical packet-based sampling of switched or routed Packet Flows, and time-based sampling of counters.

Version 5 of sFlow is described in detail in the document entitled “sFlow Version 5” available from sFlow.org (<http://www.sflow.org>).

### Using sFlow in Your Network

The advantages of using sFlow include:

- sFlow makes it possible to monitor ports of a switch, with no impact on the distributed switching performance. (See “Usage Notes” on page 24-3 for more information.)
- sFlow requires very little memory or CPU usage. Samples are not aggregated into a flow-table on the switch — they are forwarded immediately over the network to the sFlow Collector.
- The system is tolerant to packet loss in the network. (The statistical model means loss is equivalent to a slight change in the sampling rate.)
- The sFlow Collector can receive data from multiple switches, providing a real-time synchronized view of the whole network.
- The sFlow Collector can analyze traffic patterns for whatever protocols are found in the packet headers (for example, TCP/IP, IPX, Ethernet, AppleTalk). There is no need for the layer 2 switch to decode and understand all protocols.

## Definitions

The following table describes some of the main sFlow terms and concepts.

**Table 24-1 sFlow Definitions**

Term	Definition
Data Source	A Data Source refers to a location within a Network Device that can make traffic measurements. Possible Data Sources include interfaces and VLANs.
Packet Flow	A Packet Flow is defined as the path or trajectory that a packet takes through a Network Device (That is, the path that a packet takes as it is received on one interface, is subjected to a switching/routing decision, and is then sent on another interface).
Packet Flow Sampling	Packet Flow Sampling refers to the random selection of a fraction of the Packet Flows observed at a Data Source.
Sampling Rate	The Sampling Rate specifies the ratio of packets observed at the Data Source to the samples generated.
Sampling Interval	The time period between successive Counter Samples.
sFlow Instance	An sFlow Instance refers to a measurement process associated with a Data Source.
sFlow Agent	The sFlow Agent provides an interface for configuring the sFlow Instances within a device.
sFlow Collector	An sFlow Collector receives sFlow Datagrams from one or more sFlow Agents. The sFlow Collector may also configure sFlow Instances using the configuration mechanisms provided by the sFlow Agent.
sFlow Datagram	An sFlow Datagram is a UDP datagram that contains the measurement data, and information about the measurement source and process.

## sFlow Agent Functionality

Packet flow sampling and counter sampling are performed by sFlow Instances associated with individual Data Sources within the sFlow Agent. Packet flow sampling and counter sampling are designed as part of an integrated system. Both types of samples are combined in sFlow datagrams. Packet flow sampling will cause a steady, but random, stream of sFlow datagrams to be sent to the sFlow Collector. Counter samples may be taken opportunistically in order to fill these datagrams.

In order to perform packet flow sampling, an sFlow Sampler Instance is configured with a sampling rate. The packet flow sampling process results in the generation of packet flow records. In order to perform counter sampling, an sFlow Poller Instance is configured with a polling interval. The counter sampling process results in the generation of counter records. The sFlow Agent collects counter records and packet flow records and sends them in the form of sFlow datagrams to sFlow Collectors.

## Sampling Mechanisms

Two forms of sampling are performed by the sFlow Agent: statistical packet-based sampling of switched or routed packet flows, and time-based sampling of counters.

## Packet Flow Sampling

The packet flow sampling mechanism carried out by each sFlow Instance ensures that any packet observed at a Data Source has an equal chance of being sampled, irrespective of the packet flow(s) to which it belongs.

Packet flow sampling is accomplished as follows:

1. When a packet arrives on an interface, the Network Device makes a filtering decision to determine whether the packet should be dropped.
2. If the packet is not filtered (dropped), a destination interface is assigned by the switching/routing function.
3. At this point, a decision is made on whether or not to sample the packet. The mechanism involves a counter that is decremented with each packet. When the counter reaches zero a sample is taken.
4. When a sample is taken, the counter indicating how many packets to skip before taking the next sample is reset. The value of the counter is set to a random integer where the sequence of random integers used over time is the Sampling Rate.

Packet flow sampling results in the generation of Packet Flow Records. A Packet Flow Record contains information about the attributes of a packet flow, including:

- Information on the packet itself — a packet header, packet length, and packet encapsulation.
- Information about the path the packet took through the device, including information relating to the selection of the forwarding path.

## Counter Sampling

The primary objective of the counter sampling is to, in an efficient way, periodically export counters associated with Data Sources. A maximum sampling interval is assigned to each sFlow Instance associated with a Data Source.

