HP Switch Software
Access Security Guide

2910 switches

Software version W.15.07
November 2011
This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number
5008-2871
November 2011

Applicable Products
HP 2910al-24G Switch J9145A
HP 2910al-48G Switch J9147A
HP 2910al-24G-PoE+ Switch J9146A
HP 2910al-48G-PoE+ Switch J9148A

Trademark Credits
Microsoft, Windows, and Microsoft Windows NT are U.S. registered trademarks of Microsoft Corporation.

Software Credits and Notices
SSH on HP switches is based on the OpenSSH software toolkit. This product includes software developed by the OpenSSH Project for use in the OpenSSH Toolkit. For more information on OpenSSH, visit www.openssh.com.

SSL on HP switches is based on the OpenSSL software toolkit. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information on OpenSSL, visit www.openssl.org.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Portions of the software on HP switches are based on the lightweight TCP/IP (lwIP) software toolkit by Adam Dunkels, and are covered by the following notices.

Copyright © 2001-2003 Swedish Institute of Computer Science. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

SOFTWARE END USER LICENSE AGREEMENT AND HARDWARE LIMITED WARRANTY

For the software end user license agreement and the hardware limited warranty information for HP Networking products, visit www.hp.com/networking/support.
Contents

Product Documentation

About Your Switch Manual Set ........................................ xxi
  Electronic Publications ........................................... xxi
Software Feature Index ........................................... xxii

1 Security Overview

Introduction .............................................................. 1-1
  About This Guide ............................................... 1-1
  For More Information ........................................... 1-1
Access Security Features ........................................... 1-2
Network Security Features ........................................... 1-6
Getting Started with Access Security .............................. 1-9
  Physical Security .................................................. 1-9
    CLI: Management Interface Wizard ............................. 1-11
    WebAgent: Management Interface Wizard ...................... 1-12
    SNMP Security Guidelines ...................................... 1-13
Precedence of Security Options ................................... 1-15
  Precedence of Port-Based Security Options .................... 1-15
  Precedence of Client-Based Authentication:
    Dynamic Configuration Arbiter ................................. 1-15
    HP E-Network Immunity Manager ............................... 1-16
    Arbitrating Client-Specific Attributes ....................... 1-17
  HP PMC Identity Driven Manager (IDM) ......................... 1-20

2 Configuring Username and Password Security

Overview ............................................................... 2-1
Configuring Local Password Security .............................. 2-4
  Menu: Setting Passwords ......................................... 2-4
  CLI: Setting Passwords and Usernames .......................... 2-6
WebAgent: Setting Passwords and Usernames 2-9

**Saving Security Credentials in a Config File** 2-10
Benefits of Saving Security Credentials 2-10
Enabling the Storage and Display of Security Credentials 2-11
Security Settings that Can Be Saved 2-12
Executing Include-Credentials or Include-Credentials Store-in-Config 2-12
No Include-credentials store-in-config Option 2-13
Local Manager and Operator Passwords 2-14
Password Command Options 2-15
SNMP Security Credentials 2-15
TACACS+ Encryption Key Authentication 2-16
RADIUS Shared-Secret Key Authentication 2-17
Include-Credentials Radius-Tacacs-Only Option 2-18
SSH Client Public-Key Authentication 2-19
Displaying the Status of Include-Credentials on the Switch 2-22
Storage States When Using Include-Credentials 2-23
Operating Notes 2-24
Restrictions 2-26

Encrypting Credentials in the Configuration File 2-27
Overview 2-27
Enabling Encrypt-Credentials 2-28
Displaying the State of Encrypt-Credentials 2-29
Affected Commands 2-30
Important Operating Notes 2-31
Interaction with Include-Credentials Settings 2-31

Front-Panel Security 2-32
When Security Is Important 2-32
Front-Panel Button Functions 2-33
Clear Button 2-33
Reset Button 2-33
Restoring the Factory Default Configuration 2-33
Configuring Front-Panel Security 2-35
Disabling the Clear Password Function of the Clear Button 2-38
Re-Enabling the Clear Button and Setting or Changing the “Reset-On-Clear” Operation .................. 2-39
Changing the Operation of the Reset+Clear Combination .... 2-40

Password Recovery ..................................................... 2-42
Disabling or Re-Enabling the Password Recovery Process .... 2-42
Password Recovery Process ............................. 2-44

3 Web and MAC Authentication

Overview ................................................................. 3-1
Web Authentication .................................................. 3-2
MAC Authentication ............................................... 3-2
Concurrent Web and MAC Authentication .................. 3-3
Authorized and Unauthorized Client VLANs ..................... 3-3
RADIUS-Based Authentication .................................. 3-4
Wireless Clients .................................................. 3-4

How Web and MAC Authentication Operate .................. 3-5
Web-based Authentication ........................................ 3-5
MAC-based Authentication ..................................... 3-7

Terminology ............................................................ 3-9

Operating Rules and Notes ........................................ 3-10

Setup Procedure for Web/MAC Authentication ........... 3-12
Before You Configure Web/MAC Authentication ........... 3-12
Configuring the RADIUS Server To Support MAC Authentication .. 3-15
Configuring the Switch To Access a RADIUS Server ........... 3-15

Configuring Web Authentication .............................. 3-18
Overview ............................................................. 3-18
Configuration Commands for Web Authentication .......... 3-19
Show Commands for Web Authentication ....................... 3-25

Configuring MAC Authentication on the Switch ........... 3-31
Overview ............................................................. 3-31
Configuration Commands for MAC Authentication ............ 3-32
Configuring the Global MAC Authentication Password .......... 3-32
Configuring a MAC-based Address Format .................. 3-34
Configuring Custom Messages .............................. 3-37
4 TACACS+ Authentication

Overview ................................................. 4-1
Terminology Used in TACACS Applications: .............. 4-2
General System Requirements .............................. 4-4
General Authentication Setup Procedure .................. 4-4
Configuring TACACS+ on the Switch ...................... 4-7
  Before You Begin ........................................ 4-7
  CLI Commands Described in this Section ............... 4-8
  Viewing the Switch’s Current Authentication Configuration .... 4-8
  Viewing the Switch’s Current TACACS+ Server Contact Configuration .... 4-9
  Configuring the Switch’s Authentication Methods ........... 4-10
    Using the Privilege-Mode Option for Login ................ 4-10
    Authentication Parameters ............................... 4-12
  Configuring the TACACS+ Server for Single Login .......... 4-12
  Configuring the Switch’s TACACS+ Server Access ........... 4-17
How Authentication Operates ................................ 4-23
  General Authentication Process Using a TACACS+ Server .... 4-23
  Local Authentication Process ............................. 4-24
  Using the Encryption Key ................................ 4-25
    General Operation ...................................... 4-25
    Encryption Options in the Switch ....................... 4-26
Controlling WebAgent Access When
Using TACACS+ Authentication .............................. 4-27
Messages Related to TACACS+ Operation .................... 4-28
Operating Notes .......................................... 4-29
5 RADIUS Authentication, Authorization, and Accounting

Overview ................................................................. 5-1
  Authentication Services ........................................... 5-1
  Accounting Services .............................................. 5-2
  RADIUS-Administered CoS and Rate-Limiting .............. 5-2
  RADIUS-Administered Commands Authorization .............. 5-2
  SNMP Access to the Switch's Authentication Configuration MIB 5-3

Terminology ............................................................ 5-4

Switch Operating Rules for RADIUS .............................. 5-5

General RADIUS Setup Procedure ................................. 5-6

Configuring the Switch for RADIUS Authentication ........... 5-7
  Outline of the Steps for Configuring RADIUS Authentication 5-8
  1. Configure Authentication for the Access Methods
  2. Enable the (Optional) Access Privilege Option ........... 5-12
  3. Configure the Switch To Access a RADIUS Server ....... 5-14
  4. Configure the Switch's Global RADIUS Parameters ....... 5-17
  Using Multiple RADIUS Server Groups ....................... 5-22
    Commands ...................................................... 5-22
    Enhanced Commands ........................................ 5-23
    Displaying the RADIUS Server Group Information ........ 5-25

Using SNMP To View and Configure
Switch Authentication Features ................................. 5-27
  Changing and Viewing the SNMP Access Configuration .... 5-28

Local Authentication Process .................................. 5-31

Controlling WebAgent Access .................................. 5-32

Commands Authorization ......................................... 5-33
  Enabling Authorization ........................................ 5-34
  Displaying Authorization Information ....................... 5-35
  Configuring Commands Authorization on a RADIUS Server 5-35
    Using Vendor Specific Attributes (VSAs) ................ 5-35
  Example Configuration on Cisco Secure ACS for MS Windows 5-38
  Example Configuration Using FreeRADIUS ................... 5-41

VLAN Assignment in an Authentication Session ................ 5-42
Tagged and Untagged VLAN Attributes ........................................ 5-42
Additional RADIUS Attributes ................................................. 5-43
MAC-Based VLANs ............................................................... 5-46
Accounting Services .............................................................. 5-47
  Accounting Service Types .................................................. 5-47
  Operating Rules for RADIUS Accounting ................................. 5-48
  Acct-Session-ID Options in a Management Session ....................... 5-49
    Unique Acct-Session-ID Operation ................................. 5-49
    Common Acct-Session-ID Operation ............................ 5-51
Configuring RADIUS Accounting ................................................ 5-52
Steps for Configuring RADIUS Accounting ................................. 5-52
  1. Configure the Switch To Access a RADIUS Server ............... 5-53
  2. (Optional) Reconfigure the Acct-Session-ID Operation .................. 5-55
  3. Configure Accounting Types and the Controls for Sending Reports to the RADIUS Server ................. 5-56
  4. (Optional) Configure Session Blocking and Interim Updating Options ........................................ 5-61
Viewing RADIUS Statistics ...................................................... 5-62
  General RADIUS Statistics .............................................. 5-62
  RADIUS Authentication Statistics .................................. 5-64
  RADIUS Accounting Statistics ................................... 5-66
Changing RADIUS-Server Access Order ....................................... 5-67
Creating Local Privilege Levels ............................................... 5-70
  Configuring Groups for Local Authorization ......................... 5-71
  Configuring a Local User for a Group ............................... 5-72
  Displaying Command Authorization Information ...................... 5-74
Dynamic Removal of Authentication Limits .................................. 5-75
  Overview ........................................................................ 5-75
  Configuring the RADIUS VSAs ...................................... 5-75
  Displaying the Port-access Information ............................ 5-77
  Operating Notes ......................................................... 5-78
Messages Related to RADIUS Operation ..................................... 5-79
6 Configuring RADIUS Server Support for Switch Services

Overview ......................................................... 6-1

RADIUS Server Configuration for Per-Port CoS (802.1p Priority) and Rate-Limiting ........ 6-2
  Applied Rates for RADIUS-Assigned Rate Limits .................. 6-3
  Viewing the Currently Active Per-Port CoS and Rate-Limiting Configuration Specified by a RADIUS Server ........ 6-4

Configuring and Using RADIUS-Assigned Access Control Lists . . . 6-7
  Introduction ...................................................... 6-7
  Terminology ....................................................... 6-7
  Overview of RADIUS-Assigned, Dynamic ACLs ...................... 6-10
  Contrasting Dynamic (RADIUS-Assigned) and Static ACLs ........... 6-11
  How a RADIUS Server Applies a RADIUS-Assigned ACL to a Switch Port ......................... 6-12
  General ACL Features, Planning, and Configuration ................. 6-13
  The Packet-filtering Process ................................... 6-14
  Operating Rules for RADIUS-Assigned ACLs ........................ 6-15
  Configuring an ACL in a RADIUS Server .......................... 6-15
    Nas-Filter-Rule-Options ...................................... 6-16
  Configuring ACE Syntax in RADIUS Servers ........................ 6-17
    Example Using the Standard Attribute (92) In an IPv4 ACL ...... 6-18
    Example of Configuring a RADIUS-assigned ACL Using the FreeRADIUS Application .................... 6-19
    Format Details for ACEs Configured in a RADIUS-Assigned ACL .......................... 6-21
    Configuration Notes ........................................... 6-22
  Configuring the Switch To Support RADIUS-Assigned ACLs ........... 6-22
  Displaying the Current RADIUS-Assigned ACL Activity on the Switch ................................... 6-24
  ICMP Type Numbers and Keywords .................................. 6-26
  Event Log Messages ............................................. 6-27
7 Configuring Secure Shell (SSH)

Overview ........................................ 7-1
Terminology ..................................... 7-3
Prerequisite for Using SSH .................... 7-4
Public Key Formats ............................. 7-4
Steps for Configuring and Using SSH for Switch and Client Authentication .... 7-5
General Operating Rules and Notes .......... 7-7

Configuring the Switch for SSH Operation ........ 7-8
1. Assigning a Local Login (Operator) and Enable (Manager) Password .......... 7-9
2. Generating the Switch’s Public and Private Key Pair .................. 7-9
   Configuring Key Lengths ........................ 7-12
3. Providing the Switch’s Public Key to Clients .................... 7-13
4. Enabling SSH on the Switch and Anticipating SSH Client Contact Behavior ........ 7-15
5. Configuring the Switch for SSH Authentication .................. 7-20
6. Use an SSH Client To Access the Switch .................. 7-23

Further Information on SSH Client Public-Key Authentication .......... 7-24

SSH Client and Secure Sessions ................ 7-29
Opening a Secure Session to an HP Switch .......... 7-30
Operating Notes .................................. 7-31
Copying Client Key Files ...................... 7-31
Copying the SSH-Client-Known-Hosts File .......... 7-33
   Replacing or Appending the SSH-Client-Known-Hosts File .................. 7-33
   Copying the SSH Client Known Hosts File to Another Location .......... 7-34
Copying the Host Public Key .................. 7-35
Removing the SSH Client Key Pair .............. 7-35
Removing the SSH Client Known Hosts File ........ 7-36
8 Configuring Secure Socket Layer (SSL)

Overview ................................................. 8-1
Terminology .............................................. 8-3
Prerequisite for Using SSL .............................. 8-4
Steps for Configuring and Using SSL for Switch and Client Authentication .......... 8-4
General Operating Rules and Notes .................. 8-5
Configuring the Switch for SSL Operation .......... 8-6
1. Assigning a Local Login (Operator) and Enabling (Manager) Password .......... 8-6
2. Generating the Switch’s Server Host Certificate ........ 8-6
   To Generate or Erase the Switch’s Server Certificate with the CLI ............. 8-7
   Comments on Certificate Fields .................................. 8-8
   Generate a Self-Signed Host Certificate with the WebAgent .................. 8-12
   Generate a CA-Signed server host certificate with the WebAgent ............ 8-13
3. Enabling SSL on the Switch and Anticipating SSL Browser Contact Behavior .......... 8-15
   Using the CLI Interface to Enable SSL ................................ 8-16
   Using the WebAgent to Enable SSL ................................ 8-16
Common Errors in SSL Setup ............................ 8-18

9 IPv4 Access Control Lists (ACLs)

Introduction .............................................. 9-1
Overview of Options for Applying IPv4 ACLs on the Switch ........ 9-3
Static ACLS .............................................. 9-3
Dynamic Port ACLs ...................................... 9-3
Terminology .............................................. 9-7
10 Configuring Advanced Threat Protection

Introduction ......................................................... 10-1

DHCP Snooping ..................................................... 10-3
Overview ................................................................. 10-4
Enabling DHCP Snooping ........................................ 10-5
Enabling DHCP Snooping on VLANS ......................... 10-7
Configuring DHCP Snooping Trusted Ports .................. 10-7
Configuring Authorized Server Addresses ................... 10-8
Using DHCP Snooping with Option 82 ....................... 10-9
   Changing the Remote-id from a MAC to an IP Address ... 10-11
   Disabling the MAC Address Check .......................... 10-11
   The DHCP Binding Database ............................... 10-12
   Operational Notes ............................................ 10-13
   Log Messages .................................................. 10-14

Dynamic ARP Protection ........................................... 10-16
Introduction .......................................................... 10-16
Enabling Dynamic ARP Protection .............................. 10-18
Configuring Trusted Ports ........................................ 10-18
Adding an IP-to-MAC Binding to the DHCP Database ........ 10-20
Configuring Additional Validation Checks on ARP Packets .. 10-21
Verifying the Configuration of Dynamic ARP Protection .... 10-21
Displaying ARP Packet Statistics .............................. 10-22
Monitoring Dynamic ARP Protection ............................ 10-23

Dynamic IP Lockdown ............................................... 10-23
Protection Against IP Source Address Spoofing ............... 10-24
Prerequisite: DHCP Snooping .................................... 10-24
Filtering IP and MAC Addresses Per-Port and Per-VLAN .... 10-25
Enabling Dynamic IP Lockdown ................................. 10-26
Operating Notes ..................................................... 10-26
Adding an IP-to-MAC Binding to the DHCP Binding Database ... 10-28
   Potential Issues with Bindings .............................. 10-28
11 Traffic/Security Filters and Monitors

Overview .................................................. 11-1
Introduction .............................................. 11-2
  Filter Limits .......................................... 11-2
  Using Port Trunks with Filters ...................... 11-2

Filter Types and Operation ............................... 11-3
  Source-Port Filters ................................. 11-3
     Operating Rules for Source-Port Filters .......... 11-3
     Example ........................................... 11-4
  Named Source-Port Filters ......................... 11-5
     Operating Rules for Named Source-Port Filters ... 11-5
     Defining and Configuring Named Source-Port Filters 11-6
     Viewing a Named Source-Port Filter .............. 11-8
     Using Named Source-Port Filters ................. 11-8
  Static Multicast Filters ............................. 11-14
  Protocol Filters ..................................... 11-15

Configuring Traffic/Security Filters .................... 11-16
  Configuring a Source-Port Traffic Filter .......... 11-17
     Example of Creating a Source-Port Filter ........ 11-17
     Configuring a Filter on a Port Trunk .......... 11-18
  Editing a Source-Port Filter ....................... 11-19
  Configuring a Multicast or Protocol Traffic Filter 11-20
12 Configuring Port-Based and User-Based Access Control (802.1X)

Overview ................................................. 12-1
   Why Use Port-Based or User-Based Access Control? .... 12-1
   General Features ..................................... 12-1
   User Authentication Methods .......................... 12-2
      802.1X User-Based Access Control .......... 12-3
      802.1X Port-Based Access Control .......... 12-3
   Alternative To Using a RADIUS Server ............ 12-4
   Accounting ........................................... 12-4

Terminology ............................................. 12-5

General 802.1X Authenticator Operation .................... 12-8
   Example of the Authentication Process .......... 12-8
   VLAN Membership Priority ....................... 12-9

General Operating Rules and Notes ........................ 12-11

General Setup Procedure for 802.1X Access Control ........ 12-13
   Do These Steps Before You Configure 802.1X Operation .... 12-13
   Overview: Configuring 802.1X Authentication on the Switch ........ 12-16

Configuring Switch Ports as 802.1X Authenticators ........ 12-17
   1. Enable 802.1X Authentication on Selected Ports .......... 12-18
      A. Enable the Selected Ports as Authenticators and Enable the (Default) Port-Based Authentication .......... 12-18
      B. Specify User-Based Authentication or Return to Port-Based Authentication .................... 12-19
         Example: Configuring User-Based 802.1X Authentication .......... 12-20
         Example: Configuring Port-Based 802.1X Authentication .......... 12-20
   2. Reconfigure Settings for Port-Access .................. 12-21
   3. Configure the 802.1X Authentication Method ............ 12-24
   4. Enter the RADIUS Host IP Address(es) .................. 12-26
   5. Enable 802.1X Authentication on the Switch ............ 12-27
   6. Optional: Reset Authenticator Operation ............... 12-27
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Optional: Configure 802.1X Controlled Directions</td>
<td>12-27</td>
</tr>
<tr>
<td>Wake-on-LAN Traffic</td>
<td>12-28</td>
</tr>
<tr>
<td>Operating Notes</td>
<td>12-29</td>
</tr>
<tr>
<td>Example: Configuring 802.1X Controlled Directions</td>
<td>12-29</td>
</tr>
<tr>
<td>Unauthenticated VLAN Access (Guest VLAN Access)</td>
<td>12-29</td>
</tr>
<tr>
<td>Characteristics of Mixed Port Access Mode</td>
<td>12-30</td>
</tr>
<tr>
<td>Configuring Mixed Port Access Mode</td>
<td>12-31</td>
</tr>
<tr>
<td>802.1X Open VLAN Mode</td>
<td>12-32</td>
</tr>
<tr>
<td>Introduction</td>
<td>12-32</td>
</tr>
<tr>
<td>VLAN Membership Priorities</td>
<td>12-33</td>
</tr>
<tr>
<td>Use Models for 802.1X Open VLAN Modes</td>
<td>12-34</td>
</tr>
<tr>
<td>Operating Rules for Authorized-Client and Unauthorized-Client VLANS</td>
<td>12-39</td>
</tr>
<tr>
<td>Setting Up and Configuring 802.1X Open VLAN Mode</td>
<td>12-42</td>
</tr>
<tr>
<td>802.1X Open VLAN Operating Notes</td>
<td>12-47</td>
</tr>
<tr>
<td>Option For Authenticator Ports: Configure Port-Security</td>
<td>12-48</td>
</tr>
<tr>
<td>To Allow Only 802.1X-Authenticated Devices</td>
<td>12-49</td>
</tr>
<tr>
<td>Configuring Switch Ports To Operate As</td>
<td>12-50</td>
</tr>
<tr>
<td>Supplicants for 802.1X Connections to Other Switches</td>
<td>12-50</td>
</tr>
<tr>
<td>Example</td>
<td>12-50</td>
</tr>
<tr>
<td>Supplicant Port Configuration</td>
<td>12-52</td>
</tr>
<tr>
<td>Displaying 802.1X Configuration, Statistics, and Counters</td>
<td>12-55</td>
</tr>
<tr>
<td>Show Commands for Port-Access Authenticator</td>
<td>12-55</td>
</tr>
<tr>
<td>Viewing 802.1X Open VLAN Mode Status</td>
<td>12-64</td>
</tr>
<tr>
<td>Show Commands for Port-Access Supplicant</td>
<td>12-68</td>
</tr>
<tr>
<td>How RADIUS/802.1X Authentication Affects VLAN Operation</td>
<td>12-69</td>
</tr>
<tr>
<td>VLAN Assignment on a Port</td>
<td>12-70</td>
</tr>
<tr>
<td>Operating Notes</td>
<td>12-70</td>
</tr>
<tr>
<td>Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session</td>
<td>12-72</td>
</tr>
<tr>
<td>Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions</td>
<td>12-76</td>
</tr>
<tr>
<td>Messages Related to 802.1X Operation</td>
<td>12-78</td>
</tr>
</tbody>
</table>
# 13 Configuring and Monitoring Port Security