Counter sampling is accomplished as follows:

1. The sFlow Agent keep a list of counter sources being sampled.
2. When a Packet Flow Sample is generated, the sFlow Agent examines the list of counter sources and adds counters to the sample datagram, least recently sampled first.

Counters are only added to the datagram if the sources are within a short period, 5 seconds say, of failing to meet the required sampling interval.

3. Periodically, say every second, the sFlow Agent examines the list of counter sources and sends any counters that need to be sent to meet the sampling interval requirement.

The set of counters is a fixed set defined in Section 5 of the document entitled “sFlow Version 5” available from sFlow.org (<http://www.sflow.org>).

## Usage Notes

sFlow is disabled by default, and therefore must be manually enabled.

Although the switch hardware has the capability to sample packets on any port, to ensure that CPU utilization is not compromised, the number of sFlow samplers that can be configured per switch or stack of switches is limited to a maximum of 32. There is no limitation on the number of pollers that can be configured.

Under certain circumstances, the switch will drop packet samples that the sFlow implementation is not able to count and therefore cannot correctly report `sample_pool` and `drops` fields of flow

samples sent to the sFlow Collector. Under heavy load, this sample loss could be significant and could therefore affect the accuracy of the sampling analysis.

## Example Configuration

The general procedure for configuring sFlow includes:

1. Configure your sFlow Collector information to be used by the sFlow Agent on the switch. Up to eight Collectors can be configured. The information is stored in the sFlowReceiverTable.
2. Enable and configure sFlow packet flow sampling instances on each port.
3. Enable and configure sFlow counter sampling poller instances on each port.

The following is an example of the commands used to configure sFlow:

```
# configure sFlow Collector 1
# accept defaults for datagram size and port
set sflow receiver 1 owner enterasys timeout 180000
set sflow receiver 1 ip 192.168.16.91
#
#configure packet sampling instances on ports 1 through 12
#assign to sFlow Collector 1
set sflow port ge.1.1-12 sampler 1
set sflow port ge.1.1-12 sampler maxheadersize 256
set sflow port ge.1.1-12 sampler rate 2048
#
#configure counter poller instances on ports 1 through 12
#assign to sFlow Collector 1
set sflow port ge.1.1-12 poller 1
set sflow port ge.1.1-12 poller interval 20
```

## Commands

For information about...	Refer to page...
<a href="#">show sflow receivers</a>	<a href="#">24-5</a>
<a href="#">set sflow receiver owner</a>	<a href="#">24-7</a>
<a href="#">set sflow receiver ip</a>	<a href="#">24-7</a>
<a href="#">set sflow receiver maxdatagram</a>	<a href="#">24-8</a>
<a href="#">set sflow receiver port</a>	<a href="#">24-9</a>
<a href="#">clear sflow receiver</a>	<a href="#">24-9</a>
<a href="#">set sflow port poller</a>	<a href="#">24-10</a>
<a href="#">show sflow pollers</a>	<a href="#">24-11</a>
<a href="#">clear sflow port poller</a>	<a href="#">24-12</a>
<a href="#">set sflow port sampler</a>	<a href="#">24-12</a>
<a href="#">show sflow samplers</a>	<a href="#">24-13</a>

For information about...	Refer to page...
<a href="#">clear sflow port sampler</a>	<a href="#">24-14</a>
<a href="#">set sflow interface</a>	<a href="#">24-14</a>
<a href="#">show sflow interface</a>	<a href="#">24-15</a>
<a href="#">clear sflow interface</a>	<a href="#">24-16</a>
<a href="#">show sflow agent</a>	<a href="#">24-17</a>

## show sflow receivers

Use this command to display the contents of the sFlow Receivers Table, or to display information about a specific sFlow Collector listed in the table.

### Syntax

```
show sflow receivers [index]
```

### Parameters

<i>index</i>	(Optional) Specifies a specific Collector to display information about.
--------------	---

### Defaults

The contents of the sFlow Receivers Table is displayed.

### Mode

Switch command, read-only.

### Usage

Executing this command without specifying an index into the sFlow Receivers Table displays information about all the Collectors configured on the switch.

If you specify an individual Collector by its index number, additional information is displayed for that Collector.

### Examples

This example displays the sFlow Receivers Table.

```
B5(su)->show sflow receivers
```

```
Receiver Owner      Time out   Max Datagram Port  IP Address
  Index   String                Size
-----
  1      ets1      17766      1400      6343  10.1.2.117
```

This example displays information about the Collector with index 1.

```
B5(su)->show sflow receivers 1
```

```
Receiver Index      1
Owner String        ets1
Time out            17758
```

```

IP Address:                10.1.2.117
Address Type               IPv4
Port                      6343
Datagram Version          5
Maximum Datagram Size     1400

```

The following table describes the output fields.