- **Overview** .......................................................... 13-1

- **Port Security** ....................................................... 13-2
  - Basic Operation .................................................. 13-2
  - Eavesdrop Prevention ........................................... 13-3
    - Disabling Eavesdrop Prevention ............................ 13-3
    - Feature Interactions When Eavesdrop Prevention is Disabled ........ 13-4
  - MIB Support ..................................................... 13-5
  - Blocking Unauthorized Traffic ............................... 13-5
  - Trunk Group Exclusion ......................................... 13-6
  - Planning Port Security ......................................... 13-7
  - Port Security Command Options and Operation ............. 13-8
    - Port Security Display Options ............................ 13-8
  - Configuring Port Security ..................................... 13-12
  - Retention of Static Addresses ............................... 13-17

- **Clear MAC Address Table** ..................................... 13-22
  - Configuring Clearing of Learned MAC Addresses ............. 13-23

- **MAC Lockdown** ................................................... 13-24
  - Differences Between MAC Lockdown and Port Security ......... 13-26
  - MAC Lockdown Operating Notes ................................ 13-27
  - Deploying MAC Lockdown ....................................... 13-28

- **MAC Lockout** ..................................................... 13-32

- **Port Security and MAC Lockout** .............................. 13-34

- **Reading Intrusion Alerts and Resetting Alert Flags** ........ 13-35
  - Notice of Security Violations ............................... 13-35
  - How the Intrusion Log Operates ............................ 13-36
  - Keeping the Intrusion Log Current by Resetting Alert Flags .... 13-36
    - Menu: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags ................. 13-37
    - CLI: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags ................... 13-39
  - Using the Event Log To Find Intrusion Alerts ............... 13-41

- **Operating Notes for Port Security** .......................... 13-42
14 Using Authorized IP Managers

Overview ................................................................. 14-1
Options ................................................................. 14-2
Access Levels .......................................................... 14-2

Defining Authorized Management Stations ......................... 14-3
Overview of IP Mask Operation ..................................... 14-3
Menu: Viewing and Configuring IP Authorized Managers ....... 14-4
CLI: Viewing and Configuring Authorized IP Managers ........ 14-5
Listing the Switch’s Current Authorized IP Manager(s) ......... 14-5
Configuring IP Authorized Managers for the Switch .......... 14-6

WebAgent: Configuring IP Authorized Managers ................. 14-8
Web Proxy Servers ............................................... 14-9
How to Eliminate the Web Proxy Server ......................... 14-9
Using a Web Proxy Server to Access the WebAgent ........ 14-9

Building IP Masks ...................................................... 14-10
Configuring One Station Per Authorized Manager IP Entry .... 14-10
Configuring Multiple Stations Per Authorized Manager IP Entry . 14-10
Additional Examples for Authorizing Multiple Stations .... 14-12

Operating Notes ....................................................... 14-13

15 Key Management System

Overview ................................................................. 15-1
Terminology .......................................................... 15-2

Configuring Key Chain Management ................................ 15-2
Creating and Deleting Key Chain Entries .......................... 15-3
Assigning a Time-Independent Key to a Chain ................ 15-4
Assigning Time-Dependent Keys to a Chain ................... 15-5

Index
Product Documentation

About Your Switch Manual Set

Note

For the latest version of all HP switch documentation, including Release Notes covering recently added features, please visit the HP Networking web site at www.hp.com/Networking/support.

Electronic Publications

The latest version of each of the publications listed below is available in PDF format on the HP Networking web site, as described in the Note at the top of this page.

- **Installation and Getting Started Guide**—Explains how to prepare for and perform the physical installation and connect the switch to your network.
- **Basic Operation Guide**—Describes how to use the switch interfaces and introduces basic operations.
- **Management and Configuration Guide**—Describes how to configure, manage, and monitor basic switch operation.
- **Advanced Traffic Management Guide**—Explains how to configure traffic management features such as VLANs, MSTP, and QoS.
- **Multicast and Routing Guide**—Explains how to configure IGMP and IP routing features.
- **Access Security Guide**—Explains how to configure access security features and user authentication on the switch.
- **IPv6 Configuration Guide**—Describes the IPv6 protocol operations that are supported on the switch.
- **Command Line Interface Reference Guide**—Provides a comprehensive description of CLI commands, syntax, and operations.
- **Event Log Message Reference Guide**—Provides a comprehensive description of event log messages.
- **Release Notes**—Describe new features, fixes, and enhancements that become available between revisions of the main product guide.
Software Feature Index

This feature index indicates which manual to consult for information on a given software feature.

**Intelligent Edge Software Features.** These features are automatically included on all switches.

<table>
<thead>
<tr>
<th>Intelligent Edge Software Features</th>
<th>Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q VLAN Tagging</td>
<td>X</td>
</tr>
<tr>
<td>802.1X Port-Based Priority</td>
<td>X</td>
</tr>
<tr>
<td>802.1X Multiple Authenticated Clients Per Port</td>
<td>X</td>
</tr>
<tr>
<td>Access Control Lists (ACLs)</td>
<td>X</td>
</tr>
<tr>
<td>AAA Authentication</td>
<td>X</td>
</tr>
<tr>
<td>Authorized IP Managers</td>
<td>X</td>
</tr>
<tr>
<td>Authorized Manager List (Web, Telnet, TFTP)</td>
<td>X</td>
</tr>
<tr>
<td>Auto MDIX Configuration</td>
<td>X</td>
</tr>
<tr>
<td>BOOTP</td>
<td>X</td>
</tr>
<tr>
<td>Config File</td>
<td></td>
</tr>
<tr>
<td>Console Access</td>
<td>X</td>
</tr>
<tr>
<td>Copy Command</td>
<td>X</td>
</tr>
<tr>
<td>Core Dump</td>
<td>X</td>
</tr>
<tr>
<td>CoS (Class of Service)</td>
<td></td>
</tr>
<tr>
<td>Debug</td>
<td>X</td>
</tr>
<tr>
<td>DHCP Configuration</td>
<td>X</td>
</tr>
<tr>
<td>Intelligent Edge Software Features</td>
<td>Manual</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td>Management and</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td></td>
<td>Advanced Traffic</td>
</tr>
<tr>
<td></td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Multicast and</td>
</tr>
<tr>
<td></td>
<td>Routing</td>
</tr>
<tr>
<td></td>
<td>Access Security</td>
</tr>
<tr>
<td></td>
<td>Guide</td>
</tr>
<tr>
<td></td>
<td>IPv6 Configuration</td>
</tr>
<tr>
<td></td>
<td>Guide</td>
</tr>
<tr>
<td></td>
<td>Basic Operation Guide</td>
</tr>
<tr>
<td>DHCP Option 82</td>
<td>X</td>
</tr>
<tr>
<td>DHCP Snooping</td>
<td>X</td>
</tr>
<tr>
<td>DHCP/Bootp Operation</td>
<td>X</td>
</tr>
<tr>
<td>Diagnostic Tools</td>
<td>X</td>
</tr>
<tr>
<td>Diagnostics and Troubleshooting (IPv6)</td>
<td>X</td>
</tr>
<tr>
<td>Downloading Software</td>
<td>X</td>
</tr>
<tr>
<td>Dynamic ARP Protection</td>
<td>X</td>
</tr>
<tr>
<td>Dynamic Configuration Arbiter</td>
<td>X</td>
</tr>
<tr>
<td>Dynamic IP Lockdown</td>
<td>X</td>
</tr>
<tr>
<td>Eavesdrop Protection</td>
<td>X</td>
</tr>
<tr>
<td>Event Log</td>
<td>X</td>
</tr>
<tr>
<td>Factory Default Settings</td>
<td>X</td>
</tr>
<tr>
<td>Flow Control (802.3x)</td>
<td>X</td>
</tr>
<tr>
<td>File Management</td>
<td>X</td>
</tr>
<tr>
<td>File Transfers</td>
<td>X</td>
</tr>
<tr>
<td>Friendly Port Names</td>
<td>X</td>
</tr>
<tr>
<td>Guaranteed Minimum Bandwidth (GMB)</td>
<td>X</td>
</tr>
<tr>
<td>GVRP</td>
<td>X</td>
</tr>
<tr>
<td>Identity-Driven Management (IDM)</td>
<td>X</td>
</tr>
<tr>
<td>IGMP</td>
<td>X</td>
</tr>
<tr>
<td>Interface Access (Telnet, Console/Serial, Web)</td>
<td>X</td>
</tr>
<tr>
<td>IP Addressing</td>
<td>X</td>
</tr>
<tr>
<td>IPv6 Addressing</td>
<td>X</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>IP Preserve (IPv6)</td>
<td>X</td>
</tr>
<tr>
<td>IP Routing</td>
<td></td>
</tr>
<tr>
<td>Jumbo Packets</td>
<td>X</td>
</tr>
<tr>
<td>Key Management System (KMS)</td>
<td></td>
</tr>
<tr>
<td>LACP</td>
<td></td>
</tr>
<tr>
<td>LLDP</td>
<td></td>
</tr>
<tr>
<td>LLDP-MED</td>
<td></td>
</tr>
<tr>
<td>Loop Protection</td>
<td></td>
</tr>
<tr>
<td>MAC Address Management</td>
<td></td>
</tr>
<tr>
<td>MAC Lockdown</td>
<td></td>
</tr>
<tr>
<td>MAC Lockout</td>
<td></td>
</tr>
<tr>
<td>MAC-based Authentication</td>
<td></td>
</tr>
<tr>
<td>Management VLAN</td>
<td></td>
</tr>
<tr>
<td>MLDv1</td>
<td></td>
</tr>
<tr>
<td>Monitoring and Analysis</td>
<td></td>
</tr>
<tr>
<td>Multicast Filtering</td>
<td></td>
</tr>
<tr>
<td>Multiple Configuration Files</td>
<td></td>
</tr>
<tr>
<td>Network Management Applications (SNMP)</td>
<td></td>
</tr>
<tr>
<td>OpenView Device Management</td>
<td></td>
</tr>
<tr>
<td>Passwords and Password Clear Protection</td>
<td></td>
</tr>
<tr>
<td>PCM/PCM+</td>
<td></td>
</tr>
<tr>
<td>Ping</td>
<td>X</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>X</td>
</tr>
<tr>
<td>Intelligent Edge Software Features</td>
<td>Manual</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Port Monitoring</td>
<td>X</td>
</tr>
<tr>
<td>Port Security</td>
<td>X</td>
</tr>
<tr>
<td>Port Status</td>
<td>X</td>
</tr>
<tr>
<td>Port Trunking (LACP)</td>
<td>X</td>
</tr>
<tr>
<td>Port-Based Access Control (802.1X)</td>
<td>X</td>
</tr>
<tr>
<td>Power over Ethernet (PoE and PoE+)</td>
<td>X</td>
</tr>
<tr>
<td>Protocol Filters</td>
<td>X</td>
</tr>
<tr>
<td>Protocol VLANS</td>
<td>X</td>
</tr>
<tr>
<td>Quality of Service (QoS)</td>
<td>X</td>
</tr>
<tr>
<td>RADIUS Authentication and Accounting</td>
<td>X</td>
</tr>
<tr>
<td>RADIUS-Based Configuration</td>
<td>X</td>
</tr>
<tr>
<td>Rate-Limiting</td>
<td>X</td>
</tr>
<tr>
<td>RIP</td>
<td>X</td>
</tr>
<tr>
<td>RMON 1,2,3,9</td>
<td>X</td>
</tr>
<tr>
<td>Routing</td>
<td>X</td>
</tr>
<tr>
<td>Routing - IP Static</td>
<td>X</td>
</tr>
<tr>
<td>Secure Copy</td>
<td>X</td>
</tr>
<tr>
<td>Secure Copy (IPv6)</td>
<td>X</td>
</tr>
<tr>
<td>sFlow</td>
<td>X</td>
</tr>
<tr>
<td>SFTP</td>
<td>X</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>X</td>
</tr>
<tr>
<td>SNMP (IPv6)</td>
<td>X</td>
</tr>
<tr>
<td>Software Downloads (SCP/SFTP, TFPT, Xmodem)</td>
<td>X</td>
</tr>
<tr>
<td>Intelligent Edge Software Features</td>
<td>Manual</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Source-Port Filters</td>
<td>X</td>
</tr>
<tr>
<td>Spanning Tree (STP, RSTP, MSTP)</td>
<td>X</td>
</tr>
<tr>
<td>SSHv2 (Secure Shell) Encryption</td>
<td>X</td>
</tr>
<tr>
<td>SSH (IPv6)</td>
<td>X</td>
</tr>
<tr>
<td>SSL (Secure Socket Layer)</td>
<td>X</td>
</tr>
<tr>
<td>Stacking</td>
<td>X</td>
</tr>
<tr>
<td>Syslog</td>
<td>X</td>
</tr>
<tr>
<td>System Information</td>
<td>X</td>
</tr>
<tr>
<td>TACACS+ Authentication</td>
<td>X</td>
</tr>
<tr>
<td>Telnet Access</td>
<td>X</td>
</tr>
<tr>
<td>Telnet (IPv6)</td>
<td>X</td>
</tr>
<tr>
<td>TFTP</td>
<td>X</td>
</tr>
<tr>
<td>Time Protocols (TimeP, SNTP)</td>
<td>X</td>
</tr>
<tr>
<td>Time Protocols (IPv6)</td>
<td>X</td>
</tr>
<tr>
<td>Traffic Mirroring</td>
<td>X</td>
</tr>
<tr>
<td>Traffic/Security Filters</td>
<td>X</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>X</td>
</tr>
<tr>
<td>Uni-Directional Link Detection (UDLD)</td>
<td>X</td>
</tr>
<tr>
<td>UDP Forwarder</td>
<td>X</td>
</tr>
<tr>
<td>USB Device Support</td>
<td>X</td>
</tr>
<tr>
<td>VLANS</td>
<td>X</td>
</tr>
<tr>
<td>VLAN Mirroring (1 static VLAN)</td>
<td>X</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td>X</td>
</tr>
<tr>
<td>Intelligent Edge Software Features</td>
<td>Manual</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td>Management and Configura-</td>
</tr>
<tr>
<td></td>
<td>Advanced Traffic Manage-</td>
</tr>
<tr>
<td></td>
<td>Multicast and Routing</td>
</tr>
<tr>
<td></td>
<td>Access Security Guide</td>
</tr>
<tr>
<td></td>
<td>IPv6 Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>Basic Operation Guide</td>
</tr>
<tr>
<td>Web Authentication RADIUS Support</td>
<td>X</td>
</tr>
<tr>
<td>Web-based Authentication</td>
<td>X</td>
</tr>
<tr>
<td>Web UI</td>
<td>X</td>
</tr>
</tbody>
</table>
Security Overview

Introduction

This chapter provides an overview of the security features included on your switch. Table 1-1 on page 1-2 outlines the access security and authentication features, while Table 1-2 on page 1-6 highlights the additional features designed to help secure and protect your network. For detailed information on individual features, see the references provided.

Before you connect your switch to a network, HP strongly recommends that you review the section titled “Getting Started with Access Security” on page 1-9. It outlines potential threats for unauthorized switch and network access, and provides guidelines on how to prepare the switch for secure network operation.

About This Guide

This Access Security Guide describes how to configure security features on your switch.

For More Information

For IPv6-specific security settings and features, refer to the IPV6 Configuration Guide for your switch.

For information on which product manual to consult for a specific software feature, refer to the “Software Feature Index” on page xxii of this guide.

For the latest version of all HP switch documentation, including Release Notes covering recently added features and other software topics, visit the HP Networking web site at www.hp.com/support/manuals.
Access Security Features

This section provides an overview of the switch’s access security features, authentication protocols, and methods. Table 1-1 lists these features and provides summary configuration guidelines. For more in-depth information, see the references provided (all chapter and page references are to this Access Security Guide unless a different manual name is indicated).

Note

The Management Interface wizard provides a convenient step-by-step method to prepare the switch for secure network operation. See “Quick Start: Using the Management Interface Wizard” on page 1-10 for details.

Table 1-1. Access Security and Switch Authentication Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>Security Guidelines</th>
<th>More Information and Configuration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>no password</td>
<td>Configuring a local Manager password is a fundamental step in reducing the possibility of unauthorized access through the switch’s WebAgent and console (CLI and Menu) interfaces. The Manager password can easily be set by any one of the following methods:</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td></td>
<td>• CLI: password manager command, or Management interface wizard</td>
<td>“Configuring Local Password Security” on page 2-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WebAgent: the password options under the Security tab, or Management interface wizard</td>
<td>“Quick Start: Using the Management Interface Wizard” on page 1-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Menu interface: Console Passwords option</td>
<td>“Using SNMP To View and Configure Switch Authentication Features” on page 6-21</td>
</tr>
</tbody>
</table>
Access Security Features

The default remote management protocols enabled on the switch are plain text protocols, which transfer passwords in open or plain text that is easily captured. To reduce the chances of unauthorized users capturing your passwords, secure and encrypted protocols such as SSH and SSL (see below for details) should be used for remote access. This enables you to employ increased access security while still retaining remote client access.

Also, access security on the switch is incomplete without disabling Telnet and the standard Web browser access (WebAgent). Among the methods for blocking unauthorized access attempts using Telnet or the WebAgent are the following two CLI commands:

- **no telnet-server**: This command blocks inbound Telnet access.
- **no web-management**: This command prevents use of the WebAgent through http (port 80) server access.

If you choose not to disable Telnet and the WebAgent, you may want to consider using RADIUS accounting to maintain a record of password-protected access to the switch.

### SSH

SSH provides Telnet-like functions through encrypted, authenticated transactions of the following types:

- **client public-key authentication**: uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a stored public key can gain access to the switch.
- **switch SSH and user password authentication**: this option is a subset of the client public-key authentication, and is used if the switch has SSH enabled without a login access configured to authenticate the client’s key. In this case, the switch authenticates itself to clients, and users on SSH clients then authenticate themselves to the switch by providing passwords stored on a RADIUS or TACACS+ server, or locally on the switch.
- **secure copy (SC) and secure FTP (SFTP)**: By opening a secure, encrypted SSH session, you can take advantage of SC and SFTP to provide a secure alternative to TFTP for transferring sensitive switch information. For more on SC and SFTP, refer to the section titled “Using Secure Copy and SFTP” in the “File Transfers” appendix of the Management and Configuration Guide for your switch.

---

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>Security Guidelines</th>
<th>More Information and Configuration Details</th>
</tr>
</thead>
</table>
| Telnet and Web-browser access (WebAgent) | enabled | The default remote management protocols enabled on the switch are plain text protocols, which transfer passwords in open or plain text that is easily captured. To reduce the chances of unauthorized users capturing your passwords, secure and encrypted protocols such as SSH and SSL (see below for details) should be used for remote access. This enables you to employ increased access security while still retaining remote client access. Also, access security on the switch is incomplete without disabling Telnet and the standard Web browser access (WebAgent). Among the methods for blocking unauthorized access attempts using Telnet or the WebAgent are the following two CLI commands:  
- **no telnet-server**: This command blocks inbound Telnet access.  
- **no web-management**: This command prevents use of the WebAgent through http (port 80) server access. | “Quick Start: Using the Management Interface Wizard” on page 1-10 For more on Telnet and the WebAgent, refer to the chapter on “Interface Access and System Information” in the Basic Operation Guide. For RADIUS accounting, refer to Chapter 8, “RADIUS Authentication and Accounting” |
| SSH | disabled | SSH provides Telnet-like functions through encrypted, authenticated transactions of the following types:  
- client public-key authentication: uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a stored public key can gain access to the switch.  
- switch SSH and user password authentication: this option is a subset of the client public-key authentication, and is used if the switch has SSH enabled without a login access configured to authenticate the client’s key. In this case, the switch authenticates itself to clients, and users on SSH clients then authenticate themselves to the switch by providing passwords stored on a RADIUS or TACACS+ server, or locally on the switch.  
- secure copy (SC) and secure FTP (SFTP): By opening a secure, encrypted SSH session, you can take advantage of SC and SFTP to provide a secure alternative to TFTP for transferring sensitive switch information. For more on SC and SFTP, refer to the section titled “Using Secure Copy and SFTP” in the “File Transfers” appendix of the Management and Configuration Guide for your switch. | “Quick Start: Using the Management Interface Wizard” on page 1-10 Chapter 8 “Configuring Secure Shell (SSH)” |
## Security Overview
### Access Security Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>Security Guidelines</th>
<th>More Information and Configuration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>disabled</td>
<td>Secure Socket Layer (SSL) and Transport Layer Security (TLS) provide remote Web browser access (WebAgent) to the switch via authenticated transactions and encrypted paths between the switch and management station clients capable of SSL/TLS operation. The authenticated type includes server certificate authentication with user password authentication.</td>
<td>“Quick Start: Using the Management Interface Wizard” on page 1-10 Chapter 9, “Configuring Secure Socket Layer (SSL)”</td>
</tr>
<tr>
<td>SNMP</td>
<td>public, unrestricted</td>
<td>In the default configuration, the switch is open to access by management stations running SNMP management applications capable of viewing and changing the settings and status data in the switch’s MIB (Management Information Base). Thus, controlling SNMP access to the switch and preventing unauthorized SNMP access should be a key element of your network security strategy.</td>
<td>“SNMP Security Guidelines” on page 1-13; see the section “Using SNMP Tools To Manage the Switch” in the Management and Configuration Guide</td>
</tr>
<tr>
<td>Authorized IP Managers</td>
<td>none</td>
<td>This feature uses IP addresses and masks to determine whether to allow management access to the switch across the network through the following: Telnet and other terminal emulation applications, The WebAgent, SNMP (with a correct community name)</td>
<td>Chapter 15, “Using Authorized IP Managers”</td>
</tr>
<tr>
<td>Secure Management VLAN</td>
<td>disabled</td>
<td>This feature creates an isolated network for managing the HP switches that offer this feature. When a secure management VLAN is enabled, CLI, Menu interface, and WebAgent access is restricted to ports configured as members of the VLAN.</td>
<td>Advanced Traffic Management Guide, refer to the chapter “Static Virtual LANs (VLANs)”</td>
</tr>
<tr>
<td>ACLs for Management Access Protection</td>
<td>none</td>
<td>ACLs can also be configured to protect management access by blocking inbound IP traffic that has the switch itself as the destination IP address.</td>
<td>“Access Control Lists (ACLs)” on page 1-7 Chapter 10, “IPv4 Access Control Lists (ACLs)”</td>
</tr>
<tr>
<td>TACACS+ Authentication</td>
<td>disabled</td>
<td>This application uses a central server to allow or deny access to TACACS-aware devices in your network. TACACS+ uses username/password sets with associated privilege levels to grant or deny access through either the switch’s serial (console) port or remotely, with Telnet. If the switch fails to connect to a TACACS+ server for the necessary authentication service, it defaults to its own locally configured passwords for authentication control. TACACS+ allows both login (read-only) and enable (read/write) privilege level access.</td>
<td>Chapter 5, “TACACS+ Authentication”</td>
</tr>
<tr>
<td>RADIUS Authentication</td>
<td>disabled</td>
<td>For each authorized client, RADIUS can be used to authenticate operator or manager access privileges on the switch via the serial port (CLI and Menu interface), Telnet, SSH, and Secure FTP/Secure Copy (SFTP/SCP) access methods.</td>
<td>Chapter 6, “RADIUS Authentication and Accounting”</td>
</tr>
</tbody>
</table>
### Security Overview

Access Security Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>Security Guidelines</th>
<th>More Information and Configuration Details</th>
</tr>
</thead>
</table>
| **802.1X Access Control**| none            | This feature provides port-based or user-based authentication through a RADIUS server to protect the switch from unauthorized access and to enable the use of RADIUS-based user profiles to control client access to network services. Included in the general features are the following:  
  - user-based access control supporting up to 32 authenticated clients per port  
  - port-based access control allowing authentication by a single client to open the port  
  - switch operation as a supplicant for point-to-point connections to other 802.1X-compliant HP switches | Chapter 13 “Configuring Port-Based and User-Based Access Control (802.1X)”                                   |
| **Web and MAC Authentication** | none            | These options are designed for application on the edge of a network to provide port-based security measures for protecting private networks and the switch itself from unauthorized access. Because neither method requires clients to run any special supplicant software, both are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option.  
Both methods rely on using a RADIUS server for authentication. This simplifies access security management by allowing you to control access from a master database in a single server. It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN. Web authentication uses a web page login to authenticate users for access to the network. MAC authentication grants access to a secure network by authenticating device MAC addresses for access to the network. | Chapter 4, “Web and MAC Authentication”                                                                 |
Network Security Features

This section outlines features and defence mechanisms for protecting access through the switch to the network. For more detailed information, see the indicated chapters.

Table 1-2. Network Security—Default Settings and Security Guidelines

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>Security Guidelines</th>
<th>More Information and Configuration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure File Transfers</td>
<td>not applicable</td>
<td>Secure Copy and SFTP provide a secure alternative to TFTP and auto-TFTP for transferring sensitive information such as configuration files and log information between the switch and other devices.</td>
<td>Management and Configuration Guide, Appendix A “File Transfers”, refer to the section “Using Secure Copy and SFTP”</td>
</tr>
<tr>
<td>USB Autorun</td>
<td>enabled (disabled once a password has been set)</td>
<td>Used in conjunction with HP PCM+, this feature allows diagnosis and automated updates to the switch via the USB flash drive. When enabled in secure mode, this is done with secure credentials to prevent tampering. Note that the USB Autorun feature is disabled automatically, once a password has been set on the switch.</td>
<td>Management and Configuration Guide, Appendix A “File Transfers”, refer to the section “USB Autorun”</td>
</tr>
</tbody>
</table>
| Traffic/Security Filters | none | These statically configured filters enhance in-band security (and improve control over access to network resources) by forwarding or dropping inbound network traffic according to the configured criteria. Filter options include:  
- **source-port filters**: Inbound traffic from a designated, physical source-port will be forwarded or dropped on a per-port (destination) basis.  
- **multicast filters**: Inbound traffic having a specified multicast MAC address will be forwarded to outbound ports or dropped on a per-port (destination) basis.  
- **protocol filters**: Inbound traffic having the selected frame (protocol) type will be forwarded or dropped on a per-port (destination) basis. | Chapter 12, “Traffic/Security Filters and Monitors” |
Security Overview
Network Security Features

Access Control Lists (ACLs)  
ACLs can filter traffic to or from a host, a group of hosts, or entire subnets. Layer 3 IP filtering with Access Control Lists (ACLs) enables you to improve network performance and restrict network use by creating policies for:

- **Switch Management Access**: Permits or denies in-band management access. This includes preventing the use of certain TCP or UDP applications (such as Telnet, SSH, WebAgent, and SNMP) for transactions between specific source and destination IP addresses.

- **Application Access Security**: Eliminating unwanted IP, TCP, or UDP traffic by filtering packets where they enter or leave the switch on specific interfaces.

Note on ACL Security Use:
ACLs can enhance network security by blocking selected IP traffic, and can serve as one aspect of maintaining network security. However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete security solution.

Port Security, MAC Lockdown, and MAC Lockout  
The features listed below provide device-based access security in the following ways:

- **Port security**: Enables configuration of each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch. Some switch models also include eavesdrop prevention in the port security feature.

- **MAC lockout**: This “static addressing” feature is used as an alternative to port security to prevent station movement and MAC address “hijacking” by allowing a given MAC address to use only one assigned port on the switch. MAC lockout also restricts the client device to a specific VLAN.

- **MAC lockout**: This feature enables blocking of a specific MAC address so that the switch drops all traffic to or from the specified address.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>Security Guidelines</th>
<th>More Information and Configuration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Lists (ACLs)</td>
<td>none</td>
<td>ACLs can filter traffic to or from a host, a group of hosts, or entire subnets. Layer 3 IP filtering with Access Control Lists (ACLs) enables you to improve network performance and restrict network use by creating policies for: • Switch Management Access: Permits or denies in-band management access. This includes preventing the use of certain TCP or UDP applications (such as Telnet, SSH, WebAgent, and SNMP) for transactions between specific source and destination IP addresses.) • Application Access Security: Eliminating unwanted IP, TCP, or UDP traffic by filtering packets where they enter or leave the switch on specific interfaces. Note on ACL Security Use: ACLs can enhance network security by blocking selected IP traffic, and can serve as one aspect of maintaining network security. However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete security solution.</td>
<td>Chapter 10, “IPv4 Access Control Lists (ACLs)”</td>
</tr>
<tr>
<td>Port Security, MAC Lockdown, and MAC Lockout</td>
<td>none</td>
<td>The features listed below provide device-based access security in the following ways: • Port security: Enables configuration of each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch. Some switch models also include eavesdrop prevention in the port security feature. • MAC lockout: This “static addressing” feature is used as an alternative to port security to prevent station movement and MAC address “hijacking” by allowing a given MAC address to use only one assigned port on the switch. MAC lockout also restricts the client device to a specific VLAN. • MAC lockout: This feature enables blocking of a specific MAC address so that the switch drops all traffic to or from the specified address.</td>
<td>Chapter 13, “Configuring and Monitoring Port Security”</td>
</tr>
</tbody>
</table>

See also “Precedence of Port-Based Security Options” on page 1-15
## Security Overview
### Network Security Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>Security Guidelines</th>
<th>More Information and Configuration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Management System (KMS)</strong></td>
<td>none</td>
<td>KMS is available in several HP switch models and is designed to configure and maintain key chains for use with KMS-capable routing protocols that use time-dependent or time-independent keys. (A key chain is a set of keys with a timing mechanism for activating and deactivating individual keys.) KMS provides specific instances of routing protocols with one or more Send or Accept keys that must be active at the time of a request.</td>
<td>Chapter 16, “Key Management System”</td>
</tr>
<tr>
<td><strong>Spanning Tree Protection</strong></td>
<td>none</td>
<td>These features prevent your switch from malicious attacks or configuration errors:</td>
<td>Advanced Traffic Management Guide, refer to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>BPDU Filtering and BPDU Protection</strong>: Protects the network from denial-of-service attacks that use spoofing BPDU by dropping incoming BPDU frames and/or blocking traffic through a port.</td>
<td>the chapter &quot;Multiple Instance Spanning-Tree Operation&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>STP Root Guard</strong>: Protects the STP root bridge from malicious attacks or configuration mistakes.</td>
<td></td>
</tr>
<tr>
<td><strong>DHCP Snooping, Dynamic ARP Protection, and Dynamic IP Lockdown</strong></td>
<td>none</td>
<td>These features provide the following additional protections for your network:</td>
<td>Chapter 11, “Configuring Advanced Threat Protection”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>DHCP Snooping</strong>: Protects your network from common DHCP attacks, such as address spoofing and repeated address requests.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Dynamic ARP Protection</strong>: Protects your network from ARP cache poisoning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Dynamic IP Lockdown</strong>: Prevents IP source address spoofing on a per-port and per-VLAN basis</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Instrumentation Monitor</strong>: Helps identify a variety of malicious attacks by generating alerts for detected anomalies on the switch.</td>
<td></td>
</tr>
</tbody>
</table>
Getting Started with Access Security

HP switches are designed as “plug and play” devices, allowing quick and easy installation in your network. In its default configuration the switch is open to unauthorized access of various types. When preparing the switch for network operation, therefore, HP strongly recommends that you enforce a security policy to help ensure that the ease in getting started is not used by unauthorized persons as an opportunity for access and possible malicious actions.

Since security incidents can originate with sources inside as well as outside of an organization, your access security provisions must protect against internal and external threats while preserving the necessary network access for authorized clients and users. It is important to evaluate the level of management access vulnerability existing in your network and take steps to ensure that all reasonable security precautions are in place. This includes both configurable security options and physical access to the switch.

Switch management access is available through the following methods:

- Front panel access to the console serial port (see “Physical Security”)
- Inbound Telnet access
- Web-browser access (WebAgent)
- SNMP access

For guidelines on locking down your switch for remote management access, see “Quick Start: Using the Management Interface Wizard” on page 1-10.

Physical Security

Physical access to the switch allows the following:

- use of the console serial port (CLI and Menu interface) for viewing and changing the current configuration and for reading status, statistics, and log messages.
- use of the switch’s USB port for file transfers and autorun capabilities.
- use of the switch’s Clear and Reset buttons for these actions:
  - clearing (removing) local password protection
  - rebooting the switch
  - restoring the switch to the factory default configuration (and erasing any non-default configuration settings)
Keeping the switch in a locked wiring closet or other secure space helps to prevent unauthorized physical access.

As additional precautions, you can do the following:
- Disable or re-enable the password-clearing function of the Clear button.
- Configure the Clear button to reboot the switch after clearing any local usernames and passwords.
- Modify the operation of the Reset+Clear button combination so that the switch reboots, but does not restore the switch’s factory default settings.
- Disable or re-enable password recovery.
- Disable USB autorun by setting a Manager password, or enable USB autorun in secure mode so that security credentials are required to use this feature.

For the commands used to configure the Clear and Reset buttons, refer to “Front-Panel Security” on page 2-23. For information on using USB Autorun, refer to the sections on “Using USB to Transfer Files to and from the Switch” and “Using USB Autorun” in the Management and Configuration Guide, Appendix A “File Transfers”.

**Figure 1-1. Quick Start: Using the Management Interface Wizard**

The Management Interface wizard provides a convenient step-by-step method to prepare the switch for secure network operation. It guides you through the process of locking down the following switch operations or protocols:
- setting local passwords
- restricting SNMP access
- enabling/disabling Telnet
- enabling/disabling SSH
- enabling/disabling remote Web management (WebAgent)
- restricting WebAgent access to SSL
- enabling/disabling USB autorun
- setting timeouts for SSH/Telnet sessions

The wizard can also be used to view the pre-configured defaults and see the current settings for switch access security. The wizard can be launched either via the CLI (see page 1-11) or the WebAgent (see page 1-12).

**Note**

The wizard’s security settings can also be configured using standard commands via the CLI, Menu, or WebAgent. For full details on preparing and configuring the switch for SSH and SSL operation, refer to chapters 7 and 8 respectively.
CLI: Management Interface Wizard

To configure security settings using the CLI wizard, follow the steps below:

1. At the command prompt, type `setup mgmt-interfaces`.

   The welcome banner appears and the first setup option is displayed (Operator password). As you advance through the wizard, each setup option displays the current value in brackets [] as shown in Figure 1-2.

   ![Figure 1-2. Example of Management Interface Wizard Configuration](image-url)
2. When you enter the wizard, you have the following options:
   - To update a setting, type in a new value, or press [Enter] to keep the current value.
   - To quit the wizard without saving any changes, press [CTRL-C] at any time.
   - To access online Help for any option, press [?].

   After you have gone through each setup option, the wizard displays the summary configuration together with a prompt to save the changes (see Figure 1-2 on page 1-11 for an example).

3. When the message appears asking if you want to save these changes, you have the following options:
   - To save your changes, press [Enter].
   - To cancel any changes without saving, type [n] and then press [Enter].

   After pressing [Enter], the wizard exits to the command line prompt.

**CLI Wizard: Operating Notes and Restrictions.**

- Once a password has been configured on the switch, you cannot remove it using the CLI wizard. Passwords can be removed by executing the no password command directly from the CLI.
- When you restrict SNMP access to SNMPv3 only, the options SNMPv2 community name and access level will not appear.
- The wizard displays the first available SNMPv2 community and allows the user to modify the first community access parameters.
- The wizard creates a new SNMP community only when no communities have been configured on the switch.
- The USB Autorun feature is disabled as soon as an operator or manager password is set on the switch. Once a password has been set, the USB autorun option is no longer provided as part of the wizard.

**WebAgent: Management Interface Wizard**

To use the Management Interface wizard from the WebAgent, follow the steps below:

1. In the navigation tree, select Security.

2. Click on the Security Wizard. The Welcome window appears.
This page allows you to choose between two setup types:

- **Typical**—provides a multiple page, step-by-step method to configure security settings, with on-screen instructions for each option.
- **Advanced**—provides a single summary screen in which to configure all security settings at once.

Refer to the WebAgent Online Help for detailed information about using the Management Interface wizard.

**SNMP Security Guidelines**

In the default configuration, the switch is open to access by management stations running SNMP (Simple Network Management Protocol) management applications capable of viewing and changing the settings and status data in the switch's MIB (Management Information Base). Thus, controlling SNMP access to the switch and preventing unauthorized SNMP access should be a key element of your network security strategy.

**General SNMP Access to the Switch.** The switch supports SNMP versions 1, 2c, and 3, including SNMP community and trap configuration. The default configuration supports versions 1 and 2c compatibility, which uses plain text and does not provide security options.

HP recommends that you enable SNMP version 3 for improved security. SNMPv3 includes the ability to configure restricted access and to block all non-version 3 messages (which blocks version 1 and 2c unprotected operation).

SNMPv3 security options include:

- configuring device communities as a means for excluding management access by unauthorized stations
- configuring for access authentication and privacy
- reporting events to the switch CLI and to SNMP trap receivers
- restricting non-SNMPv3 agents to either read-only access or no access
- co-existing with SNMPv1 and v2c if necessary

**SNMP Access to the Authentication Configuration MIB.** A management station running an SNMP networked device management application, such as HP PCM+ or HP OpenView, can access the switch's management information base (MIB) for read access to the switch's status and read/write access to the switch's authentication configuration (hpSwitchAuth). This means that the switch's default configuration now allows SNMP access to security settings in hpSwitchAuth.
If SNMP access to the hpSwitchAuth MIB is considered a security risk in your network, then you should implement the following security precautions:

- If SNMP access to the authentication configuration (hpSwitchAuth) MIB described above is not desirable for your network, use the following command to disable this feature:

  `snmp-server mib hpswitchauthmib excluded`

- If you choose to leave the authentication configuration MIB accessible, then you should do the following to help ensure that unauthorized workstations cannot use SNMP tools to access the MIB:
  a. Configure SNMP version 3 management and access security on the switch.
  b. Disable SNMP version 2c on the switch.

For details on this feature, refer to the section titled “Using SNMP To View and Configure Switch Authentication Features” on page 5-27.

For more information on configuring SNMP, refer to the section “Using SNMP Tools To Manage the Switch” in the chapter “Configuring for Network Management Applications” in the Management and Configuration Guide for your switch.
Security Overview

Precedence of Security Options

This section explains how port-based security options, and client-based attributes used for authentication, get prioritized on the switch.

Precedence of Port-Based Security Options

Where the switch is running multiple security options, it implements network traffic security based on the OSI (Open Systems Interconnection model) precedence of the individual options, from the lowest to the highest. The following list shows the order in which the switch implements configured security features on traffic moving through a given port.

1. Disabled/Enabled physical port
2. MAC lockout (Applies to all ports on the switch.)
3. MAC lockdown
4. Port security
5. Authorized IP Managers
6. Application features at higher levels in the OSI model, such as SSH. (The above list does not address the mutually exclusive relationship that exists among some security features.)

Precedence of Client-Based Authentication:
Dynamic Configuration Arbiter

The Dynamic Configuration Arbiter (DCA) is implemented to determine the client-specific parameters that are assigned in an authentication session.

A client-specific authentication configuration is bound to the MAC address of a client device and may include the following parameters:

- Untagged client VLAN ID
- Tagged VLAN IDs
- Per-port CoS (802.1p) priority
- Per-port rate-limiting on inbound traffic
- Client-based ACLs
DCA allows client-specific parameters configured in any of the following ways to be applied and removed as needed in a specified hierarchy of precedence. When multiple values for an individual configuration parameter exist, the value applied to a client session is determined in the following order (from highest to lowest priority) in which a value configured with a higher priority overrides a value configured with a lower priority:

1. Attribute profiles applied through the Network Immunity network-management application using SNMP (see “HP E-Network Immunity Manager”)
2. 802.1X authentication parameters (RADIUS-assigned)
3. Web- or MAC-authentication parameters (RADIUS-assigned)
4. Local, statically-configured parameters

Although RADIUS-assigned settings are never applied to ports for non-authenticated clients, the Dynamic Configuration Arbiter allows you to configure and assign client-specific port configurations to non-authenticated clients, provided that a client’s MAC address is known in the switch in the forwarding database. DCA arbitrates the assignment of attributes on both authenticated and non-authenticated ports.

DCA does not support the arbitration and assignment of client-specific attributes on trunk ports.

**HP E-Network Immunity Manager**

HP E-Network Immunity Manager (NIM) is a plug-in to HP PCM+ and a key component of the HP E-Network Immunity security solution that provides comprehensive detection and per-port-response to malicious traffic at the HP network edge. NIM allows you to apply policy-based actions to minimize the negative impact of a client’s behavior on the network. For example, using NIM you can apply a client-specific profile that adds or modifies per-port rate-limiting and VLAN ID assignments.

**Note**

NIM actions only support the configuration of per-port rate-limiting and VLAN ID assignment; NIM does not support CoS (802.1p) priority assignment and ACL configuration.

NIM-applied parameters temporarily override RADIUS-configured and locally configured parameters in an authentication session. When the NIM-applied action is removed, the previously applied client-specific parameter (locally
configured or RADIUS-assigned) is re-applied unless there have been other configuration changes to the parameter. In this way, NIM allows you to minimize network problems without manual intervention.

NIM also allows you to configure and apply client-specific profiles on ports that are not configured to authenticate clients (unauthorized clients), provided that a client’s MAC address is known in the switch’s forwarding database.

The profile of attributes applied for each client (MAC address) session is stored in the hpicfUsrProfile MIB, which serves as the configuration interface for Network Immunity Manager. A client profile consists of NIM-configured, RADIUS-assigned, and statically configured parameters. Using `show` commands for 802.1X, web or MAC authentication, you can verify which RADIUS-assigned and statically configured parameters are supported and if they are supported on a per-port or per-client basis.

A NIM policy accesses the hpicfUsrProfileMIB through SNMP to perform the following actions:

- Bind (or unbind) a profile of configured attributes to the MAC address of a client device on an authenticated or unauthenticated port.
- Configure or unconfigure an untagged VLAN for use in an authenticated or unauthenticated client session.

Note that the attribute profile assigned to a client is often a combination of NIM-configured, RADIUS-assigned, and statically configured settings. Precedence is always given to the temporarily applied NIM-configured parameters over RADIUS-assigned and locally configured parameters.

For information on HP E-Network Immunity Manager, go to the HP Networking web site at [www.hp.com/solutions](http://www.hp.com/solutions), click on Security, and then click on Security Products.

Arbitrating Client-Specific Attributes

In previous releases, client-specific authentication parameters for 802.1X Web, and MAC authentication are assigned to a port using different criteria. A RADIUS-assigned parameter is always given highest priority and overrides statically configured local passwords. 802.1X authentication parameters override Web or MAC authentication parameters.