**Table 24-2 show sflow receivers Output Descriptions**

Output...	What it displays...
Receiver Index	Index number of a specific Collector entry in the sFlow Receivers Table. Up to 8 Collectors may be configured.
Owner String	Identity string of the Collector. An empty string indicates that the entry is unclaimed and cannot be assigned to a sampler or poller instance. The owner string is configured with the <a href="#">set sflow receiver owner</a> command.
Time Out	The time remaining, in seconds, before the sampler or poller is released and stops sending samples to this receiver/Collector. The timeout value is configured with the <a href="#">set sflow receiver owner</a> command.
IP Address	The IP address of this receiver/Collector. The IP address is configured with the <a href="#">set sflow receiver ip</a> command.
Address Type	Whether the Collector IP address is IPv4 or IPv6.
Port	The UDP port number on this receiver/Collector to which sample datagrams should be sent. The default value is 6343, which can be changed with the <a href="#">set sflow receiver port</a> command.
Datagram Version	Specifies the sFlow version used for formatting the sample datagrams.
Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram to this receiver/Collector. The default value is 1400 bytes, which can be changed with the <a href="#">set sflow receiver maxdatagram</a> command.



## set sflow receiver owner

Use this command to configure the owner identity string and timeout value for an sFlow Collector in the switch's sFlow Receivers Table.

### Syntax

```
set sflow receiver index owner owner-string timeout timeout
```

### Parameters

<i>index</i>	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The <i>index</i> can range from 1 to 8.
<b>owner</b> <i>owner-string</i>	The identity string of the receiver/Collector being configured. The string can be up to 127 characters in length.
<b>timeout</b> <i>timeout</i>	The time, in seconds, remaining before the receiver/Collector being configured and all associated samplers and pollers expire. The value can range from 0 to 4294967295 seconds.

### Defaults

None.

### Mode

Switch command, read-write.

### Usage

In order for an sFlow Collector to be assigned to receive sample datagrams from the sFlow Agent on the switch, an entry for that Collector must be configured in the switch's sFlow Receivers Table. An entry must contain an owner identity string, a non-zero timeout value, and the IP address of the Collector. Configure the IP address with the [set sflow receiver ip](#) command.

An entry without an owner identity string is considered unclaimed and cannot be assigned as a receiver to sampler or poller instances.

Once the timer set by this command expires, the receiver/Collector and all the samplers and pollers associated with this Collector expire and are removed from the switch's configuration. In order to start sending sample data to the Collector again, the Collector must be reconfigured with a new timeout value and samplers and pollers must be configured again. Therefore, you should consider setting the timeout value to the largest value that is reasonable for your environment.

### Example

This example configures an entry for index 1 in the sFlow Receivers Table.

```
B5(su)->set sflow receiver 1 owner ets1 timeout 180000
```

## set sflow receiver ip

Use this command to configure the IP address of an sFlow Collector in the switch's sFlow Receivers Table.

### Syntax

```
set sflow receiver index ip ipaddr
```

## Parameters

---

<i>index</i>	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The <i>index</i> can range from 1 to 8.
<b>ip</b> <i>ipaddr</i>	The IP address of the receiver/Collector being configured.

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

In order for an sFlow Collector to be assigned to receive sample datagrams from the sFlow Agent on the switch, an entry for that Collector must be configured in the switch's sFlow Receivers Table. An entry must contain an owner identity string, a non-zero timeout value, and the IP address of the Collector. Configure the owner identity string and timeout value with the [set sflow receiver owner](#) command.

## Example

This example configures an IP address of 10.10.10.10 to index entry 1.

```
B5(su)->set sflow receiver 1 ip 10.10.10.10
```

# set sflow receiver maxdatagram

Use this command to set the maximum number of data bytes that can be sent in a single sample datagram.

## Syntax

```
set sflow receiver index maxdatagram bytes
```

## Parameters

---

<i>index</i>	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The <i>index</i> can range from 1 to 8.
<b>maxdatagram</b> <i>bytes</i>	Specifies the maximum number of data bytes that can be sent in a single sample datagram. This size should be set to avoid fragmentation of the sFlow datagrams.  The value of <i>bytes</i> can range from 200 to 9116. The default is 1400.

---

## Defaults

Default maximum datagram size is 1400 bytes.

## Mode

Switch command, read-write.

## Example

This example sets the maximum datagram size to 2800 bytes for index entry 1.

```
B5(su)->set sflow receiver 1 maxdatagram 2800
```

## set sflow receiver port

Use this command to configure the UDP port on the sFlow Controller to which the switch will send sample datagrams.