DCA stores three levels of client-specific authentication parameters and prioritizes them according to the following hierarchy of precedence:

1. NIM access policy (applied through SNMP)
2. RADIUS-assigned
Security Overview

Precedence of Security Options

1. 802.1X authentication
2. Web or MAC authentication

3. Statically (local) configured

Client-specific configurations are applied on a per-parameter basis on a port. In a client-specific profile, if DCA detects that a parameter has configured values from two or more levels in the hierarchy of precedence described above, DCA decides which parameters to add or remove, or whether to fail the authentication attempt due to an inability to apply the parameters.

For example, NIM may configure only rate-limiting for a specified client session, while RADIUS-assigned values may include both an untagged VLAN ID and a rate-limiting value to be applied. In this case, DCA applies the NIM-configured rate-limiting value and the RADIUS-assigned VLAN (if there are no other conflicts).

Also, you can assign NIM-configured parameters (for example, VLAN ID assignment or rate-limiting) to be activated in a client session when a threat to network security is detected. When the NIM-configured parameters are later removed, the parameter values in the client session return to the RADIUS-configured or locally configured settings, depending on which are next in the hierarchy of precedence.

In addition, DCA supports conflict resolution for QoS (port-based CoS priority) and rate-limiting (ingress) by determining whether to configure either strict or non-strict resolution on a switch-wide basis. For example, if multiple clients authenticate on a port and a rate-limiting assignment by a newly authenticating client conflicts with the rate-limiting values assigned to previous clients, by using Network Immunity you can configure the switch to apply any of the following attributes:

- Apply only the latest rate-limiting value assigned to all clients.
- Apply a client-specific rate-limiting configuration to the appropriate client session (overwrites any rate-limit previously configured for other client sessions on the port).

For information about how to configure RADIUS-assigned and locally configured authentication settings, refer to:

- RADIUS-assigned 802.1X authentication: “Configuring Port-Based and User-Based Access Control (802.1X)” on page 12-1.
- RADIUS-assigned Web or MAC authentication: “Web and MAC Authentication” on page 3-1.
Security Overview
Precedence of Security Options

HP PMC Identity Driven Manager (IDM)

HP PMC IDM is a plug-in to HP PCM+ and uses RADIUS-based technologies to create a user-centric approach to network access management and network activity tracking and monitoring. IDM enables control of access security policy from a central management server, with policy enforcement to the network edge, and protection against both external and internal threats.

Using IDM, a system administrator can configure automatic and dynamic security to operate at the network edge when a user connects to the network. This operation enables the network to:

- approve or deny access at the edge of the network instead of in the core;
- distinguish among different users and what each is authorized to do;
- configure guest access without compromising internal security.

Criteria for enforcing RADIUS-based security for IDM applications includes classifiers such as:

- authorized user identity
- authorized device identity (MAC address)
- software running on the device
- physical location in the network
- time of day

Responses can be configured to support the networking requirements, user (SNMP) community, service needs, and access security level for a given client and device.

For more information on IDM, go to the HP Networking web site at www.hp.com/solutions, click on Security, and then click Security Products.
Configuring Username and Password Security

Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>WebAgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Usernames</td>
<td>none</td>
<td>—</td>
<td>—</td>
<td>page 2-9</td>
</tr>
<tr>
<td>Set a Password</td>
<td>none</td>
<td>page 2-4</td>
<td>page 2-6</td>
<td>page 2-9</td>
</tr>
<tr>
<td>Delete Password Protection</td>
<td>n/a</td>
<td>page 2-5</td>
<td>page 2-7</td>
<td>page 2-9</td>
</tr>
<tr>
<td>show front-panel-security</td>
<td>n/a</td>
<td>—</td>
<td>page 1-13</td>
<td>—</td>
</tr>
<tr>
<td>front-panel-security</td>
<td>—</td>
<td>—</td>
<td>page 1-13</td>
<td>—</td>
</tr>
<tr>
<td>password-clear</td>
<td>enabled</td>
<td>—</td>
<td>page 1-13</td>
<td>—</td>
</tr>
<tr>
<td>reset-on-clear</td>
<td>disabled</td>
<td>—</td>
<td>page 1-14</td>
<td>—</td>
</tr>
<tr>
<td>factory-reset</td>
<td>enabled</td>
<td>—</td>
<td>page 1-15</td>
<td>—</td>
</tr>
<tr>
<td>password-recovery</td>
<td>enabled</td>
<td>—</td>
<td>page 1-15</td>
<td>—</td>
</tr>
</tbody>
</table>

Console access includes both the menu interface and the CLI. There are two levels of console access: Manager and Operator. For security, you can set a *password pair* (username and password) on each of these levels.

**Notes**

Usernames are optional. Also, in the menu interface, you can configure passwords, but not usernames. To configure usernames, use the CLI or the WebAgent.

Usernames and passwords for Manager and Operator access can also be configured using SNMP. For more information, refer to “Using SNMP To View and Configure Switch Authentication Features” on page 5-27.
Overview

Usernames and passwords for Manager and Operator access can also be configured using the Management Interface Wizard. For more information, refer to “Quick Start: Using the Management Interface Wizard” on page 1-10.

<table>
<thead>
<tr>
<th>Level</th>
<th>Actions Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>Access to all console interface areas.</td>
</tr>
<tr>
<td></td>
<td><em>This is the default level.</em> That is, if a Manager password has not been set prior to starting the current console session, then anyone having access to the console can access any area of the console interface.</td>
</tr>
<tr>
<td>Operator</td>
<td>Access to the Status and Counters menu, the Event Log, and the CLI*, but no Configuration capabilities. On the Operator level, the configuration menus, Download OS, and Reboot Switch options in the Main Menu are not available.</td>
</tr>
</tbody>
</table>

*A Allows use of the ping, link-test, show, menu, exit, and logout commands, plus the enable command if you can provide the Manager password.

To configure password security:

1. Set a Manager password pair (and an Operator password pair, if applicable for your system).
2. Exit from the current console session. A Manager password pair will now be needed for full access to the console.

If you do steps 1 and 2, above, then the next time a console session is started for either the menu interface or the CLI, a prompt appears for a password. Assuming you have protected both the Manager and Operator levels, the level of access to the console interface will be determined by which password is entered in response to the prompt.

If you set a Manager password, you may also want to configure an inactivity timer. This causes the console session to end after the specified period of inactivity, thus giving you added security against unauthorized console access.

**Note**

If the console inactivity-timer expires, any outbound Telnet or SSH sessions open on the switch are terminated.
You can use either of the following to set the inactivity timer:

- **Menu Interface**: System Information screen (Select “2. Switch Configuration.)
- **CLI**: Use the `console inactivity-timer < 0 | 1 | 10 | 15 | 20 | 30 | 60 | 120 >`

### Notes

The manager and operator passwords and (optional) usernames control access to the menu interface, CLI, and WebAgent.

If you configure only a Manager password (with no Operator password), and in a later session the Manager password is not entered correctly in response to a prompt from the switch, then the switch does not allow management access for that session.

If the switch has a password for both the Manager and Operator levels, and neither is entered correctly in response to the switch's password prompt, then the switch does not allow management access for that session.

Passwords are case-sensitive.

When configuring an operator or manager password a message will appear indicating that (USB) autorun has been disabled. For more information on the autorun feature, refer to the Appendix A on “File Transfers” in the Management and Configuration Guide for your switch.

### Caution

*If the switch has neither a Manager nor an Operator password, anyone having access to the switch through either Telnet, the serial port, or the WebAgent can access the switch with full manager privileges. Also, if you configure only an Operator password, entering the Operator password enables full manager privileges.*

The rest of this chapter covers how to:

- Set passwords
- Delete passwords
- Recover from a lost password
- Maintain front-panel security
Configuring Local Password Security

Menu: Setting Passwords

As noted earlier in this section, usernames are optional. Configuring a username requires either the CLI or the WebAgent.

1. From the Main Menu select:
   3. Console Passwords

Figure 2-1.  The Set Password Screen

2. To set a new password:
   a. Select **Set Manager Password** or **Set Operator Password**. You will then be prompted with **Enter new password**.
   b. Type a password of up to 64 ASCII characters with no spaces and press **[Enter]**. (Remember that passwords are case-sensitive.)
   c. When prompted with **Enter new password again**, retype the new password and press **[Enter]**.

After you configure a password, if you subsequently start a new console session, you will be prompted to enter the password. (If you use the CLI or WebAgent to configure an optional username, the switch will prompt you for the username, and then the password.)
To Delete Password Protection (Including Recovery from a Lost Password): This procedure deletes all usernames (if configured) and passwords (Manager and Operator).

If you have physical access to the switch, press and hold the Clear button (on the front of the switch) for a minimum of one second to clear all password protection, then enter new passwords as described earlier in this chapter.

If you do not have physical access to the switch, you will need Manager-Level access:

1. Enter the console at the Manager level.
2. Go to the Set Passwords screen as described above.
3. Select Delete Password Protection. You will then see the following prompt:
   
   Continue Deletion of password protection? No

4. Press the Space bar to select Yes, then press [Enter].
5. Press [Enter] to clear the Password Protection message.

To Recover from a Lost Manager Password: If you cannot start a console session at the Manager level because of a lost Manager password, you can clear the password by getting physical access to the switch and pressing and holding the Clear button for a minimum of one second. This action deletes all passwords and usernames (Manager and Operator) used by both the console and the WebAgent.
Configuring Username and Password Security

Configuring Local Password Security

CLI: Setting Passwords and Usernames

Commands Used in This Section

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>See below.</td>
</tr>
</tbody>
</table>

Configuring Manager and Operator Passwords.

Note

The password command has changed. You can now configure manager and operator passwords in one step. See “Saving Security Credentials in a Config File” on page 2-10 of this guide.

Syntax: `[no] password <manager | operator | all | port-access> [user-name ASCII-STR] [<plaintext | sha1> ASCII-STR]

Sets or clears local password/username for a given access level. The command sets or changes existing password(s). If no password is provided in the command, you are prompted to enter the new password twice. The no form of the command removes specific local password protection.

Note: “port-access” is available only if “include-credentials” is enabled.

- `<manager | operator | port-access | all>`: Level of access
- `username`: Username up to 64 characters
- `<plaintext | sha1>`: Format for the password entry, and the password itself (up to 64 characters). The default type is plaintext, which is also the only type accepted for the port-access parameter.

```
HP Switch(config)# password manager
New password: *******
Please retype new password: *******
HP Switch(config)# password operator
New password: *******
Please retype new password: *******
```

Password entries appear as asterisks.
You must type the password entry twice.

Figure 2-2. Example of Configuring Manager and Operator Passwords
To Remove Password Protection. Removing password protection means to eliminate password security. This command prompts you to verify that you want to remove one or both passwords, then clears the indicated password(s). (This command also clears the username associated with a password you are removing.) For example, to remove the Operator password (and username, if assigned) from the switch, you would do the following:

```
HP Switch(config)# no password
Password protection will be deleted, do you want to continue [y/n]? y
HP Switch(config)#
```

Figure 2-3. Removing a Password and Associated Username from the Switch

The effect of executing the command in figure 2-3 is to remove password protection from the Operator level. (This means that anyone who can access the switch console can gain Operator access without having to enter a username or password.)

If you want to remove both operator and manager password protection, use the `no password all` command.

Username and Password Length.

The limit on username and password length is 64 characters for the following authentication methods:

- Front-end—WEB User Interface, SSH, and Telnet
- Back-end—RADIUS, TACACS+, and Local

General Rules for Usernames and Passwords

Usernames and passwords are case-sensitive. ASCII characters in the range of 33-126 are valid, including:

- A through Z uppercase characters
- a through z lower case characters
- 0 through 9 numeric characters
- Special characters ‘ ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : " , < > / ?

(see Restrictions, below)
The SPACE character is allowed to form a username or password pass-phrase. The username must be in quotes, for example “The little brown fox”. A space is not allowed as part of a username without the quotes. A password that includes a space or spaces should not have quotes.

Restrictions for the Setmib Command

Usernames and passwords can be set using the CLI command `setmib`. They cannot be set using SNMP.

- Quotes are permitted for enclosing other characters, for example, a username or password of `abcd` can be enclosed in quotes “abcd” without the quotes becoming part of the username or password itself. Quotes can also be inserted between other characters of a username or password, for example, `ab"cd`. A pair of quotes enclosing characters followed by any additional characters is invalid, for example, “abc”d.

- Spaces are allowed in usernames and passwords. The username or password must be enclosed in quotes, for example, “one two three”. A blank space or spaces between quotes is allowed, for example, “ “.

Additional Restrictions

Some authentication servers prevent the usage of special symbols such as the backslash (\) and quotes ("”). The switch allows the use of these symbols in configurable credentials, but using them may limit access for some users who may use different client software. Please refer to the vendor's documentation for specific information about these restrictions.

Operating Notes on Upgrading or Downgrading Software Versions

When you update software from a version that does not support long pass-words to a version that supports long passwords, the existing usernames and passwords continue to be there; no further action is required.

Before downgrading to a software version that does not include this feature, use one of the following procedures:

1. Reset the username and/or password to be no more than 16 characters in length, and without any special characters, using the CLI command `password` or the equivalent in the WebAgent. Then execute a CLI `write memory` command (required if the `include-credentials` feature has ever been enabled).
Configuring Username and Password Security

Configuring Local Password Security

HP Switch(config)# password manager
New password: ********
Please retype new password: *******
HP Switch(config)# write mem

Or

2. Execute the CLI command no password all. This clears all the passwords. Then execute a CLI write memory command (required if the include-credentials feature has ever been enabled).

   HP Switch(config)# no password all
   Password protections will be deleted, do you want to continue [y/n]? y
   HP Switch(config)# write mem

Or

3. Clear the password by using the "Clear" button on the switch. Then execute a CLI write memory command (required if the include-credentials feature has ever been enabled).

If You Cannot Access the Switch Using the Previous Password

If you cannot access the switch after a software version downgrade, clear the password by using the "Clear" button on the switch to regain access. Then boot into a software version that supports long passwords, and perform steps 1, 2, or 3 in the preceding section.

WebAgent: Setting Passwords and Usernames

In the WebAgent you can enter passwords and (optional) usernames. See the WebAgent Online Help for detailed information.
Configuring Username and Password Security
Saving Security Credentials in a Config File

Saving Security Credentials in a Config File

You can store and view the following security settings in the running-config file associated with the current software image by entering the `include-credentials` command (formerly this information was stored only in internal flash memory):

- Local manager and operator passwords and (optional) user names that control access to a management session on the switch through the CLI, menu interface, or WebAgent
- SNMP security credentials used by network management stations to access a switch, including authentication and privacy passwords
- Port-access passwords and usernames used as 802.1X authentication credentials for access to the switch
- TACACS+ encryption keys used to encrypt packets and secure authentication sessions with TACACS+ servers
- RADIUS shared secret (encryption) keys used to encrypt packets and secure authentication sessions with RADIUS servers
- Secure Shell (SSH) public keys used to authenticate SSH clients that try to connect to the switch.

Benefits of Saving Security Credentials

The benefits of including and saving security credentials in a configuration file are as follows:

- After making changes to security parameters in the running configuration, you can experiment with the new configuration and, if necessary, view the new security settings during the session. After verifying the configuration, you can then save it permanently by writing the settings to the startup-config file.
- By permanently saving a switch’s security credentials in a configuration file, you can upload the file to a TFTP server or Xmodem host, and later download the file to the HP switches on which you want to use the same security settings without having to manually configure the settings (except for SNMPv3 user parameters) on each switch.
Configuring Username and Password Security
Saving Security Credentials in a Config File

By storing different security settings in different files, you can test different security configurations when you first download a new software version that supports multiple configuration files, by changing the configuration file used when you reboot the switch.

For more information about how to experiment with, upload, download, and use configuration files with different software versions, refer to the following:

- The chapter on “Switch Memory and Configuration” in the Basic Operation Guide.
- “Configuring Local Password Security” on page 2-4 in this guide.

Enabling the Storage and Display of Security Credentials

To enable the security settings, enter the include-credentials command.

**Syntax:**

```
[no] include-credentials [radius-tacacs-only | store-in-config]
```

Enables the inclusion and display of the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys in the running configuration. (Earlier software releases store these security configuration settings only in internal flash memory and do not allow you to include and view them in the running-config file.)

To view the currently configured security settings in the running configuration, enter one of the following commands:

- **show running-config**: Displays the configuration settings in the current running-config file.
- **write terminal**: Displays the configuration settings in the current running-config file.

For more information, refer to “Switch Memory and Configuration” in the Basic Operation Guide.

To view the current status of include-credentials on the switch, enter **show include-credentials**. See “Displaying the Status of Include-Credentials on the Switch” on page 2-22.

The “no” form of the command disables only the display and copying of these security parameters from the running configuration, while the security settings remain active in the running configuration.

Default: The security credentials described in “Security Settings that Can Be Saved” on page 2-12 are not stored in the running configuration.
Configuring Username and Password Security

Saving Security Credentials in a Config File

Security Settings that Can Be Saved

The security settings that can be saved to a configuration file are:

- Local manager and operator passwords and user names
- SNMP security credentials, including SNMPv1 community names and SNMPv3 usernames, authentication, and privacy settings
- 802.1X port-access passwords and usernames
- TACACS+ encryption keys
- RADIUS shared secret (encryption) keys
- Public keys of SSH-enabled management stations that are used by the switch to authenticate SSH clients that try to connect to the switch

Executing Include-Credentials or Include-Credentials Store-in-Config

When `include-credentials` or `include-credentials store-in-config` is executed for the first time, for example, on a new switch, or when you previously have successfully executed the `no include-credentials store-in-config` command, the passwords and SSH keys are not currently stored in the configuration file (not activated). This warning message displays.

radius-tacacs-only: When executed with the `radius-tacacs-only` option, only the RADIUS and TACACS security keys are included in the configuration when saving files remotely.

The `radius-tacacs-only` option can be disabled with either command:

```
no include-credentials
no include-credentials radius-tacacs-only
```

`store-in-config`: Stores passwords and SSH authorized keys in the configuration files. This happens automatically when `include-credentials` is enabled.

The `no include-credentials store-in-config` command disables include-credentials AND removes credentials stored in the configuration files. The switch reverts to storing only a single set of passwords and SSH keys, regardless of which configuration file is booted.
No Include-credentials store-in-config Option

The **no include-credentials** command disables include-credentials. Credentials continue to be stored in the active and inactive configurations, but are not displayed in the config file.

When **no include-credentials** is used with the **store-in-config** option, **include-credentials** is disabled and the credentials stored in the config files are removed. The switch is restored to its default state and only stores one set of operator/manager passwords and SSH keys.

If you choose to execute the **no include-credentials store-in-config** command, you are also presented with the option of setting new switch passwords, as shown in Figure 2-5.

You are also queried about retaining the current SSH authorized keys on the switch. If you enter "y", the currently active authorized key files are renamed to the pre-include-credentials names, for example:

```
/file/mgr_auth_keys.2 -> /file/mgr_auth_keys
/file/authorized_keys.2 -> /file/authorized_keys
```

All remaining authorized keys files with an extension are deleted.
Configuring Username and Password Security

Saving Security Credentials in a Config File

Figure 2-5. Example of no include-credentials store-in-config Messages and Options

Local Manager and Operator Passwords

The information saved to the running-config file when the `include-credentials` command is entered includes:

```
password manager [user-name <name>] <hash-type> <pass-hash>
password operator [user-name <name>] <hash-type> <pass-hash>
```

where
- `<name>` is an alphanumeric string for the user name assigned to the manager or operator.
- `<hash-type>` indicates the type of hash algorithm used: SHA-1 or plain text.
- `<pass-hash>` is the SHA-1 authentication protocol's hash of the password or clear ASCII text.

For example, a manager username and password may be stored in a running-config file as follows:

```
password manager user-name George SHA1 2fd4e1c67a2d28fced849e1bb76e7391b93eb12
```

HP Switch(config)# no include-credentials store-in-config

This will remove any switch passwords and inactive SSH authorized keys from all configuration files. This will also restore the functionality to store only a single set of passwords and authorized keys on the switch.

Do you want to continue (y/n)? y

The SSH authorized keys associated with the active configuration will be deleted. Would you like to retain these as the switch global SSH authorized keys (y/n)? y

Do you want to set new switch passwords (y/n)? y

Operator username: admin
Operator password: ********
Confirm password: ********
Manager username: GeorgeV
Manager password: ********
Confirm password: ********

HP Switch(config)
Use the write memory command to save the password configurations in the startup-config file. The passwords take effect when the switch boots with the software version associated with that configuration file.

Caution

If a startup configuration file includes other security credentials, but does not contain a manager or operator password, the switch will not have password protection and can be accessed through Telnet, the serial port, or WebAgent with full manager privileges.

Password Command Options

The password command has the following options:

Syntax: [no] password <manager | operator | port-access> [user-name <name>] [plaintext <password>]

Set or clear a local username/password for a given access level.

- manager: configures access to the switch with manager-level privileges.
- operator: configures access to the switch with operator-level privileges.
- port-access: configures access to the switch through 802.1X authentication with operator-level privileges.
- user-name <name>: the optional text string of the user name associated with the password.
- <password>: the clear ASCII text string for the password.

For more information about configuring local manager and operator passwords, refer to “Configuring Username and Password Security” on page 2-1 in this guide.

SNMP Security Credentials

SNMPv1 community names and write-access settings, and SNMPv3 usernames continue to be saved in the running configuration file even when you enter the include-credentials command.

In addition, the following SNMPv3 security parameters are also saved:

snmpv3 user "<name>" [auth <md5|sha> "<auth-pass>"] [priv "<priv-pass>"]
Configuring Username and Password Security

Saving Security Credentials in a Config File

where:

\(<\text{name}>\) is the name of an SNMPv3 management station.

\([\text{auth} <\text{md5} | \text{sha}>]\) is the (optional) authentication method used for the management station.

\(<\text{auth-pass}>\) is the hashed authentication password used with the configured authentication method.

\([\text{priv} <\text{priv-pass}>]\) is the (optional) hashed privacy password used by a privacy protocol to encrypt SNMPv3 messages between the switch and the station.

The following example shows the additional security credentials for SNMPv3 users that can be saved in a running-config file:

```
smtpv3 user boris \\
auth md5 "9e4cfe901f21cf9d21079debeca453" \\
priv "82ca4dc998782d61a1e914f5d8f16824"

smtpv3 user alan \\
auth sha "8db602b8f293ed9bc00ac98cf9109708ecdf" \\
priv "5bc4313e9f6c7c2953a99a3a9406764fe8bb629a538"
```

Figure 2-6. Example of Security Credentials Saved in the Running-Config

Although you can enter an SNMPv3 authentication or privacy password in either clear ASCII text or the SHA-1 hash of the password, the password is displayed and saved in a configuration file only in hashed format, as shown in the preceding example.

For more information about the configuration of SNMP security parameters, refer to the chapter on “Configuring for Network Management Applications” in the Management and Configuration Guide for your switch.

TACACS+ Encryption Key Authentication

You can use TACACS+ servers to authenticate users who request access to a switch through Telnet (remote) or console (local) sessions. TACACS+ uses an authentication hierarchy consisting of:

- Remote passwords assigned in a TACACS+ server
- Local manager and operator passwords configured on the switch.

When you configure TACACS+, the switch first tries to contact a designated TACACS+ server for authentication services. If the switch fails to connect to any TACACS+ server, it defaults to its own locally assigned passwords for authentication control if it has been configured to do so.
Configuring Username and Password Security
Saving Security Credentials in a Config File

For improved security, you can configure a global or server-specific encryption key that encrypts data in TACACS+ packets transmitted between a switch and a RADIUS server during authentication sessions. The key configured on the switch must match the encryption key configured in each TACACS+ server application. (The encryption key is sometimes referred to as “shared secret” or “secret” key.) For more information, see “TACACS+ Authentication” on page 4-1 in this guide.

TACACS+ shared secret (encryption) keys can be saved in a configuration file by entering this command:

   HP Switch(config)# tacacs-server key <keystring>

The option <keystring> is the encryption key (in clear text) used for secure communication with all or a specific TACACS+ server.

RADIUS Shared-Secret Key Authentication

You can use RADIUS servers as the primary authentication method for users who request access to a switch through Telnet, SSH, WebAgent, console, or port-access (802.1X). The shared secret key is a text string used to encrypt data in RADIUS packets transmitted between a switch and a RADIUS server during authentication sessions. Both the switch and the server have a copy of the key; the key is never transmitted across the network. For more information, refer to “3. Configure the Switch To Access a RADIUS Server” on page 5-14 in this guide.

RADIUS shared secret (encryption) keys can be saved in a configuration file by entering this command:

   HP Switch(config)# radius-server key <keystring>

The option <keystring> is the encryption key (in clear text) used for secure communication with all or a specific RADIUS server.
Include-Credentials Radius-Tacacs-Only Option

This option allows you to execute include-credentials for only RADIUS and TACACS. The radius-tacacs-only option does not cause the switch to store authentication passwords and SSH keys in the configuration file.

Syntax:  

```
[no] include-credentials [radius-tacacs-only | store-in-config]
```

Enables the inclusion of passwords and security credentials in each configuration file when the file is saved onto a remote server or workstation.

When no include-credentials is executed, include-credentials is disabled. Credentials continue to be stored in the active and inactive configuration files but are not displayed.

radius-tacacs-only: When executed with the radius-tacacs-only option, only the RADIUS and TACACS security keys are included in the configuration when saving files remotely.

The radius-tacacs-only option can be disabled with either command:

```
no include-credentials
no include-credentials radius-tacacs-only
```

store-in-config: Stores passwords and SSH authorized keys in the configuration files. This happens automatically when include-credentials is enabled.

The no include-credentials store-in-config command disables include-credentials and removes credentials stored in the configuration files. The switch reverts to storing only a single set of passwords and SSH keys, regardless of which configuration file is booted.

When include-credentials radius-tacacs-only is executed, this warning message displays.
SSH Client Public-Key Authentication

Secure Shell version 2 (SSHv2) is used by HP switches to provide remote access to SSH-enabled management stations. Although SSH provides Telnet-like functions, unlike Telnet, SSH provides encrypted, two-way authenticated transactions. SSH client public-key authentication is one of the types of authentication used.

Client public-key authentication uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a public key stored on the switch can gain access at the manager or operator level. For more information about how to configure and use SSH public keys to authenticate SSH clients that try to connect to the switch, refer to “Configuring Secure Shell (SSH)” on page 7-1 in this guide.

The SSH security credential that is stored in the running configuration file is configured with the `ip ssh public-key` command used to authenticate SSH clients for manager or operator access, along with the hashed content of each SSH client public-key.

**Syntax:** `ip ssh public-key <manager | operator> keystring`

Set a key for public-key authentication.

- **manager:** allows manager-level access using SSH public-key authentication.
- **operator:** allows operator-level access using SSH public-key authentication.

---

Figure 2-7. Example of Caution Message Displayed for radius-tacacs-only Option
Configuring Username and Password Security
Saving Security Credentials in a Config File

**keystring:** A legal SSHv2 (RSA or DSA) public key. The text string for the public key must be a single quoted token. If the keystring contains double-quotes, it can be quoted with single quotes ("keystring"). The following restrictions for a keystring apply:

- A keystring cannot contain both single and double quotes.
- A keystring cannot have extra characters, such as a blank space or a new line. However, to improve readability, you can add a backslash at the end of each line.

---

**Note**

The `ip ssh public-key` command allows you to configure only one SSH client public-key at a time. The `ip ssh public-key` command behavior includes an implicit append that never overwrites existing public-key configurations on a running switch.

If you download a software configuration file that contains SSH client public-key configurations, the downloaded public-keys overwrite any existing keys, as happens with any other configured values.

---
Configuring Username and Password Security

Saving Security Credentials in a Config File

To display the SSH public-key configurations (72 characters per line) stored in a configuration file, enter the `show config` or `show running-config` command. The following example shows the SSH public keys configured for manager access, along with the hashed content of each SSH client public-key, that are stored in a configuration file:

![Example of SSH Public Keys](image)

```plaintext
... include-credentials
ip ssh public-key manager "ssh-dss \ EvYnTKxQ31bWvr/bT7W58NX/YJ1ZKTV22QJCicUUZVw1NFJCs@0v03XS4 \ BhkXjthHzg6D701otgizU006/Xzf4/J9XkJHk0CmbHIgtB1sbRYBxj3KZ4A \ klymvIaU09X5TDAAAAAPQCpwXnbwFTFpaXnxsvDvLSxa7wAAATABwuxUP \ pv2scqFPXQgthaTkwGgtqDFW/+K4xRsKAnIaxuG0qLbenehki+ND4TkK2d \ EeidDh7qHusBhOFXMI2g73Rpe2rNqKn5f/QV95kdNwW1bxuusBAzvfaJptd \ gca6yR4sSTuBcaKiorYj60kk144E1fDwieQx8zABQAAAEu7/1kV0dS \ G0vE0eJD23TLxnv94plXhrRKCfAvwYU+piG+Q1e1l1w92sMxPA1XJzSY \ imEp4pNWXEmc101pXMKnkhunuMMPaPMaQT8NJT6un6hqf/LdQ2qjJu1yV9 \ LWyLg5ybS1kFLeOt0ooZJbpy+U2e4jh2Bb7sX3G50= spock@sfc.gov" \ ip ssh public-key manager 'ssh-rsa \ AAAAB3NzaClcy2EAAADAQABAAAaqDy09RDD52JZP8k2F2YXubgwRANOR \ JRs1Eov6y1RK3xKmvgVatz1+mspiEmPS4wNK7bX/1oXmGrcGcEt8kx1ZQ \ ogCF5zs50PlnxnXvAdF5s5AwQdf4MhCqvtQCe1nt6Lxh42OfRg+yWqGQG \ M6H1eCULwXXSclp2Hysakw== "TectiaClientKey [1024-bit rsa, \ nobody@testmachine, Mon Aug 15 2005 14:47:34]"

ip ssh public-key manager "ssh-rsa \ AAAAB3NzaClcy2EAAADAQABAAAaqDy09RDD52JZP8k2F2YXubgwRANOR \ JRs1Eov6y1RK3xKmvgVatz1+mspiEmPS4wNK7bX/1oXmGrcGcEt8kx1ZQ \ ogCF5zs50PlnxnXvAdF5s5AwQdf4MhCqvtQCe1nt6Lxh42OfRg+yWqGQG \ M6H1eCULwXXSclp2Hysakw== "TectiaClientKey [1024-bit rsa, \ nobody@testmachine, Mon Aug 15 2005 14:47:34]"

ip ssh public-key manager "ssh-rsa \ AAAAB3NzaClcy2EAAADAQABAAAaqDy09RDD52JZP8k2F2YXubgwRANOR \ JRs1Eov6y1RK3xKmvgVatz1+mspiEmPS4wNK7bX/1oXmGrcGcEt8kx1ZQ \ ogCF5zs50PlnxnXvAdF5s5AwQdf4MhCqvtQCe1nt6Lxh42OfRg+yWqGQG \ M6H1eCULwXXSclp2Hysakw== "TectiaClientKey [1024-bit rsa, \ nobody@testmachine, Mon Aug 15 2005 14:47:34]"
```

Figure 2-8. Example of SSH Public Keys

If a switch configuration contains multiple SSH client public keys, each public key is saved as a separate entry in the configuration file. You can configure up to ten SSH client public-keys on a switch.
Displaying the Status of Include-Credentials on the Switch

The `show include-credentials` command provides the current status of include-credentials on the switch.

**Syntax:**

```
show include-credentials
```

Displays information about the passwords and SSH keys stored in the configuration.

- **Stored in Configuration - Yes:** The passwords and SSH keys are stored in the configuration. Include-credentials was executed.
- **Stored in Configuration - No:** There is only one set of operator/manager passwords and one set of SSH keys for the switch.
- **Enabled in Active Configuration:** Include-credentials is either enabled or disabled.
- **RADIUS/TACACS only:** Displayed when the option is configured.

```
HP Switch(config)# show include-credentials
Stored in Configuration : Yes
Enabled in Active Configuration : N/A
RADIUS/TACACS Only : Yes
```

**Figure 2-9. Example of Output for show include-credentials Command**
Storage States When Using Include-Credentials

The following table shows the states of several access types when the factory default settings are in effect or when include-credentials is enabled or not enabled.

<table>
<thead>
<tr>
<th>Type</th>
<th>Factory Default</th>
<th>Include-Credentials Enabled</th>
<th>Include-Credentials Disabled but Active</th>
<th>No Include-Credentials Executed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager/Operator Passwords &amp; port access</td>
<td>Single set for switch Stored outside config Not displayed in config file</td>
<td>One set per stored config Stored in config Displayed in config</td>
<td>Same as include-credentials enabled Not displayed in config</td>
<td>One set for switch No credentials displayed in config</td>
</tr>
<tr>
<td>SSH Public Key</td>
<td>One set for switch Stored in flash Not displayed in config</td>
<td>One set per stored config Stored in flash Displayed in config</td>
<td>Same as include-credentials enabled Not displayed in config</td>
<td>One set for switch No credentials displayed in config</td>
</tr>
<tr>
<td>SNMPv3 auth and priv</td>
<td>Stored in flash Not displayed in config</td>
<td>Stored in flash Displayed in config</td>
<td>Same as include-credentials enabled Not displayed in config</td>
<td>No credentials displayed in config</td>
</tr>
<tr>
<td>RADIUS &amp; TACACS keystings</td>
<td>Not displayed in config</td>
<td>Stored in flash Displayed in config</td>
<td>Same as include-credentials enabled Not displayed in config</td>
<td>No credentials displayed in config</td>
</tr>
</tbody>
</table>

**Note:** When no include-credentials store-in-config is executed, the switch is restored to its default state and only stores one set of operator/manager passwords and SSH keys.
Operating Notes

**Caution**

- When you first enter the `include-credentials` command to save the additional security credentials to the running configuration, these settings are moved from internal storage on the switch to the running-config file. You are prompted by a warning message to perform a `write memory` operation to save the security credentials to the startup configuration. The message reminds you that if you do not save the current values of these security settings from the running configuration, they will be lost the next time you boot the switch and will revert to the values stored in the startup configuration.

- When you boot a switch with a startup configuration file that contains the `include-credentials` command, any security credentials that are stored in internal flash memory are ignored and erased. The switch will load only the security settings in the startup configuration file.

- Security settings are no longer automatically saved internally in flash memory and loaded with the startup configuration when a switch boots up. The configuration of all security credentials requires that you use the `write memory` command to save them in the startup configuration in order for them to not be lost when you log off. A warning message reminds you to permanently save a security setting.

- After you enter the `include-credentials` command, the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys are saved in the running configuration. Use the `no include-credentials` command to disable the display and copying of these security parameters from the running configuration (using the `show running-config` and `copy running-config` commands), without disabling the configured security settings on the switch.

- After you enter the `include-credentials` command, you can toggle between the non-display and display of security credentials in `show` and `copy` command output by alternately entering the `no include-credentials` and `include-credentials` commands.

- After you permanently save security configurations to the current startup-config file using the `write memory` command, you can view and manage security settings with the following commands:
  - `show config`: Displays the configuration settings in the current startup-config file.
Configuring Username and Password Security
Saving Security Credentials in a Config File

- **copy config <source-filename> config <target-filename>:** Makes a local copy of an existing startup-config file by copying the contents of the startup-config file in one memory slot to a new startup-config file in another, empty memory slot.
- **copy config tftp:** Uploads a configuration file from the switch to a TFTP server.
- **copy tftp config:** Downloads a configuration file from a TFTP server to the switch.
- **copy config xmodem:** Uploads a configuration file from the switch to an Xmodem host.
- **copy xmodem config:** Downloads a configuration file from an Xmodem host to the switch.

For more information, see “Transferring Startup-Config Files To or From a Remote Server” in the Management and Configuration Guide.

- The switch can store up to three configuration files. Each configuration file contains its own security credentials and these security configurations may differ. It is the responsibility of the system administrator to ensure that the appropriate security credentials are contained in the configuration file that is loaded with each software image and that all security credentials in the file are supported.

- If you have already enabled the storage of security credentials (including local manager and operator passwords) by entering the `include-credentials` command, the `Reset-on-clear` option is disabled. When you press the Clear button on the front panel, the manager and operator usernames and passwords are deleted from the running configuration. However, the switch does not reboot after the local passwords are erased. (The `reset-on-clear` option normally reboots the switch when you press the Clear button.)

For more information about the `Reset-on-clear` option and other front-panel security features, see “Configuring Front-Panel Security” on page 2-35 in this guide.
Restrictions

The following restrictions apply when you enable security credentials to be stored in the running configuration with the `include-credentials` command:

- The private keys of an SSH host cannot be stored in the running configuration. Only the public keys used to authenticate SSH clients can be stored. An SSH host’s private key is only stored internally, for example, on the switch or on an SSH client device.

- SNMPv3 security credentials saved to a configuration file on a switch cannot be used after downloading the file on a different switch. The SNMPv3 security parameters in the file are only supported when loaded on the same switch for which they were configured. This is because when SNMPv3 security credentials are saved to a configuration file, they are saved with the engine ID of the switch as shown here:

```
snmpv3 engine-id 00:00:00:0b:00:00:08:00:09:01:10:01
```

If you download a configuration file with saved SNMPv3 security credentials on a switch, when the switch loads the file with the current software version the SNMPv3 engine ID value in the downloaded file must match the engine ID of the switch in order for the SNMPv3 users to be configured with the authentication and privacy passwords in the file. (To display the engine ID of a switch, enter the `show snmpv3 engine-id` command. To configure authentication and privacy passwords for SNMPv3 users, enter the `snmpv3 user` command.)

If the engine ID in the saved SNMPv3 security settings in a downloaded configuration file does not match the engine ID of the switch:

- The SNMPv3 users are configured, but without the authentication and privacy passwords. You must manually configure these passwords on the switch before the users can have SNMPv3 access with the privileges you want.

- Only the `snmpv3 user <user_name>` credentials from the SNMPv3 settings in a downloaded configuration file are loaded on the switch, for example:

```
snmpv3 user boris
snmpv3 user alan
```

- You can store 802.1X authenticator (port-access) credentials in a configuration file. However, 802.1X supplicant credentials cannot be stored.
Encrypting Credentials in the Configuration File

Overview

A security risk is present when credentials used for authentication to remote devices such as RADIUS or TACACS+ servers are displayed in the configuration file in plain text. The encrypt-credentials command allows the storing, displaying, and transferring of credentials in encrypted form.

When the encrypt-credentials feature is enabled, the affected credentials will be encrypted using aes-256-cbc encryption. By default, a fixed, hard-coded 256-bit key that is common to all HP networking devices is used. This allows transfer of configurations with all relevant credentials and provides much more security than plaintext passwords in the configuration.

Additionally, you can set a separate, 256-bit pre-shared key, however, you must now set the pre-shared key on the destination device before transferring the configuration. The pre-shared key on the destination device must be identical to the pre-shared key on the source device or the affected security credentials will not be usable. This key is only accessible using the CLI, and is not visible in any file transfers.

Note

It is expected that plaintext passwords will continue to be used for configuring the switch. The encrypted credentials option is available primarily for the backup and restore of configurations.

Only the aes-256-cbc encryption type is available.
Enabling Encrypt-Credentials

To enable encrypt-credentials, enter this command.

**Syntax:**  
[no] encrypt-credentials [pre-shared-key <plaintext | hex>]

When encrypt-credentials is enabled without any parameters, it enables the encryption of relevant security parameters in the configuration.

The no form of the command disables the encrypt-credentials feature. If specified with pre-shared-key option, clears the pre-shared-key used to encrypt credentials.

pre-shared-key: When specified, sets the pre-shared-key that is used for all AES encryption. If no key is set, an HP switch default AES key is used.

Default: HP switch default AES key

plaintext: Set the key using plaintext.

hex: Set the key as a 64 hexadecimal character string (32 bytes). You must enter 64 hexadecimal digits to set this key.

When encrypt-credentials is enabled without any parameters, a caution message displays advising you about the effect of the feature with prior software versions, and actions that are recommended. All versions of the command force a configuration save after encrypting or re-encrypting sensitive data in the configuration.
Configuring Username and Password Security
Encrypting Credentials in the Configuration File

Configuring Username and Password Security
Encrypting Credentials in the Configuration File

Configuring Username and Password Security
Encrypting Credentials in the Configuration File

Configuring Username and Password Security
Encrypting Credentials in the Configuration File

Configuring Username and Password Security
Encrypting Credentials in the Configuration File

Configuring Username and Password Security
Encrypting Credentials in the Configuration File

Configuring Username and Password Security
Encrypting Credentials in the Configuration File

Configuring Username and Password Security
Encrypting Credentials in the Configuration File

Displaying the State of Encrypt-Credentials

To display whether encrypt-credentials is enabled or disabled, enter the show encrypt-credentials command. This command is available only from the manager context.
Configuring Username and Password Security
Encrypting Credentials in the Configuration File

<table>
<thead>
<tr>
<th>Existing Command</th>
<th>New Equivalent Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Switch(config)# radius-server key secret1</td>
<td>HP Switch(config)# radius-server encrypted-key</td>
</tr>
<tr>
<td></td>
<td>U2FsdGVkX18XWadTeFN+bhxKA/q+s5cV1NiYyx+TuA=</td>
</tr>
<tr>
<td>HP Switch(config)# radius-server host 10.0.0.1 key secret1</td>
<td>HP Switch(config)# radius-server host 10.0.0.1</td>
</tr>
<tr>
<td></td>
<td>encrypted-key</td>
</tr>
<tr>
<td></td>
<td>U2FsdGVkX18XWadTeFN+bhxKA/q+s5cV1NiYyx+TuA=</td>
</tr>
<tr>
<td>HP Switch(config)# tacacs-server key secret1</td>
<td>HP Switch(config)# tacacs-server encrypted-key</td>
</tr>
<tr>
<td></td>
<td>U2FsdGVkX18XWadTeFN+bhxKA/q+s5cV1NiYyx+TuA=</td>
</tr>
<tr>
<td>HP Switch(config)# tacacs-server host 10.0.0.1 key secret1</td>
<td>HP Switch(config)# tacacs-server host 10.0.0.1</td>
</tr>
<tr>
<td></td>
<td>encrypted-key</td>
</tr>
<tr>
<td></td>
<td>U2FsdGVkX18XWadTeFN+bhxKA/q+s5cV1NiYyx+TuA=</td>
</tr>
<tr>
<td>HP Switch(config)# key-chain example key 1 key-string secret1</td>
<td>HP Switch(config)# key-chain example key 1 encrypted-key</td>
</tr>
<tr>
<td></td>
<td>U2FsdGVkX18XWadTeFN+bhxKA/q+s5cV1NiYyx+TuA=</td>
</tr>
<tr>
<td>HP Switch(config)# aaa port-access supplicant 24 secret secret1</td>
<td>HP Switch(config)# aaa port-access supplicant 24 identity id1 encrypted-secret secret1</td>
</tr>
<tr>
<td></td>
<td>U2FsdGVkX18XWadTeFN+bhxKA/q+s5cV1NiYyx+TuA=</td>
</tr>
<tr>
<td>HP Switch(config)# snntp authentication key-id 33 authentication-mode md5 key-value secret1</td>
<td>HP Switch(config)# snntp authentication key-id 33 authentication-mode md5 encrypted-key</td>
</tr>
<tr>
<td></td>
<td>U2FsdGVkX18XWadTeFN+bhxKA/q+s5cV1NiYyx+TuA=</td>
</tr>
<tr>
<td>HP Switch(config)# password manager plaintext secret1</td>
<td>HP Switch(config)# encrypted-password manager</td>
</tr>
<tr>
<td></td>
<td>U2FsdGVkX18XWadTeFN+bhxKA/q+s5cV1NiYyx+TuA=</td>
</tr>
</tbody>
</table>

Several commands will have encryption available for configuration.