### Syntax

```
set sflow receiver index port port
```

### Parameters

<i>index</i>	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The <i>index</i> can range from 1 to 8.
<b>port</b> <i>port</i>	Specifies the UDP port on the receiver/Collector to which the sample datagrams should be sent. By default, the port is 6343.

### Defaults

The default port value is 6343.

### Mode

Switch command, read-write.

### Example

This example changes the sFlow receiver port on the Collector to 1234.

```
B5(su)->set sflow receiver 1 port 1234
```

## clear sflow receiver

Use this command to delete a receiver/Collector from the sFlow Receivers Table, or to return certain parameters to their default values for the specified Collector.

### Syntax

```
clear sflow receiver index [ip | maxdatagram | owner [timeout] | port]
```

### Parameters

<i>index</i>	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The <i>index</i> can range from 1 to 8.
<b>ip</b>	(Optional) Clear the IP address.
<b>maxdatagram</b>	(Optional) Return the maximum datagram size to 1400 bytes.
<b>owner</b>	(Optional) Clear the owner identity string. Entries in the sFlow Receiver Table without an identity string are considered unclaimed.
<b>timeout</b>	(Optional) Clear the timeout value of the specified entry.

<b>port</b> <i>port</i>	(Optional) Clear the UDP port on the receiver/Collector to which the sample datagrams should be sent. The value is reset to the default of 6343.
-------------------------	--

## Defaults

If no optional parameters are specified, the entire entry is cleared.

## Mode

Switch command, read-write.

## Usage

You can clear the IP address, maximum datagram size, or UDP port without deleting an entry from the sFlow Receivers Table. If you clear the owner or timeout, the entire entry is cleared. If you enter only an entry index and none of the optional parameters, the entire entry is cleared.

Once an entry is cleared, all pollers and samplers associated with that receiver are also removed from the switch configuration.

## Example

This example returns the maximum datagram size to the default of 1400 bytes for the Collector with index 1.

```
B5(su)->clear sflow receiver 1 maxdatagram
```

# set sflow port poller

Use this command to configure poller instances on ports, or data sources.

## Syntax

```
set sflow port port-string poller {index | interval seconds}
```

## Parameters

<i>port-string</i>	Specifies the port or ports (data sources) on which the poller instance is being configured.
<i>index</i>	Index number in the sFlow Receivers Table for the receiver/Collector with which the poller instance is associated. The <i>index</i> can range from 1 to 8.
<b>interval</b> <i>seconds</i>	Specifies the polling interval, which can range from 0 to 86400 seconds. A value of 0 disables counter sampling.

## Defaults

The default interval value is 0 seconds, which disables counter sampling.

## Mode

Switch command, read-write.

## Usage

A poller instance performs counter sampling on the data source to which it is configured. Refer to [“Sampling Mechanisms”](#) on page 24-2 for more information.

You must first associate a receiver/Collector in the sFlow Receivers Table with the poller instance, before configuring the polling interval.

When a receiver times out or is cleared from the sFlow Receivers Table, all poller and sampler instances associated with that receiver are also cleared from the switch’s configuration.

## Example

The following example configures poller instances on ports ge.1.1 through ge.1.8 and associates them with receiver 1. Then, a polling interval of 240 seconds is configured.

```
B5(su)->set sflow port ge.1.1-8 poller 1
B5(su)->set sflow port ge.1.1-8 poller interval 240
```

## show sflow pollers

Use this command to display information about configured poller instances.

### Syntax

```
show sflow pollers
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example displays the output of this command.

```
B5(su)->show sflow pollers

  Poller      Receiver  Poller
  Data Source  Index     Interval
  -----
  ge.1.1      1         240
  ge.1.2      1         240
  ge.1.3      1         240
  ge.1.4      1         240
  ge.1.5      1         240
  ge.1.6      1         240
  ge.1.7      1         240
  ge.1.8      1         240
```

## clear sflow port poller

Use this command to change the poller interval or to remove poller instances.

### Syntax

```
clear sflow port port-string poller [interval]
```

### Parameters

<i>port-string</i>	Specifies the port or ports on which the poller instance is being cleared.
<b>interval</b>	(Optional) Specifies that the polling interval should be cleared to 0. A value of 0 disables counter sampling.

### Defaults

If **interval** is not specified, the poller instance is cleared.

### Mode

Switch command, read-write.

### Example

This example removes the poller instance on port ge.1.1.

```
B5(su)->clear sflow port ge.1.1 poller
```

## set sflow port sampler

Use this command to configure sampler instances on ports, or data sources.

### Syntax

```
set sflow port port-string sampler {index | maxheadersize bytes | rate rate}
```

### Parameters

<i>port-string</i>	Specifies the port or ports (data sources) on which the sampler instance is being configured.
<i>index</i>	Index number in the sFlow Receivers Table for the receiver/Collector with which the sampler instance is associated. The <i>index</i> can range from 1 to 8.
<b>maxheadersize</b> <i>bytes</i>	Specifies the maximum number of bytes that should be copied from the sampler packet. The value can range from 20 to 256 bytes. The default is 128 bytes.
<b>rate</b> <i>rate</i>	Specifies the statistical sampling rate for sampling from this data source. The value of <i>rate</i> specifies the number of incoming packets from which one packet will be sampled. For example, if the rate is 1024, one packet will be sampled from every 1024 ingressing packets on this data source.  The rate can range from 1024 to 65536. A value of 0 disables sampling. The default value is 0.

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

A sampler instance performs packet flow sampling on the data source to which it is configured. Refer to “[Sampling Mechanisms](#)” on page 24-2 for more information.

You must first associate a receiver/Collector in the sFlow Receivers Table with the sampler instance, before configuring the sampling rate or maximum number of bytes copied from sampled packets.

When a receiver times out or is cleared from the sFlow Receivers Table, all poller and sampler instances associated with that receiver are also cleared from the switch’s configuration.

A maximum of 32 sampler instances can be configured per switch or stack of switches.

## Example

The following example configures sampler instances on ports ge.1.1 through ge.1.8 and associates them with receiver 1. Then, a sampling rate of 1024 is configured. The default max header size of 128 bytes is used.

```
B5(su)->set sflow port ge.1.1-8 sampler 1
B5(su)->set sflow port ge.1.1-8 sampler rate 1024
```

# show sflow samplers

Use this command to display information about configured sampler instances.

## Syntax

```
show sflow samplers
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-only.

## Example

This example displays the output of this command.

```
B5(su)->show sflow samplers
  Sampler      Receiver  Packet      Max Header
  Data Source  Index     Sampling Rate  Size
  -----
  ge.1.1       1         1024         128
```

ge.1.2	1	1024	128
ge.1.3	1	1024	128
ge.1.4	1	1024	128
ge.1.5	1	1024	128
ge.1.6	1	1024	128
ge.1.7	1	1024	128
ge.1.8	1	1024	128

## clear sflow port sampler

Use this command to change the sampler rate or maximum header size, or to remove sampler instances.

### Syntax

```
clear sflow port port-string sampler [maxheadersize | rate]
```

### Parameters

---

<i>port-string</i>	Specifies the port or ports on which the sampler instance is being cleared.
<b>maxheadersize</b>	(Optional) Specifies that the maximum header size should be cleared to the default value of 128 bytes.
<b>rate</b>	(Optional) Specifies that the sampling rate should be cleared to the default value of 0, which disables sampling by the instance.

---

### Defaults

If neither optional parameter is specified, the sampler instance is cleared.

### Mode

Switch command, read-write.

### Example

This example removes the sampler instance on port ge.1.1.

```
B5(su)->clear sflow port ge.1.1 sampler
```

## set sflow interface

Use this command to specify the interface used for the source IP address of the sFlow Agent when sending sampling datagrams to the sFlow Collector.

### Syntax

```
set sflow interface {loopback loop-ID | vlan vlan-ID}
```

### Parameters

---

<b>loopback</b> <i>loop-ID</i>	Specifies the loopback interface to be used. The value of <i>loop-ID</i> can range from 0 to 7.
--------------------------------	---

---



---

<b>vlan</b> <i>vlan-ID</i>	Specifies the VLAN interface to be used. The value of vlan-ID can range from 1 to 4093.
----------------------------	---

---

## Defaults

None.

## Mode

Switch command, read-write.

## Usage

This command allows you to configure the management interface used by the sFlow Agent when sending sampling datagrams to the sFlow Collector. Any of the interfaces, including VLAN routing interfaces, can be configured as the management interface.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the Host VLAN will be used as the management interface.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

## Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the management interface for the sFlow Agent.

```
B5(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
B5(rw)->router(Config-if(Vlan 100))#exit
B5(rw)->router(Config)#exit
B5(rw)->router#exit
B5(rw)->router>exit
B5(rw)->set sflow interface vlan 100

B5(rw)->show sflow interface
vlan 100 192.168.10.1
```

## show sflow interface

Use this command to display the interface used by the sFlow Agent when sending sampling datagrams to the sFlow Collector.

### Syntax

```
show sflow interface
```

### Parameters

None.

## Defaults

None.