Affected Commands

Figure 2-13. Example of Status of Encrypt-Credentials when the pre-shared-key Has Not Been Set

Figure 2-14. Example of Status of Encrypt-Credentials When the Pre-shared Key Has Been Set
Important Operating Notes

- If you load a prior software version that does not contain the encrypt-credentials feature, it is important to back up the configuration and then execute the `erase startup` command on the switch. Features that have encrypted parameters configured will not work until those parameters are cleared and reconfigured.

- HP recommends that when executing an “encrypted-<option>” command, you copy and paste the encrypted parameter from a known encrypted password that has been generated on the same switch or another switch with the same pre-shared key (whether user-specified or a default key). If an incorrectly encrypted parameter is used, it is highly likely that the decrypted version will contain incorrect characters, and neither key will function correctly or be displayed in any `show` command.

Interaction with Include-Credentials Settings

The following table shows the interaction between `include-credentials` settings and `encrypt-credentials` settings when displaying or transferring the configuration.

<table>
<thead>
<tr>
<th>Include-Credentials Active</th>
<th>Include-Credentials Enabled</th>
<th>Encrypt-Credentials Enabled</th>
<th>Resulting Behavior for Sensitive Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Hidden (default)</td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Shown, encrypted</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td>Hidden</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Shown, encrypted</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Shown, plaintext</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Shown, encrypted</td>
<td></td>
</tr>
</tbody>
</table>
Front-Panel Security

The front-panel security features provide the ability to independently enable or disable some of the functions of the two buttons located on the front of the switch for clearing the password (Clear button) or restoring the switch to its factory default configuration (Reset+Clear buttons together). The ability to disable Password Recovery is also provided for situations which require a higher level of switch security.

The front-panel Security features are designed to prevent malicious users from:
- Resetting the password(s) by pressing the Clear button
- Restoring the factory default configuration by using the Reset+Clear button combination.
- Gaining management access to the switch by having physical access to the switch itself

When Security Is Important

Some customers require a high level of security for information. Also, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires that systems handling and transmitting confidential medical records must be secure.

It used to be assumed that only system and network administrators would be able to get access to a network switch because switches were typically placed in secure locations under lock and key. For some customers this is no longer true. Others simply want the added assurance that even if someone did manage to get to the switch that data would still remain secure.

If you do not invoke front-panel security on the switch, user-defined passwords can be deleted by pushing the Clear button on the front panel. This function exists so that if customers forget the defined passwords they can still get back into the switch and reset the passwords. This does, however, leave the switch vulnerable when it is located in an area where non-authorized people have access to it. Passwords could easily be cleared by pressing the Clear button. Someone who has physical access to the switch may be able to erase the passwords (and possibly configure new passwords) and take control of the switch.
As a result of increased security concerns, customers now have the ability to stop someone from removing passwords by disabling the Clear and/or Reset buttons on the front of the switch.

Front-Panel Button Functions

Clear Button

Pressing the Clear button alone for one second resets the password(s) configured on the switch.

![Figure 2-15. Press the Clear Button for One Second To Reset the Password(s)](image)

Reset Button

Pressing the Reset button alone for one second causes the switch to reboot.

![Figure 2-16. Press and hold the Reset Button for One Second To Reboot the Switch](image)

Restoring the Factory Default Configuration

You can also use the Reset button together with the Clear button (Reset+Clear) to **restore the factory default configuration** for the switch. To do this:

1. Press and hold the Reset button.
Configuring Username and Password Security

Front-Panel Security

2. While holding the Reset button, press and hold the Clear button.

3. Release the Reset button.

4. When the Test LED to the right of the Clear button begins flashing, release the Clear button.
It can take approximately 20-25 seconds for the switch to reboot. This process restores the switch configuration to the factory default settings.

Configuring Front-Panel Security

Using the `front-panel-security` command from the global configuration context in the CLI you can:

- Disable or re-enable the password-clearing function of the Clear button. Disabling the Clear button means that pressing it does not remove local password protection from the switch. (This action affects the Clear button when used alone, but does not affect the operation of the Reset+Clear combination described under “Restoring the Factory Default Configuration” on page 2-33.)

- Configure the Clear button to reboot the switch after clearing any local usernames and passwords. This provides an immediate, visual means (plus an Event Log message) for verifying that any usernames and passwords in the switch have been cleared.

- Modify the operation of the Reset+Clear combination (page 2-33) so that the switch still reboots, but does not restore the switch’s factory default configuration settings. (Use of the Reset button alone, to simply reboot the switch, is not affected.)

- Disable or re-enable Password Recovery.
Syntax: show front-panel-security

Displays the current front-panel-security settings:

Clear Password: Shows the status of the Clear button on the front panel of the switch. Enabled means that pressing the Clear button erases the local usernames and passwords configured on the switch (and thus removes local password protection from the switch). Disabled means that pressing the Clear button does not remove the local usernames and passwords configured on the switch. (Default: Enabled.)

Reset-on-clear: Shows the status of the reset-on-clear option (Enabled or Disabled). When reset-on-clear is disabled and Clear Password is enabled, then pressing the Clear button erases the local usernames and passwords from the switch. When reset-on-clear is enabled, pressing the Clear button erases the local usernames and passwords from the switch and reboots the switch. (Enabling reset-on-clear automatically enables clear-password.) (Default: Disabled.)

Note: If you have stored security credentials (including the local manager and operator usernames and passwords) to the running config file by entering the include-credentials command, the Reset-on-clear option is ignored. If you press the Clear button on the front panel, the manager and operator usernames and passwords are deleted from the startup configuration file, but the switch does not reboot. For more information about storing security credentials, see “Saving Security Credentials in a Config File” on page 2-10 in this guide.

Factory Reset: Shows the status of the System Reset button on the front panel of the switch. Enabled means that pressing the System Reset button reboots the switch and also enables the System Reset button to be used with the Clear button (page 2-33) to reset the switch to its factory-default configuration. (Default: Enabled.)
Password Recovery: Shows whether the switch is configured with the ability to recover a lost password. (Refer to “Password Recovery Process” on page 2-44.) (Default: Enabled.)

CAUTION: Disabling this option removes the ability to recover a password on the switch. Disabling this option is an extreme measure and is not recommended unless you have the most urgent need for high security. If you disable password-recovery and then lose the password, you will have to use the Reset and Clear buttons (page 2-33) to reset the switch to its factory-default configuration and create a new password.

For example, show front-panel-security produces the following output when the switch is configured with the default front-panel security settings.

```
HP Switch(config)# show front-panel-security
Clear Password        - Enabled
Reset-on-clear      - Disabled
Factory Reset         - Enabled
Password Recovery     - Enabled
```

Figure 2-17. The Default Front-Panel Security Settings
Disabling the Clear Password Function of the Clear Button

**Syntax:** no front-panel-security password-clear

_In the factory-default configuration, pressing the Clear button on the switch's front panel erases any local usernames and passwords configured on the switch. This command disables the password clear function of the Clear button, so that pressing it has no effect on any local usernames and passwords. For redundant management systems, this command only affects the active management module._

(_Default: Enabled._)

**Note:** Although the Clear button does not erase passwords when disabled, you can still use it with the Reset button (Reset+Clear) to restore the switch to its factory default configuration, as described under “Restoring the Factory Default Configuration” on page 2-33.

This command displays a Caution message in the CLI. If you want to proceed with disabling the Clear button, type [Y]; otherwise type [N]. For example:

```
HP Switch(config)# no front-panel-security password-clear
**** CAUTION ****
Disabling the clear button prevents switch passwords from being easily reset or recovered. Ensure that you are familiar with the front panel security options before proceeding.

Continue with disabling the clear button [y/n]? y
```

```
HP Switch(config)# show front-panel-security
Clear Password - Disabled
Factory Reset    - Enabled
Password Recovery- Enabled
```

_Indicates the command has disabled the Clear button on the switch’s front panel. In this case the Show command does not include the reset-on-clear status because it is inoperable while the Clear Password functionality is disabled, and must be reconfigured whenever Clear Password is re-enabled._

_Figure 2-18. Example of Disabling the Clear Button and Displaying the New Configuration_
Re-Enabling the Clear Button and Setting or Changing the “Reset-On-Clear” Operation

**Syntax:**  
[no] front-panel-security password-clear reset-on-clear

This command does both of the following:
- Re-enables the password-clearing function of the Clear button on the switch’s front panel.
- Specifies whether the switch reboots if the Clear button is pressed.

To re-enable password-clear, you must also specify whether to enable or disable the `reset-on-clear` option.

**Defaults:**
- `password-clear`: *Enabled*.
- `reset-on-clear`: *Disabled*.

Thus:
- To enable password-clear with reset-on-clear disabled, use this syntax:
  ```
  no front-panel-security password-clear reset-on-clear
  ```
- To enable password-clear with reset-on-clear also enabled, use this syntax:
  ```
  front-panel-security password-clear reset-on-clear
  ```

(Either form of the command enables `password-clear`.)

For redundant management systems, this command only affects the active management module.

**Note:** If you disable `password-clear` and also disable the `password-recovery` option, you can still recover from a lost password by using the Reset+Clear button combination at reboot as described on page 2-33. Although the Clear button does not erase passwords when disabled, you can still use it with the Reset button (Reset+Clear) to restore the switch to its factory default configuration. You can then get access to the switch to set a new password.

For example, suppose that `password-clear` is disabled and you want to restore it to its default configuration (enabled, with `reset-on-clear` disabled).
Configuring Username and Password Security

Front-Panel Security

Changing the Operation of the Reset+Clear Combination

In their default configuration, using the Reset+Clear buttons in the combination described under “Restoring the Factory Default Configuration” on page 2-33 replaces the switch’s current startup-config file with the factory-default startup-config file, then reboots the switch, and removes local password protection. This means that anyone who has physical access to the switch could use this button combination to replace the switch’s current configuration with the factory-default configuration, and render the switch accessible without the need to input a username or password. You can use the factory-reset command to prevent the Reset+Clear combination from being used for this purpose.
Syntax: [no] front-panel-security factory-reset

Disables or re-enables the following functions associated with using the Reset+Clear buttons in the combination described under “Restoring the Factory Default Configuration” on page 2-33:

- Replacing the current startup-config file with the factory-default startup-config file
- Clearing any local usernames and passwords configured on the switch

(Default: Both functions enabled.)

For redundant management systems, this command only affects the active management module.

Notes: The Reset+Clear button combination always reboots the switch, regardless of whether the “no” form of the command has been used to disable the above two functions. Also, if you disable factory-reset, you cannot disable the password-recovery option, and the reverse.

```
HP Switch(config)# no front-panel-security factory-reset

**** CAUTION ****
Disabling the factory reset option prevents switch configuration and passwords from being easily reset or recovered. Ensure that you are familiar with the front panel security options before proceeding.

Continue with disabling the factory reset option[y/n]? y
```

HP Switch(config)# show front-panel-security

Clear Password    - Enabled
Reset-on-clear   - Disabled
Factory Reset     - Disabled
Password Recovery - Enabled

The command to disable the factory-reset operation produces this caution. To complete the command, press [Y]. To abort the command, press [N].

Completes the command to disable the factory reset option.

Displays the current front-panel-security configuration, with Factory Reset disabled.

Figure 2-20. Example of Disabling the Factory Reset Option
Password Recovery

The password recovery feature is enabled by default and provides a method for regaining management access to the switch (without resetting the switch to its factory default configuration) in the event that the system administrator loses the local manager username (if configured) or password. Using Password Recovery requires:

- **password-recovery** enabled (the default) on the switch prior to an attempt to recover from a lost username/password situation
- Contacting your HP Customer Care Center to acquire a one-time-use password

Disabling or Re-Enabling the Password Recovery Process

Disabling the password recovery process means that the only method for recovering from a lost manager username (if configured) and password is to reset the switch to its factory-default configuration, which removes any non-default configuration settings.
Disabling **password-recovery** requires that **factory-reset** be enabled, and locks out the ability to recover a lost manager username (if configured) and password on the switch. In this event, there is no way to recover from a lost manager username/password situation without resetting the switch to its factory-default configuration. This can disrupt network operation and make it necessary to temporarily disconnect the switch from the network to prevent unauthorized access and other problems while it is being reconfigured. Also, with **factory-reset** enabled, unauthorized users can use the Reset+Clear button combination to reset the switch to factory-default configuration and gain management access to the switch.

**Syntax:**  
```
[no] front-panel-security password-recovery
```

*Enables or (using the “no” form of the command) disables the ability to recover a lost password.*

*When this feature is enabled, the switch allows management access through the password recovery process described below. This provides a method for recovering from a lost manager username (if configured) and password. When this feature is disabled, the password recovery process is disabled and the only way to regain management access to the switch is to use the Reset+Clear button combination (page 2-33) to restore the switch to its factory default configuration.*

**Note:** To disable **password-recovery**:

- You must have physical access to the front panel of the switch.
- The **factory-reset** parameter must be enabled (the default).

*For redundant management systems, this command only affects the active management module.*

*(Default: Enabled.)*

**Steps for Disabling Password-Recovery.**

1. Set the CLI to the global interface context.
2. Use **show front-panel-security** to determine whether the factory-reset parameter is enabled. If it is disabled, use the **front-panel-security factory-reset** command to enable it.
3. Press and release the Clear button on the front panel of the switch.
4. Within 60-seconds of pressing the Clear button, enter the following command:

   ```
   no front-panel-security password-recovery
   ```
Configuring Username and Password Security

Password Recovery

5. Do one of the following after the “CAUTION” message appears:
   - If you want to complete the command, press [Y] (for “Yes”).
   - If you want to abort the command, press [N] (for “No”)

   Figure 2-21 shows an example of disabling the password-recovery parameter.

   ```
   HP Switch(config)# no front-panel-security password-recovery
   **** CAUTION ****
   Disabling the clear button without password recovery prevents switch passwords from being reset. If the switch password is lost, restoring the default factory configuration will be required to regain access!
   Continue with disabling password recovery [y/n]? y
   HP Switch(config)#
   ```

   **Figure 2-21. Example of the Steps for Disabling Password-Recovery**

Password Recovery Process

If you have lost the switch’s manager username/password, but password-recovery is enabled, then you can use the Password Recovery Process to gain management access to the switch with an alternate password supplied by HP.

**Note**

If you have disabled password-recovery, which locks out the ability to recover a manager username/password pair on the switch, then the only way to recover from a lost manager username/password pair is to use the Reset+Clear button combination described under “Restoring the Factory Default Configuration” on page 2-33. This can disrupt network operation and make it necessary to temporarily disconnect the switch from the network to prevent unauthorized access and other problems while it is being reconfigured.

To use the password-recovery option to recover a lost password:

1. Note the switch’s base MAC address. It is shown on the label located on the upper right front corner of the switch.

2. Contact your HP Customer Care Center for further assistance. Using the switch’s MAC address, the HP Customer Care Center will generate and provide a “one-time use” alternate password you can use with the to gain management access to the switch. Once you gain access, you can configure a new, known password.
The alternate password provided by the HP Customer Care Center is valid only for a single login attempt. You cannot use the same “one-time-use” password if you lose the password a second time. Because the password algorithm is randomized based upon your switch's MAC address, the password will change as soon as you use the “one-time-use” password provided to you by the HP Customer Care Center.
Configuring Username and Password Security
Password Recovery
Web and MAC Authentication

Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Web Authentication</td>
<td>n/a</td>
<td>—</td>
<td>3-18</td>
<td>—</td>
</tr>
<tr>
<td>Configure MAC Authentication</td>
<td>n/a</td>
<td>—</td>
<td>3-31</td>
<td>—</td>
</tr>
<tr>
<td>Display Web Authentication Status and Config</td>
<td>n/a</td>
<td>—</td>
<td>3-25</td>
<td>—</td>
</tr>
<tr>
<td>Display MAC Authentication Status and Config</td>
<td>n/a</td>
<td>—</td>
<td>3-42</td>
<td>—</td>
</tr>
</tbody>
</table>

Web and MAC authentication are designed for employment on the “edge” of a network to provide port-based security measures for protecting private networks and a switch from unauthorized access. Because neither method requires clients to run special supplicant software (unlike 802.1X authentication), both Web and MAC authentication are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option. Only a web browser (for Web authentication) or a MAC address (for MAC authentication) is required.

Both Web and MAC authentication methods rely on a RADIUS server to authenticate network access. This simplifies access security management by allowing you to control access from a master database in a single server. (You can use up to three RADIUS servers to provide backups in case access to the primary server fails.) It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN.

On a port configured for Web or MAC Authentication, the switch operates as a port-access authenticator using a RADIUS server and the CHAP protocol. Inbound traffic is processed by the switch alone, until authentication occurs. Some traffic from the switch to an unauthorized client is supported (for example, broadcast or unknown destination packets) before authentication occurs.
Web and MAC Authentication

Overview

Web Authentication

The Web Authentication (Web-Auth) method uses a web page login to authenticate users for access to the network. When a client connects to the switch and opens a web browser, the switch automatically presents a login page.

**Note**

A proxy server is not supported for use by a browser on a client device that accesses the network through a port configured for web authentication.

- In the login page, a client enters a username and password, which the switch forwards to a RADIUS server for authentication. After authenticating a client, the switch grants access to the secured network. Besides a web browser, the client needs no special supplicant software.

MAC Authentication

The MAC Authentication (MAC-Auth) method grants access to a secure network by authenticating devices for access to the network. When a device connects to the switch, either by direct link or through the network, the switch forwards the device’s MAC address to the RADIUS server for authentication. The RADIUS server uses the device MAC address as the username and password, and grants or denies network access in the same way that it does for clients capable of interactive logons. (The process does not use either a client device configuration or a logon session.) MAC authentication is well-suited for clients that are not capable of providing interactive logons, such as telephones, printers, and wireless access points. Also, because most RADIUS servers allow for authentication to depend on the source switch and port through which the client connects to the network, you can use MAC-Auth to “lock” a particular device to a specific switch and port.

**Note**

802.1X port-access, Web authentication, and MAC authentication can be configured at the same time on the same port. A maximum of 32 clients is supported on the port. (The default is one client.)

Web and/or MAC authentication and MAC lockdown, MAC lockout, and port-security are mutually exclusive on a given port. If you configure any of these authentication methods on a port, you must disable LACP on the port.
Concurrent Web and MAC Authentication

Web authentication and MAC authentication can be configured at the same time on a port. It is assumed that MAC authentication will use an existing MAC address. The following conditions apply for concurrent Web and MAC authentication:

- A specific MAC address cannot be authenticated by both Web and MAC authentication at the same time.
- Each new Web/MAC Auth client always initiates a MAC authentication attempt. This same client can also initiate Web authentication at any time before the MAC authentication succeeds. If either authentication succeeds then the other authentication (if in progress) is ended. No further Web/MAC authentication attempts are allowed until the client is deauthenticated.
- Web and MAC authentications are not allowed on the same port if unauthenticated VLAN (that is, a guest VLAN) is enabled for MAC authentication. An unauthenticated VLAN can’t be enabled for MAC authentication if Web and MAC authentication are both enabled on the port.
- Hitless reauthentication must be of the same type (MAC) that was used for the initial authentication. Non-hitless reauthentication can be of any type.

The remaining Web/MAC functionality, including interactions with 802.1X, remains the same. Web and MAC authentication can be used for different clients on the same port.

Normally, MAC authentication finishes much sooner than Web authentication. However, if Web authentication should complete first, MAC authentication will cease even though it is possible that MAC authentication could succeed. There is no guarantee that MAC authentication ends before Web authentication begins for the client.

Concurrent Web and MAC authentication is backward compatible with all existing user configurations.

Authorized and Unauthorized Client VLANs

Web-Auth and MAC-Auth provide a port-based solution in which a port belongs to one, untagged VLAN at a time. The switch supports up to 32 simultaneous client sessions per port. All authenticated client sessions operate in the same untagged VLAN. (If you want the switch to simultaneously...
support multiple client sessions in different VLANs for a network application, design your system so that clients request network access on different switch ports.)

In the default configuration, the switch blocks access to all clients that the RADIUS server does not authenticate. However, you can configure an individual port to provide limited network services and access to unauthorized clients by using an “unauthorized” VLAN for each session. The unauthorized VLAN ID assignment can be the same for all ports, or different, depending on the services and access you plan to allow for unauthenticated clients.

You configure access to an optional, unauthorized VLAN when you configure Web and MAC authentication on a port.

RADIUS-Based Authentication

In Web and MAC authentication, you use a RADIUS server to temporarily assign a port to a static VLAN to support an authenticated client. When a RADIUS server authenticates a client, the switch-port membership during the client’s connection is determined according to the following hierarchy:

1. A RADIUS-assigned VLAN
2. An authorized VLAN specified in the Web- or MAC-Auth configuration for the subject port.
3. A static, port-based, untagged VLAN to which the port is configured. A RADIUS-assigned VLAN has priority over switch-port membership in any VLAN.

Wireless Clients

You can allow wireless clients to move between switch ports under Web/MAC Authentication control. Clients may move from one Web-authorized port to another or from one MAC-authorized port to another. This capability allows wireless clients to move from one access point to another without having to reauthenticate.
How Web and MAC Authentication Operate

Before gaining access to the network, a client first presents authentication credentials to the switch. The switch then verifies the credentials with a RADIUS authentication server. Successfully authenticated clients receive access to the network, as defined by the System Administrator. Clients who fail to authenticate successfully receive no network access or limited network access as defined by the System Administrator.

Web-based Authentication

When a client connects to a Web-Auth enabled port, communication is redirected to the switch. A temporary IP address is assigned by the switch and a login screen is presented for the client to enter their username and password.

The default User Login screen is shown in Figure 3-1.