## Mode

Switch mode, read-only.

## Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the sFlow Agent.

```
B5(rw)->show sflow interface
loopback 1 192.168.10.1
```

# clear sflow interface

Use this command to clear the management interface used by the sFlow Agent back to the default of the Host VLAN.

## Syntax

```
clear sflow interface
```

## Parameters

None.

## Defaults

None.

## Mode

Switch command, read-write.

## Example

This command returns the management interface used by the sFlow Agent back to the default of the Host VLAN.

```
B5(rw)->show sflow interface
vlan 100 192.168.10.1
B5(rw)->clear sflow interface
B5(rw)->
```

---

## show sflow agent

Use this command to display information about the sFlow Agent.

### Syntax

```
show sflow agent
```

### Parameters

None.

### Defaults

None.

### Mode

Switch command, read-only.

### Example

This example displays the output of this command.

```
B5(rw)->show sflow agent
```

```
sFlow Version          1.3;Enterasys Networks.;06.41.01.0017
IP Address             192.168.0.100
```





## Policy and Authentication Capacities

This appendix lists the policy and authentication capacities of the Enterasys B5 as of the date this document was published. Please refer to the Release Notes for your firmware version for the latest capacity information.

### Policy Capacities

Refer to the “Configuring Policy” Feature Guide for an in-depth discussion of Policy configuration. This Feature Guide is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads/>

**Table A-1 Policy Capacities**

Feature	Capacity
Maximum policy roles (profiles) per system	15
Maximum number of unique rules per system	1536
Maximum number of ether type rules	256
Maximum number of MAC rules	256
Maximum number of Layer 3/4 rules	1024
Maximum number of rules per single role	250
Maximum number of masks	No limit
CoS rate limiting (IRL) support	Yes
Priority-based rate limiting	No
Rule-based rate limiting	No
Role-based rate limiting	Yes
Fixed rule precedence	Yes
Supported rule types	
ether type (numuser = 1) <sup>1, 2</sup>	vlan/cos/drop/fwd (max 7 vlan rules per profile)
mac dest/mac source	cos/drop/fwd
ip protocol <sup>1</sup>	cos/drop/fwd
ip dest socket/ip source socket	cos/drop/fwd
ip tos <sup>1</sup>	cos/drop/fwd
tcp dest port/ tcp source port	cos/drop/fwd

**Table A-1 Policy Capacities (Continued)**

Feature	Capacity
udp dest port/udp source port	cos/drop/fwd
icmp type <sup>1</sup>	No

1. These rules cannot be masked.
2. Ether type to vlan rules require that multiauth numusers = 1 (that is, only one authenticated user is allowed per port).

## Authentication Capacities

Refer to the “Configuring User Authentication” Feature Guide for an in-depth discussion of authentication configuration. This Feature Guide is located on the Enterasys Networks web site:

<https://extranet.enterasys.com/downloads/>

**Table A-2 Authentication Capacities**

Authentication Feature	Capacity
IEEE 802.1x (dot1x) authentication	Supported
MAC-based authentication	Supported
Port Web Authentication (PWA)	Supported
RFC 3580 dynamic VLAN assignment based on authentication response	Supported, for 802.1x, MAC-based, and PWA authentication methods
Multi-user authentication maximum users per port when policy mactable response is:	
policy mode	4
both, hybrid mode	4
tunnel mode	4
User + IP phone (Configured with a policy admin rule) Multiauth numusers set to 2 or greater	Supported

## Numerics

802.1D 9-1  
802.1p 11-16, 12-1  
802.1Q 10-1  
802.1s 9-2  
802.1w 9-1  
802.1x 22-8, 22-23

## A

Access Groups 22-86  
Access Lists 22-83 to 22-84  
Addresses  
    MAC, adding entries to routing table 19-5  
Advertised Ability 7-16  
AES encryption protocol 8-10  
Alias  
    node 14-39  
ARP  
    dynamic inspection 17-16  
    entries, adding in routing mode 19-9  
    proxy, enabling 19-10  
    timeout 19-11  
Authentication  
    EAPOL 22-23  
    MAC 22-25  
    Port web 22-68  
    RADIUS server 22-8, 22-11  
    SSH 22-81  
Auto-negotiation 7-16

## B

banner motd 3-25  
Baud Rate 3-31  
Broadcast  
    settings for IP routing 19-12  
    suppression, enabling on ports 7-35