![User Login Screen](image)

**Figure 3-1. Example of Default User Login Screen**

When a client connects to the switch, it sends a DHCP request to receive an IP address to connect to the network. To avoid address conflicts in a secure network, you can specify a temporary IP address pool to be used by DHCP by configuring the `dhcp-addr` and `dhcp-lease` options when you enable web authentication with the `aaa port-access web-based` command.

The Secure Socket Layer (SSLv3/TLSv1) feature provides remote web access to the network via authenticated transactions and encrypted paths between the switch and management station clients capable of SSL/TLS. If you have
Web and MAC Authentication
How Web and MAC Authentication Operate

enabled SSL on the switch, you can specify the `ssl-login` option when you configure web authentication so that clients who log in to specified ports are redirected to a secure login page (https://...) to enter their credentials.

The switch passes the supplied username and password to the RADIUS server for authentication and displays the following progress message:

**Authenticating...**
Please wait while your credentials are verified.

![Figure 3-2. Progress Message During Authentication](image)

If the client is authenticated and the maximum number of clients allowed on the port (`client-limit`) has not been reached, the port is assigned to a static, untagged VLAN for network access. After a successful login, a client may be redirected to a URL if you specify a URL value (`redirect-url`) when you configure web authentication.

**Access Granted**
You have been authenticated. Please wait while network connection refreshes itself.

![Figure 3-3. Authentication Completed](image)

The assigned VLAN is determined, in order of priority, as follows:

1. If there is a RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to this VLAN and temporarily drops all other VLAN memberships.

2. If there is no RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to the authorized VLAN (`auth-vid` if configured) and temporarily drops all other VLAN memberships.

3. If neither 1 or 2, above, apply, but the port is an untagged member of a statically configured, port-based VLAN, then the port remains in this VLAN.

4. If neither 1, 2, or 3, above, apply, then the client session does not have access to any statically configured, untagged VLANs and client access is blocked.
Web and MAC Authentication
How Web and MAC Authentication Operate

The assigned port VLAN remains in place until the session ends. Clients may be forced to reauthenticate after a fixed period of time (\texttt{reauth-period}) or at any time during a session (\texttt{reauthenticate}). An implicit logoff period can be set if there is no activity from the client after a given amount of time (\texttt{logoff-period}). In addition, a session ends if the link on the port is lost, requiring reauthentication of all clients. Also, if a client moves from one port to another and client moves have not been enabled (\texttt{client-moves}) on the ports, the session ends and the client must reauthenticate for network access. At the end of the session the port returns to its pre-authentication state. Any changes to the port’s VLAN memberships made while it is an authorized port take affect at the end of the session.

A client may not be authenticated due to invalid credentials or a RADIUS server timeout. The \texttt{max-retries} parameter specifies how many times a client may enter their credentials before authentication fails. The \texttt{server-timeout} parameter sets how long the switch waits to receive a response from the RADIUS server before timing out. The \texttt{max-requests} parameter specifies how many authentication attempts may result in a RADIUS server timeout before authentication fails. The switch waits a specified amount of time (\texttt{quiet-period}) before processing any new authentication requests from the client.

Network administrators may assign unauthenticated clients to a specific static, untagged VLAN (\texttt{unauth-vid}), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients the port is blocked and no network access is available. Should another client successfully authenticate through that port any unauthenticated clients on the \texttt{unauth-vid} are dropped from the port.

MAC-based Authentication

When a client connects to a MAC-Auth enabled port traffic is blocked. The switch immediately submits the client’s MAC address (in the format specified by the \texttt{addr-format}) as its certification credentials to the RADIUS server for authentication.

If the client is authenticated and the maximum number of MAC addresses allowed on the port (\texttt{addr-limit}) has not been reached, the port is assigned to a static, untagged VLAN for network access.

The assigned VLAN is determined, in order of priority, as follows:

1. If there is a RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to this VLAN and temporarily drops all other VLAN memberships.
2. If there is no RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to the Authorized VLAN (auth-vid if configured) and temporarily drops all other VLAN memberships.

3. If neither 1 or 2, above, apply, but the port is an untagged member of a statically configured, port-based VLAN, then the port remains in this VLAN.

4. If neither 1, 2, or 3, above, apply, then the client session does not have access to any statically configured, untagged VLANs and client access is blocked.

The assigned port VLAN remains in place until the session ends. Clients may be forced to reauthenticate after a fixed period of time (reauth-period) or at any time during a session (reauthenticate). An implicit logoff period can be set if there is no activity from the client after a given amount of time (logoff-period). In addition, a session ends if the link on the port is lost, requiring reauthentication of all clients. Also, if a client moves from one port to another and client moves have not been enabled (addr-moves) on the ports, the session ends and the client must reauthenticate for network access. At the end of the session the port returns to its pre-authentication state. Any changes to the port’s VLAN memberships made while it is an authenticated port take affect at the end of the session.

A client may not be authenticated due to invalid credentials or a RADIUS server timeout. The server-timeout parameter sets how long the switch waits to receive a response from the RADIUS server before timing out. The max-requests parameter specifies how many authentication attempts may result in a RADIUS server timeout before authentication fails. The switch waits a specified amount of time (quiet-period) before processing any new authentication requests from the client.

Network administrators may assign unauthenticated clients to a specific static, untagged VLAN (unauth-vid), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients the port remains in its original VLAN configuration. Should another client successfully authenticate through that port any unauthenticated clients are dropped from the port.
Terminology

**Authorized-Client VLAN:** Like the Unauthorized-Client VLAN, this is a conventional, static, untagged, port-based VLAN previously configured on the switch by the System Administrator. The intent in using this VLAN is to provide authenticated clients with network access and services. When the client connection terminates, the port drops its membership in this VLAN.

**Authentication Server:** The entity providing an authentication service to the switch. In the case of a HP Switch 8212zl running Web/MAC-Authentication, this is a RADIUS server.

**Authenticator:** In HP switch applications, a device such as a HP Switch 8212zl that requires a client or device to provide the proper credentials (MAC address, or username and password) before being allowed access to the network.

**CHAP:** Challenge Handshake Authentication Protocol. Also known as “CHAP-RADIUS”.

**Client:** In this application, an end-node device such as a management station, workstation, or mobile PC linked to the switch through a point-to-point LAN link.

**Redirect URL:** A System Administrator-specified web page presented to an authorized client following Web Authentication. HP recommends specifying this URL when configuring Web Authentication on a switch. Refer to `aaa port-access web-based [e] < port-list > [redirect-url < url >]` on page 3-24.

**Static VLAN:** A VLAN that has been configured as “permanent” on the switch by using the CLI `vlan < vid >` command or the Menu interface.

**Unauthorized-Client VLAN:** A conventional, static, untagged, port-based VLAN previously configured on the switch by the System Administrator. It is used to provide limited network access and services to clients who are not authenticated.
Operating Rules and Notes

- The switch supports concurrent 802.1X, Web and MAC authentication operation on a port (with up to 2 clients allowed). However, concurrent operation of Web and MAC authentication with other types of authentication on the same port is not supported. That is, the following authentication types are mutually exclusive on a given port:
  - Web and/or MAC Authentication (with or without 802.1X)
  - MAC lockdown
  - MAC lockout
  - Port-Security

- Order of Precedence for Port Access Management (highest to lowest):
  a. MAC lockout
  b. MAC lockdown or Port Security
  c. Port-based Access Control (802.1X) or Web Authentication or MAC Authentication

Port Access Management

When configuring a port for Web or MAC Authentication, be sure that a higher precedent port access management feature is not enabled on the port. For example, be sure that Port Security is disabled on a port before configuring the port for Web or MAC Authentication. If Port Security is enabled on the port this misconfiguration does not allow Web or MAC Authentication to occur.

- VLANs: If your LAN does not use multiple VLANs, then you do not need to configure VLAN assignments in your RADIUS server or consider using either Authorized or Unauthorized VLANs. If your LAN does use multiple VLANs, then some of the following factors may apply to your use of Web-Auth and MAC-Auth.
  - Web-Auth and MAC-Auth operate only with port-based VLANs. Operation with protocol VLANs is not supported, and clients do not have access to protocol VLANs during Web-Auth and MAC-Auth sessions.
  - A port can belong to one, untagged VLAN during any client session. Where multiple authenticated clients may simultaneously use the same port, they must all be capable of operating on the same VLAN.
During an authenticated client session, the following hierarchy determines a port’s VLAN membership:
1. If there is a RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to this VLAN and temporarily drops all other VLAN memberships.
2. If there is no RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to the Authorized VLAN (if configured) and temporarily drops all other VLAN memberships.
3. If neither 1 or 2, above, apply, but the port is an untagged member of a statically configured, port-based VLAN, then the port remains in this VLAN.
4. If neither 1, 2, or 3, above, apply, then the client session does not have access to any statically configured, untagged VLANs and client access is blocked.

After an authorized client session begins on a given port, the port’s VLAN membership does not change. If other clients on the same port become authenticated with a different VLAN assignment than the first client, the port blocks access to these other clients until the first client session ends.

The optional “authorized” VLAN (auth-vid) and “unauthorized” VLAN (unauth-vid) you can configure for Web- or MAC-based authentication must be statically configured VLANs on the switch. Also, if you configure one or both of these options, any services you want clients in either category to access must be available on those VLANs.

Where a given port’s configuration includes an unauthorized client VLAN assignment, the port will allow an unauthenticated client session only while there are no requests for an authenticated client session on that port. In this case, if there is a successful request for authentication from an authorized client, the switch terminates the unauthorized-client session and begins the authorized-client session.

When a port on the switch is configured for Web or MAC Authentication and is supporting a current session with another device, rebooting the switch invokes a re-authentication of the connection.

When a port on the switch is configured as a Web- or MAC-based authenticator, it blocks access to a client that does not provide the proper authentication credentials. If the port configuration includes an optional, unauthorized VLAN (unauth-vid), the port is temporarily placed in the unauthorized VLAN if there are no other authorized clients currently using the port with a different VLAN assignment. If an authorized client is using the port with a different VLAN or if there is no unauthorized VLAN configured, the unauthorized client does not receive access to the network.
Web and MAC Authentication
Setup Procedure for Web/MAC Authentication

- Web- or MAC-based authentication and LACP cannot both be enabled on the same port.

Web/MAC Authentication and LACP

Web or MAC authentication and LACP are not supported at the same time on a port. The switch automatically disables LACP on ports configured for Web or MAC authentication.

- Use the `show port-access web-based` commands to display session status, port-access configuration settings, and statistics for Web-Auth sessions.

- When spanning tree is enabled on a switch that uses 802.1X, Web authentication, or MAC authentication, loops may go undetected. For example, spanning tree packets that are looped back to an edge port will not be processed because they have a different broadcast/multicast MAC address from the client-authenticated MAC address. To ensure that client-authenticated edge ports get blocked when loops occur, you should enable loop protection on those ports. For more information, refer to “Loop Protection” in the chapter titled “Multiple Instance Spanning-Tree Operation” in the Advanced Traffic Management Guide for your switch.

Setup Procedure for Web/MAC Authentication

Before You Configure Web/MAC Authentication

1. Configure a local username and password on the switch for both the Operator (login) and Manager (enable) access levels. (While this is not required for a Web- or MAC-based configuration, HP recommends that you use a local user name and password pair, at least until your other security measures are in place, to protect the switch configuration from unauthorized access.)

2. Determine the switch ports that you want to configure as authenticators. Note that before you configure Web- or MAC-based authentication on a port operating in an LACP trunk, you must remove the port from the trunk. (For more information, refer to the “Web/MAC Authentication and LACP” on page 3-12.)
Web and MAC Authentication

Setup Procedure for Web/MAC Authentication

To display the current configuration of 802.1X, Web-based, and MAC authentication on all switch ports, enter the `show port-access config` command.

```
HP Switch(config)# show port-access config
```

<table>
<thead>
<tr>
<th>Port Access Status Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-access authenticator activated [No] : Yes</td>
</tr>
<tr>
<td>Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Authenticator Enabled</th>
<th>Web Auth Enabled</th>
<th>Mac Auth Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>7</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>8</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>10</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>11</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>12</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 3-4. Example of show port-access config Command Output

3. Determine whether any VLAN assignments are needed for authenticated clients.
   a. If you configure the RADIUS server to assign a VLAN for an authenticated client, this assignment overrides any VLAN assignments configured on the switch while the authenticated client session remains active. Note that the VLAN must be statically configured on the switch.
   b. If there is no RADIUS-assigned VLAN, the port can join an “Authorized VLAN” for the duration of the client session, if you choose to configure one. This must be a port-based, statically configured VLAN on the switch.
   c. If there is neither a RADIUS-assigned VLAN or an “Authorized VLAN” for an authenticated client session on a port, then the port’s VLAN membership remains unchanged during authenticated client sessions. In this case, configure the port for the VLAN in which you want it to operate during client sessions.
Web and MAC Authentication
Setup Procedure for Web/MAC Authentication

Note that when configuring a RADIUS server to assign a VLAN, you can use either the VLAN's name or VID. For example, if a VLAN configured in the switch has a VID of 100 and is named vlan100, you could configure the RADIUS server to use either “100” or “vlan100” to specify the VLAN.

4. Determine whether to use the optional “Unauthorized VLAN” mode for clients that the RADIUS server does not authenticate. This VLAN must be statically configured on the switch. If you do not configure an “Unauthorized VLAN”, the switch simply blocks access to unauthenticated clients trying to use the port.

5. Determine the authentication policy you want on the RADIUS server and configure the server. Refer to the documentation provided with your RADIUS application and include the following in the policy for each client or client device:
   - The CHAP-RADIUS authentication method.
   - An encryption key
   - One of the following:
     - If you are configuring Web-based authentication, include the username and password for each authorized client.
     - If you are configuring MAC-based authentication, enter the device MAC address in both the username and password fields of the RADIUS policy configuration for that device. Also, if you want to allow a particular device to receive authentication only through a designated port and switch, include this in your policy.

6. Determine the IP address of the RADIUS server(s) you will use to support Web- or MAC-based authentication. (For information on configuring the switch to access RADIUS servers, refer to “Configuring the Switch To Access a RADIUS Server” on page 3-15.)
Configuring the RADIUS Server To Support MAC Authentication

On the RADIUS server, configure the client device authentication in the same way that you would any other client, except:

- Configure the client device's (hexadecimal) MAC address as both username and password. Be careful to configure the switch to use the same format that the RADIUS server uses. Otherwise, the server will deny access. The switch provides four format options:
  - aabbccddee.ff (the default format)
  - aabbcc-ddeeff
  - aa-bb-cc-dd-ee-ff
  - aa:bb:cc:dd:ee:ff
  - AABBCCDDEEFF
  - AABBCCC-DDEEFF
  - AA-BB-CC-DD-EE-FF

- If the device is a switch or other VLAN-capable device, use the base MAC address assigned to the device, and not the MAC address assigned to the VLAN through which the device communicates with the authenticator switch. Note that the switch applies a single MAC address to all VLANs configured in the switch. Thus, for a given switch, the MAC address is the same for all VLANs configured on the switch. (Refer to the chapter titled “Static Virtual LANs (VLANs)” in the Advanced Traffic Management Guide for your switch.)

Configuring the Switch To Access a RADIUS Server

<table>
<thead>
<tr>
<th>RADIUS Server Configuration Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-server</td>
</tr>
<tr>
<td>[host &lt;ip-address&gt;] below</td>
</tr>
<tr>
<td>[key &lt;global-key-string&gt;] below</td>
</tr>
<tr>
<td>radius-server host &lt;ip-address&gt; key &lt;server-specific key-string&gt;</td>
</tr>
</tbody>
</table>

This section describes the minimal commands for configuring a RADIUS server to support Web-Auth and MAC Auth. For information on other RADIUS command options, refer to chapter 5, “RADIUS Authentication, Authorization, and Accounting”. 
Web and MAC Authentication
Setup Procedure for Web/MAC Authentication

Syntax: [no] radius-server
  [host < ip-address >]
  Adds a server to the RADIUS configuration or (with no)
  deletes a server from the configuration. You can config-
  ure up to three RADIUS server addresses. The switch uses
  the first server it successfully accesses. (Refer to
  “RADIUS Authentication, Authorization, and Account-
  ing” on page 5-1.)

[key < global-key-string >]
  Specifies the global encryption key the switch uses with
  servers for which the switch does not have a server-
  specific key assignment (below). This key is optional if
  all RADIUS server addresses configured in the switch
  include a server-specific encryption key. The tilde (~)
  character is allowed in the string, for example, radius-
  server key hp-switch. It is not backward compatible; the
  “~” character is lost if you use a software version that
  does not support the “~” character.
  (Default: Null.)

Syntax: radius-server host < ip-address > key <server-specific key-string>
  [no] radius-server host < ip-address > key
  Optional. Specifies an encryption key for use during
  authentication (or accounting) sessions with the speci-
  fied server. This key must match the encryption key used
  on the RADIUS server. Use this command only if the
  specified server requires a different encryption key than
  configured for the global encryption key, above. The tilde
  (~) character is allowed in the string. It is not backward
  compatible; the “~” character is lost if you use a software
  version that does not support the “~” character.

  The no form of the command removes the key configured
  for a specific server.

For example, to configure the switch to access a RADIUS server at IP address
192.168.32.11 using a server specific shared secret key of ‘1A7rd’:
Web and MAC Authentication
Setup Procedure for Web/MAC Authentication

```
HP Switch(config)# radius-server host 192.158.32.11
HP Switch(config)# radius-server host 192.158.32.11 key 1A7rd

HP Switch(config)# show radius

Status and Counters - General RADIUS Information

Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key :

<table>
<thead>
<tr>
<th>Auth</th>
<th>Acct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP Addr</td>
<td>Port</td>
</tr>
<tr>
<td>192.168.32.11</td>
<td>1812</td>
</tr>
</tbody>
</table>
```

Figure 3-5. Example of Configuring a Switch To Access a RADIUS Server
Configng Web Authentication

Overview

1. If you have not already done so, configure a local username and password pair on the switch.

2. Identify or create a redirect URL for use by authenticated clients. HP recommends that you provide a redirect URL when using Web Authentication. If a redirect URL is not specified, web browser behavior following authentication may not be acceptable.

3. If you plan to use multiple VLANs with Web Authentication, ensure that these VLANs are configured on the switch and that the appropriate port assignments have been made. Also, confirm that the VLAN used by authorized clients can access the redirect URL.

4. Use the **ping** command in the switch console interface to ensure that the switch can communicate with the RADIUS server you have configured to support Web-Auth on the switch.

5. Configure the switch with the correct IP address and encryption key to access the RADIUS server.

6. (Optional) To use SSL encryption for web authentication login, configure and enable SSL on the switch.

7. Enable web authentication on the switch ports you want to use.

8. Configure the optional settings that you want to use for web authentication; for example:
   - To avoid address conflicts in a secure network, configure the base IP address and mask to be used by the switch for temporary DHCP addresses. You can also set the lease length for these temporary IP addresses.
   - To use SSL encryption for web authentication login, configure the SSL option.
   - To redirect authorized clients to a specified URL, configure the Redirect URL option.

9. Configure how web-authenticator ports transmit traffic before they successfully authenticate a client and enter the authenticated state:
   - You can block incoming and outgoing traffic on a port before authentication occurs.
Web and MAC Authentication
Configuring Web Authentication

- You can block only incoming traffic on a port before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on unauthenticated ports configured for web authentication. For example, Wake-on-LAN traffic is transmitted on a web-authenticated egress port that has not yet transitioned to the authenticated state;

10. Test both authorized and unauthorized access to your system to ensure that Web Authentication works properly on the ports you have configured for port-access using Web Authentication.

Note

Client web browsers may not use a proxy server to access the network.

Configuration Commands for Web Authentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa port-access &lt;port-list&gt; controlled-directions &lt;both</td>
<td>in&gt;</td>
</tr>
<tr>
<td>[no] aaa port-access web-based &lt;port-list&gt;</td>
<td>3-22</td>
</tr>
<tr>
<td>[auth-vid]</td>
<td>3-22</td>
</tr>
<tr>
<td>[client-limit]</td>
<td>3-22</td>
</tr>
<tr>
<td>[dhcp-addr]</td>
<td>3-22</td>
</tr>
<tr>
<td>[dhcp-lease]</td>
<td>3-23</td>
</tr>
<tr>
<td>[logoff-period]</td>
<td>3-23</td>
</tr>
<tr>
<td>[max-requests]</td>
<td>3-23</td>
</tr>
<tr>
<td>[max-retries]</td>
<td>3-23</td>
</tr>
<tr>
<td>[quiet-period]</td>
<td>3-23</td>
</tr>
<tr>
<td>[reauth-period]</td>
<td>3-24</td>
</tr>
<tr>
<td>[reauthenticate]</td>
<td>3-24</td>
</tr>
<tr>
<td>[redirect-url]</td>
<td>3-24</td>
</tr>
<tr>
<td>[server-timeout]</td>
<td>3-24</td>
</tr>
<tr>
<td>[unauth-vid]</td>
<td>3-36</td>
</tr>
<tr>
<td>[access-denied-message &lt;&lt;access-denied-str&gt;</td>
<td>radius-response&gt;)]</td>
</tr>
</tbody>
</table>
Syntax:  aaa port-access <port-list> controlled-directions <both | in>

After you enable web-based authentication on specified ports, you can use the `aaa port-access controlled-directions` command to configure how a port transmits traffic before it successfully authenticates a client and enters the authenticated state.

**both** (default): Incoming and outgoing traffic is blocked on a port configured for web authentication before authentication occurs.

**in**: Incoming traffic is blocked on a port configured for web authentication before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on unauthenticated ports configured for web authentication.

**Prerequisites**: As implemented in 802.1X authentication, the disabling of incoming traffic and transmission of outgoing traffic on a web-authenticated egress port in an unauthenticated state (using the `aaa port-access controlled-directions in` command) is supported only if:

- The 802.1s Multiple Spanning Tree Protocol (MSTP) or 802.1w Rapid Spanning Tree Protocol (RSTP) is enabled on the switch. MSTP and RSTP improve resource utilization while maintaining a loop-free network.