## C

CDP Discovery Protocol 6-1  
CIDR 20-4  
Cisco Discovery Protocol 6-7  
Class of Service 11-7, 11-11, 11-16 to 11-22, 12-1  
Class of Service (CoS) 11-16  
Classification Policies 11-1  
Clearing NVRAM 3-50  
CLI  
    closing 3-48  
    scrolling screens 1-9  
    starting 1-6  
Command History Buffer 14-14, 14-15  
Command Line Interface. See also CLI  
Configuration  
    clearing switch parameters 3-50  
    modes for router operation 18-2  
Configuration Files

    copying 3-44  
    deleting 3-45  
    displaying 3-43  
    executing 3-44  
    show running config 3-45  
    show running-config 19-7  
Contexts (SNMP) 8-3  
Copying Configuration or Image Files 3-44

## CoS

flood control 11-18  
rate limiting 11-16

## Cost

Spanning Tree port 9-40

## D

Defaults  
    CLI behavior, described 1-8  
    factory installed 1-2  
DES encryption protocol 8-10  
DHCP server, configuring 16-1  
DHCP snooping  
    basic configuration 17-3  
    database 17-2  
    overview 17-1  
DHCP/BOOTP Relay 16-1  
Dynamic ARP inspection  
    basic configuration 17-18  
    overview 17-16  
Dynamic policy profile  
    assignment 22-3

## E

EAP pass-through 22-2, 22-18  
EAPOL 22-23  
encryption protocol  
    SNMP 8-9

## F

Flood control, via CoS 11-18  
Flow Control 7-22  
Forbidden VLAN port 10-14

## G

Getting help xxxii  
GVRP  
    enabling and disabling 10-23  
    purpose of 10-20  
    timer 10-25

## H

Hardware  
    show system 3-15, 3-26  
Help  
    keyword lookups 1-8  
Host VLAN 10-18  
hybrid authentication, about 22-52

## I

ICMP 14-16  
IGMP 13-1  
    enabling and disabling 13-2, 13-10  
Image File  
    copying 3-44  
    downloading 3-31  
Ingress Filtering 10-8, 10-11  
Interface Configuration Mode 19-2  
Interface(s)  
    configuring settings for IP 19-1  
    RIP passive 20-5  
    RIP receive 20-6  
    RIP send 20-8  
IP  
    access lists 22-83 to 22-84  
    address, setting for a routing interface 19-5  
    routes, adding in router mode 19-16  
    routes, managing in switch mode 14-19  
IPv6  
    addresses, setting 21-3  
    default router, setting 21-5  
    gateway, setting 21-5  
    management 21-1  
    Neighbor Discovery Protocol  
        displaying cache 21-7  
IRDP 20-11

## J

Jumbo Frame Support 7-14

## K

Keyword Lookups 1-8

## L

Line Editing Commands 1-10  
Link Layer Discovery Protocol (LLDP)  
    configuring 6-13  
LLDP  
    configuring 6-13  
LLDP-MED  
    configuring 6-14  
Lockout  
    set system 3-7  
Logging 14-1  
Login  
    administratively configured 1-7  
    default 1-7  
    setting accounts 3-2  
    via Telnet 1-6

## M

MAC Addresses  
    displaying 14-22  
MAC Authentication 22-25

- MAC Locking [22-57](#)
  - maximum static entries [22-63](#)
  - static [22-63](#)
- Management VLAN [10-2](#)
- maptable response [22-52](#)
- modd [3-25](#)
- Multicast Filtering [13-1](#), [13-2](#)
- Multiple Spanning Tree Protocol (MSTP) [9-2](#)

## N

- Name
  - setting for a VLAN [10-6](#)
  - setting for the system [3-27](#)
- Network Management
  - addresses and routes [14-19](#)
  - monitoring switch events and status [14-14](#)
- Node Alias [14-39](#)
- NVRAM
  - clearing [3-50](#)

## P

- Password
  - aging [3-6](#)
  - history [3-6](#), [3-7](#)
  - set new [3-5](#)
  - setting the login [3-5](#)
- Ping [14-16](#), [19-17](#)
- Policy Management
  - assigning ports [11-14](#)
  - classifying to a VLAN or Class of Service [11-7](#), [11-11](#)
  - dynamic assignment of profiles [22-3](#)
  - profiles [11-2](#), [11-16](#)
- policy maptable response,
  - about [22-52](#)
- Port Mirroring [7-38](#)
- Port Priority
  - configuring [12-2](#)
- Port String
  - syntax used in the CLI [7-1](#)
- Port Trunking [7-44](#)
- Port web authentication
  - configuring [22-68](#)
- Port(s)
  - alias [7-9](#)
  - assignment scheme [7-1](#)
  - auto-negotiation and advertised ability [7-16](#)
  - broadcast suppression [7-35](#)
  - counters, reviewing statistics [7-4](#)
  - duplex mode, setting [7-11](#)
  - flow control [7-22](#)
  - link flap
    - about [7-24](#)
    - configuration defaults [7-26](#)
    - configuring [7-25](#)
  - link traps, configuring [7-24](#)
  - MAC lock [22-60](#)
  - priority, configuring [12-2](#)

- speed, setting [7-11](#)
- status, reviewing [7-2](#)
- Power over Ethernet (PoE),
  - configuring [4-1](#)
- Priority to Transmit Queue Mapping [12-4](#)
- Prompt
  - in router mode [18-2](#)
  - set [3-24](#)
- PWA [22-68](#)

## R

- RADIUS [22-6](#)
  - realm [22-8](#)
- RADIUS Filter-ID [22-3](#)
  - attribute formats [22-3](#)
- RADIUS server [22-8](#), [22-11](#)
- Rapid Spanning Tree Protocol (RSTP) [9-1](#)
- Rate limiting, via CoS [11-16](#)
- Redistribute [20-6](#)
- remote port mirroring
  - configuring [7-42](#)
- Reset [3-50](#)
- RFC 3580 [22-49](#)
- RIP
  - CIDR [20-4](#)
  - configuration mode, enabling [20-2](#)
  - configuration tasks [20-1](#)
  - passive interface [20-5](#)
  - redistribute [20-6](#)
- Router Mode(s)
  - enabling [18-2](#)
- Routing Interfaces
  - configuring [19-2](#)
- Routing Protocol Configuration
  - IRDP [20-11](#)
  - RIP [20-1](#)

## S

- Scrolling Screens [1-9](#)
- Secure Shell (SSH) [22-80](#)
  - enabling [22-80](#)
  - regenerating new keys [22-81](#)
- Security
  - methods, overview of [22-1](#)
- Serial Port
  - downloading upgrades via [3-31](#)
- sFlow configuration [24-1](#)
- show system utilization cpu [3-16](#)
- SNMP
  - access rights [8-15](#)
  - accessing in router mode [8-3](#)
  - enabling on the switch [8-18](#)
  - encryption protocols [8-10](#)
  - MIB views [8-19](#)
  - notification parameters [8-29](#)
  - notify filters [8-29](#)
  - security models and levels [8-2](#)
  - statistics [8-3](#)
  - target addresses [8-26](#)

- target parameters [8-23](#)
- trap configuration example [8-36](#)
- users, groups and communities [8-8](#)

- SNTP [14-29](#)

- Spanning Tree [9-2](#)
  - backup root [9-21](#), [9-22](#)
  - bridge parameters [9-3](#)
  - features [9-2](#)
  - port parameters [9-34](#)
  - Rapid Spanning Tree Protocol (RSTP) [9-1](#)

- Split Horizon [20-4](#)

- SSL WebView [3-53](#)

- stacks
  - installing units [2-2](#)
  - operation [2-1](#)
  - virtual switch configuration [2-3](#)

- Syslog [14-1](#)

- System Information
  - displaying basic [3-13](#)
  - setting basic [3-9](#)

## T

- TACACS+ configuration [23-1](#)
- Technical Support [xxxii](#)
- Telnet
  - disconnecting [14-17](#)
  - enabling in switch mode [3-37](#)
- Terminal Settings [3-28](#)
- TFTP
  - downloading firmware upgrades via [3-31](#)
- Timeout
  - ARP [19-11](#)
  - CLI, system [3-30](#)
  - RADIUS [22-8](#)
- Traceroute
  - in router mode [19-17](#)
- Trap
  - SNMP configuration example [8-36](#)
- Tunnel Attributes
  - RFC 3580 RADIUS attributes [22-49](#)

## U

- User Accounts
  - default [1-7](#)
  - setting [3-2](#)

## V

- Version
  - RIP receive [20-8](#)
  - RIP send [20-8](#)
- Version Information [3-26](#)
- virtual switch, configuring [2-3](#)
- VLANs
  - assigning ingress filtering [10-11](#)
  - assigning port VLAN IDs [10-8](#)
  - authentication [22-49](#), [22-51](#)
  - classifying to [11-7](#), [11-11](#)
  - creating static [10-5](#)
  - dynamic egress [10-17](#)



egress lists [10-13](#), [22-50](#)  
enabling GVRP [10-20](#)  
forbidden ports [10-14](#)  
host, setting [10-18](#)  
ingress filtering [10-8](#)  
naming [10-6](#)  
RADIUS [22-49](#)  
secure management, creating [10-2](#)

## **W**

WebView [1-2](#), [3-51](#)  
WebView SSL [3-53](#)