The port is configured as an edge port in the network using the `spanning-tree edge-port` command.
Web and MAC Authentication
Configuring Web Authentication

**Syntax:**
```
aaa port-access <port-list> controlled-directions <both | in>
```

--- Continued ---

**Notes:**

- For information on how to configure the prerequisites for using the `aaa port-access controlled-directions` command, see Chapter 4, “Multiple Instance Spanning-Tree Operation” in the Advanced Traffic Management Guide.

- To display the currently configured Controlled Directions value for web-authenticated ports, enter the `show port-access web-based config` command as shown in Figure 3-4.

- The `aaa port-access controlled-direction in` command allows Wake-on-LAN traffic to be transmitted on a web-authenticated egress port that has not yet transitioned to the authenticated state; the `controlled-direction both` setting prevents Wake-on-LAN traffic to be transmitted on a web-authenticated egress port until authentication occurs.

  *The Wake-on-LAN feature is used by network administrators to remotely power on a sleeping workstation (for example, during early morning hours to perform routine maintenance operations, such as patch management and software updates)*

- Using the `aaa port-access controlled-directions in` command, you can enable the transmission of Wake-on-LAN traffic on unauthenticated egress ports that are configured for any of the following port-based security features:
  - 802.1X authentication
  - MAC authentication
  - Web authentication

  *Because a port can be configured for more than one type of authentication to protect the switch from unauthorized access, the last setting you configure with the `aaa port-access controlled-directions` command is applied to all authentication methods configured on the switch.*

  *For information about how to configure and use 802.1X authentication, refer to Chapter 12, “Configuring Port-Based and User-Based Access Control (802.1X)”.*

- When a web-authenticated port is configured with the `controlled-directions in` setting, eavesdrop prevention is not supported on the port.
**Web and MAC Authentication**

**Configuring Web Authentication**

**Syntax:** 

```
[no] aaa port-access web-based <port-list>
```

Enables web-based authentication on the specified ports. Use the `no` form of the command to disable web-based authentication on the specified ports.

**Syntax:**

```
aaa port-access web-based <port-list> [auth-vid <vid>]]
```

no aaa port-access web-based <port-list> [auth-vid]

Specifies the VLAN to use for an authorized client. The Radius server can override the value (accept-response includes a vid). If `auth-vid` is 0, no VLAN changes occur unless the RADIUS server supplies one.

Use the `no` form of the command to set the `auth-vid` to 0. (Default: 0).

**Syntax:**

```
aaa port-access web-based <port-list> [client-limit <1-256>]
```

Specifies the maximum number of authenticated clients to allow on the port. (Default: 1)

**Note:** On switches where Web Auth and 802.1X can operate concurrently, this limit includes the total number of clients authenticated through both methods. The limit of 256 clients only applies when there are fewer than 16,384 authentication clients on the entire switch. After the limit of 16,384 clients is reached, no additional authentication clients are allowed on any port for any method.

**Syntax:**

```
aaa port-access web-based [dhcp-addr <ip-address/mask>]
```

Specifies the base address/mask for the temporary IP pool used by DHCP. The base address can be any valid ip address (not a multicast address). Valid mask range value is <255.255.240.0 - 255.255.255.0>. (Default: 192.168.0.0/255.255.255.0)
Syntax: aaa port-access web-based [dhcp-lease <5 - 25>]

Specifies the lease length, in seconds, of the temporary IP address issued for Web Auth login purposes. (Default: 10 seconds)

Syntax: aaa port-access web-based <port-list> [logoff-period] <60-9999999>

Specifies the period, in seconds, that the switch enforces for an implicit logoff. This parameter is equivalent to the MAC age interval in a traditional switch sense. If the switch does not see activity after a logoff-period interval, the client is returned to its pre-authentication state. (Default: 300 seconds)

Syntax: aaa port-access web-based <port-list> [max-requests <1-10>]

Specifies the number of authentication attempts that must time-out before authentication fails. (Default: 2)

Syntax: aaa port-access web-based <port-list> [max-retries <1-10>]

Specifies the number of the number of times a client can enter their user name and password before authentication fails. This allows the reentry of the user name and password if necessary. (Default: 3)

Syntax: aaa port-access web-based <port-list> [quiet-period <1 - 65535>]

Specifies the time period (in seconds) the switch uses before sending an authentication request for a client that failed authentication. (Default: 60 seconds)
### Web and MAC Authentication

#### Configuring Web Authentication

**Syntax:**
```
aaa port-access web-based <port-list> [reauth-period <0 - 9999999>]
```

Specifies the time period, in seconds, the switch enforces on a client to re-authenticate. When set to 0, reauthentication is disabled. (Default: 0 seconds)

**Syntax:**
```
aaa port-access web-based <port-list> [reauthenticate]
```

Forces a reauthentication of all attached clients on the port.

**Syntax:**
```
aaa port-access web-based <port-list> [redirect-url <url>]
```

no aaa port-access web-based <port-list> [redirect-url]

Specifies the URL that a user is redirected to after a successful login. Any valid, fully-formed URL may be used, for example, http://welcome-server/welcome.htm or http://192.22.17.5. HP recommends that you provide a redirect URL when using Web Authentication.

**Note:** The redirect-url command accepts only the first 103 characters of the allowed 127 characters.

Use the `no` form of the command to remove a specified redirect URL.

(Default: There is no default URL. Browser behavior for authenticated clients may not be acceptable.)

**Syntax:**
```
aaa port-access web-based [e] <port-list> [server-timeout <1 - 300>]
```

Specifies the period, in seconds, the switch waits for a server response to an authentication request. Depending on the current max-requests value, the switch sends a new attempt or ends the authentication session.

(Default: 30 seconds)
Show Commands for Web Authentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show port-access web-based [port-list]</td>
<td>3-25</td>
</tr>
<tr>
<td>show port-access web-based clients [port-list]</td>
<td>3-26</td>
</tr>
<tr>
<td>show port-access web-based clients &lt;port-list&gt; detailed</td>
<td>3-27</td>
</tr>
<tr>
<td>show port-access web-based config [port-list]</td>
<td>3-28</td>
</tr>
<tr>
<td>show port-access web-based config &lt;port-list&gt; detailed</td>
<td>3-29</td>
</tr>
<tr>
<td>show port-access web-based config [port-list] auth-server</td>
<td>3-30</td>
</tr>
<tr>
<td>show port-access web-based config [port-list] web-server</td>
<td>3-30</td>
</tr>
</tbody>
</table>

**Syntax:** show port-access web-based [port-list]

Displays the status of all ports or specified ports that are enabled for Web authentication. The information displayed for each port includes:

- Number of authorized and unauthorized clients
- VLAN ID number of the untagged VLAN used. If the switch supports MAC-based (untagged) VLANs, MACbased is displayed to show that multiple untagged VLANs are configured for authentication sessions.
- If tagged VLANs (statically configured or RADIUS-assigned) are used (Yes or No)
- If client-specific per-port CoS (Class of Service) values are configured (Yes or No) or the numerical value of the CoS (802.1p priority) applied to all inbound traffic. For client-specific per-port CoS values, enter the show port-access web-based clients detailed command.
- If per-port rate-limiting for inbound traffic is applied (Yes or No) or the percentage value of the port's available bandwidth applied as a rate-limit value.
- If RADIUS-assigned ACLs are applied

Information on ports not enabled for Web Authentication is not displayed.
Web and MAC Authentication
Configuring Web Authentication

HP Switch(config)# show port-access web-based

<table>
<thead>
<tr>
<th>Port Access Web-Based Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>

Figure 3-6. Example of show port-access web-based Command Output

Syntax: show port-access web-based clients [port-list]

Displays the session status, name, and address for each web-authenticated client on the switch. The IP address displayed is taken from the DHCP binding table (learned through the DHCP Snooping feature).

If DHCP snooping is not enabled on the switch, n/a (not available) is displayed for a client's IP address.

If a web-authenticated client uses an IPv6 address, n/a - IPv6 is displayed.

If DHCP snooping is enabled but no MAC-to-IP address binding for a client is found in the DHCP binding table, n/a - no info is displayed.

HP Switch(config)# show port-access web-based clients

<table>
<thead>
<tr>
<th>Port Access Web-Based Client Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>

Figure 3-7. Example of show port-access web-based clients Command Output
Web and MAC Authentication
Configuring Web Authentication

Syntax:  

show port-access web-based clients <port-list> detailed

Displays detailed information on the status of web-authenticated client sessions on specified switch ports. Shows session status, name, and address for each web-authenticated client on the switch. The IP address displayed is taken from the DHCP binding table (learned through DHCP snooping). The following can appear if the client’s IP address is not available:

- **n/a**—DHCP snooping is not enabled on the switch; **n/a** is displayed for a client’s IP address.
- **n/a-IPv6**—a web-authenticated client uses an IPv6 address.
- **n/a-no info**—DHCP snooping is enabled but no MAC-to-IP address binding for a client is found in the DHCP binding table.

```
HP Switch(config)# show port-access web-based clients 1 detailed

Port Access Web-Based Client Status Detailed

Client Base Details :
Port : 1
Session Status : authenticated  Session Time(sec) : 6
Username : webuser1    MAC Address : 0010b5-891a9e
IP : n/a

Access Policy Details :
COS Map : 11111111  In Limit % : 98
Untagged VLAN : 4006  Out Limit % : 100
Tagged VLANs : 1, 3, 5, 6, 334, 2566
RADIUS-ACL List :
  deny in udp from any to 10.2.8.233 CNT
    Hit Count: 0
  permit in udp from any to 10.2.8.233 CNT
    Hit Count: 0
  deny in tcp from any to 10.2.8.233 CNT
    Hit Count: 0
  permit in tcp from any to 10.2.8.233 CNT
    Hit Count: 0
  permit in tcp from any to 0.0.0.0/0 CNT
    Hit Count: 0

Figure 3-8.  Example of show port-access web-based clients detailed Command Output
```
Web and MAC Authentication
Configuring Web Authentication

Syntax: show port-access web-based config [port-list]

Displays the currently configured Web Authentication settings for all switch ports or specified ports, including:

- Temporary DHCP base address and mask
- Support for RADIUS-assigned dynamic VLANs (Yes or No)
- Controlled directions setting for transmitting Wake-on-LAN traffic on egress ports
- Authorized and unauthorized VLAN IDs
If the authorized or unauthorized VLAN ID value is 0, the default VLAN ID is used unless overridden by a RADIUS-assigned value.

```
HP Switch(config)# show port-access web-based config

Port Access Web-Based Configuration

DHCP Base Address : 192.168.0.0
DHCP Subnet Mask : 255.255.255.0
DHCP Lease Length : 10
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Limit</th>
<th>Moves</th>
<th>Logoff Period</th>
<th>Re-Auth Period</th>
<th>Unauth VLAN ID</th>
<th>Auth VLAN ID</th>
<th>Cntrl Dir</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>in</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 3-9. Example of show port-access web-based config Command Output
Web and MAC Authentication
Configuring Web Authentication

**Syntax:**
```
show port-access web-based config <port-list> detailed
```

*Displays more detailed information on the currently configured Web Authentication settings for specified ports.*

HP Switch(config)# show port-access web-based config 1 detailed

<table>
<thead>
<tr>
<th>Port Access Web-Based Detailed Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Client Limit</td>
</tr>
<tr>
<td>Logoff Period</td>
</tr>
<tr>
<td>Unauth VLAN ID</td>
</tr>
<tr>
<td>Max Requests</td>
</tr>
<tr>
<td>Server Timeout</td>
</tr>
<tr>
<td>Max Retries</td>
</tr>
</tbody>
</table>

**Figure 3-10. Example of show port-access web-based config detail Command Output**
**Web and MAC Authentication**

**Configuring Web Authentication**

**Syntax:**  
```
show port-access web-based config [port-list] auth-server
```

Displays the currently configured Web Authentication settings for all switch ports or specified ports and includes RADIUS server-specific settings, such as:

- Timeout waiting period
- Number of timeouts supported before authentication login fails
- Length of time (quiet period) supported between authentication login attempts

```
HP Switch(config)# show port-access web-based config auth-server
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Client Limit</th>
<th>Client Moves</th>
<th>Logoff Period</th>
<th>Re-Auth Period</th>
<th>Max Req</th>
<th>Quiet Period</th>
<th>Server Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>3</td>
<td>60</td>
<td>30</td>
</tr>
<tr>
<td>2</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>3</td>
<td>60</td>
<td>30</td>
</tr>
</tbody>
</table>

Figure 3-11. Example of show port-access web-based config auth-server Command Output

**Syntax:**  
```
show port-access web-based config [port-list] web-server
```

Displays the currently configured Web Authentication settings for all ports or specified ports, including web-specific settings for password retries, SSL login status, and a redirect URL, if specified.
Configuring MAC Authentication on the Switch

Overview

1. If you have not already done so, configure a local username and password pair on the switch.

2. If you plan to use multiple VLANs with MAC Authentication, ensure that these VLANs are configured on the switch and that the appropriate port assignments have been made.

3. Use the `ping` command in the switch console interface to ensure that the switch can communicate with the RADIUS server you have configured to support MAC-Auth on the switch.

4. Configure the switch with the correct IP address and encryption key to access the RADIUS server.

5. Configure the switch for MAC-Auth:
   a. Configure MAC Authentication on the switch ports you want to use.

6. Test both the authorized and unauthorized access to your system to ensure that MAC Authentication works properly on the ports you have configured for port-access.
Web and MAC Authentication
Configuring MAC Authentication on the Switch

Configuration Commands for MAC Authentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa port-access mac-based addr-format</td>
<td>3-32</td>
</tr>
<tr>
<td>[no] aaa port-access mac-based password &lt;password-value&gt;</td>
<td>below</td>
</tr>
<tr>
<td>[no] aaa port-access mac-based [e] &lt;port-list&gt;</td>
<td>3-34</td>
</tr>
<tr>
<td>[addr-limit]</td>
<td>3-35</td>
</tr>
<tr>
<td>[addr-moves]</td>
<td>3-35</td>
</tr>
<tr>
<td>[auth-vid]</td>
<td>3-35</td>
</tr>
<tr>
<td>[logoff-period]</td>
<td>3-35</td>
</tr>
<tr>
<td>[max-requests]</td>
<td>3-36</td>
</tr>
<tr>
<td>[quiet-period]</td>
<td>3-36</td>
</tr>
<tr>
<td>[reauth-period]</td>
<td>3-36</td>
</tr>
<tr>
<td>[reauthenticate]</td>
<td>3-36</td>
</tr>
<tr>
<td>[server-timeout]</td>
<td>3-36</td>
</tr>
<tr>
<td>[unauth-period]</td>
<td>3-36</td>
</tr>
<tr>
<td>[unauth-vid]</td>
<td>3-36</td>
</tr>
</tbody>
</table>

Configuring the Global MAC Authentication Password

MAC authentication only requires that an entry is placed in the user database with the device's MAC address as both the username and the password, creating the opportunity for malicious device spoofing using the readily available MAC address. To make spoofing more difficult, the global password option allows a network administrator to configure a common MAC authentication password that is used for all MAC authentications sent to the RADIUS server.

When implementing the global MAC authentication password option, it is important that the user database on the RADIUS server has the MAC authentication password as the password for each device performing MAC authentication.
Use this command to configure the global MAC authentication password.

**Syntax:**  

```
[no] aaa port-access mac-based password <password-value>
```

*Specify the global password to be used by all MAC authenticating devices.*

*The no form of the command disables the feature.*

```bash
HP Switch(config)# aaa port-access mac-based password secretMAC1
HP Switch(config)# show port-access mac-based config
```

**Port Access MAC-Based Configuration**

<table>
<thead>
<tr>
<th>MAC Address Format : no-delimiter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password : secretMAC1</td>
</tr>
</tbody>
</table>

**Unauth Redirect Configuration URL :**

- Unauth Redirect Client Timeout (sec) : 1800
- Unauth Redirect Restrictive Filter : Disabled
- Total Unauth Redirect Client Count : 0

<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Limit</th>
<th>Moves</th>
<th>Logoff Period</th>
<th>Re-Auth Period</th>
<th>Unauth VLAN ID</th>
<th>Auth VLAN ID</th>
<th>Cntrl Dir</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>2</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>3</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>6</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>7</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>8</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
</tbody>
</table>

**Figure 3-12. Example of Configuring a Global MAC Authentication Password**

**Note**  

The password value will display in an exported config file when `include-credentials` is enabled.
Configuring a MAC-based Address Format

**Syntax:**
```
```

Specifies the MAC address format to be used in the RADIUS request message. This format must match the format used to store the MAC addresses in the RADIUS server. (Default: no-delimiter)

- **no-delimiter** — specifies an aabbccddeeff format.
- **single-dash** — specifies an aabbcc-ddeeff format.
- **multi-dash** — specifies an aa-bb-cc-dd-ee-ff format.
- **no-delimiter-uppercase** — specifies an AABBCCDDEEFF format.
- **single-dash-uppercase** — specifies an AABBCC-DDEEFF format.
- **multi-dash-uppercase** — specifies an AA-BB-CC-DD-EE-FF format.

Configuring Other MAC-based Commands

**Syntax:**
```
[no] aaa port-access mac-based < port-list >
```

Enables MAC-based authentication on the specified ports. Use the **no** form of the command to disable MAC-based authentication on the specified ports.
Web and MAC Authentication
Configuring MAC Authentication on the Switch

Syntax: aaa port-access mac-based [e] < port-list > [addr-limit <1-256>]
Specifies the maximum number of authenticated MACs to allow on the port. (Default: 1)
Note: On switches where MAC Auth and 802.1X can operate concurrently, this limit includes the total number of clients authenticated through both methods. The limit of 256 clients only applies when there are fewer than 16,384 authentication clients on the entire switch. After the limit of 16,384 clients is reached, no additional authentication clients are allowed on any port for any method.

Syntax: [no] aaa port-access mac-based [e] < port-list > [addr-moves]
Allows client moves between the specified ports under MAC Auth control. When enabled, the switch allows addresses to move without requiring a re-authentication. When disabled, the switch does not allow moves and when one does occur, the user will be forced to re-authenticate. At least two ports (from port(s) and to port(s)) must be specified. Use the no form of the command to disable MAC address moves between ports under MAC Auth control. (Default: disabled – no moves allowed)

Syntax: aaa port-access mac-based [e] < port-list > [auth-vid <vid>]
no aaa port-access mac-based [e] < port-list > [auth-vid]
Specifies the VLAN to use for an authorized client. The Radius server can override the value (accept-response includes a vid). If auth-vid is 0, no VLAN changes occur unless the RADIUS server supplies one. Use the no form of the command to set the auth-vid to 0. (Default: 0).

Syntax: aaa port-access mac-based [e] < port-list > [logoff-period] <60-9999999>
Specifies the period, in seconds, that the switch enforces for an implicit logoff. This parameter is equivalent to the MAC age interval in a traditional switch sense. If the switch does not see activity after a logoff-period interval, the client is returned to its pre-authentication state. (Default: 300 seconds)
Web and MAC Authentication
Configuring MAC Authentication on the Switch

**Syntax:**
```plaintext
aaa port-access mac-based [e] < port-list > [max-requests <1-10>]
```
Specifies the number of authentication attempts that must time-out before authentication fails. (Default: 2)

**Syntax:**
```plaintext
aaa port-access mac-based [e] < port-list > [quiet-period <1 - 65535>]
```
Specifies the time period (in seconds) that the switch waits before processing an authentication request from a MAC address that failed authentication. (Default: 60 seconds)

**Syntax:**
```plaintext
aaa port-access mac-based [e] < port-list > [reauth-period <0 - 9999999>]
```
Specifies the time period (in seconds) that the switch enforces on a client to re-authenticate. The client remains authenticated while the reauthentication occurs.

When set to 0, reauthentication is disabled.
(Default: 0 seconds)

**Syntax:**
```plaintext
aaa port-access mac-based [e] < port-list > [reauthenticate]
```
Forces a reauthentication of all attached clients on the port.

**Syntax:**
```plaintext
aaa port-access mac-based [e] < port-list > [server-timeout <1 - 300>]
```
Specifies the period, in seconds, the switch waits for a server response to an authentication request. Depending on the current max-requests value, the switch sends a new attempt or ends the authentication session.
(Default: 30 seconds)

**Syntax:**
```plaintext
aaa port-access mac-based [e] < port-list > [unauth-period]
```
Sets the period of time the switch waits before moving the port to the VLAN for unauthenticated clients.

**Syntax:**
```plaintext
aaa port-access mac-based [e] < port-list > [unauth-vid <vid>]
no aaa port-access mac-based [e] < port-list > [unauth-vid]
```
Specifies the VLAN to use for a client that fails authentication. If unauth-vid is 0, no VLAN changes occur.
Use the no form of the command to set the unauth-vid to 0.
(Default: 0)
Configuring Custom Messages

This feature allows administrators to configure custom messages that are displayed when authentication with the RADIUS server fails. The messages are appended to the existing internal web page that displays during the authentication process. Messages can be configured using the CLI, or centrally using the RADIUS server, and can provide a description of the reason for the failure as well as possible steps to take to resolve the authentication issue. There is no change to the current web authentication functionality.

**Syntax:**

```gments [no] aaa port-access web-based access-denied-message <<access-denied-str>| radius-response>
```

Specifies the text message (ASCII string) shown on the web page after an unsuccessful login attempt. The message must be enclosed in quotes.

The **no** form of the command means that no message is displayed upon failure to authenticate.

**Default:** The internal web page is used. No message will be displayed upon authentication failure.

**access-denied-str:** The text message that is appended to the end of the web page when there is an unsuccessful authentication request. The string can be up to 250 ASCII characters.

**radius-response:** Use the text message provided in the RADIUS server response to the authentication request.

```
HP Switch(config)# aaa port-access web-based access-denied-message “Please contact your system administrator to obtain authentication privileges.”
```

Figure 3-13. Example of Configuring an Access Denied Message on the Switch
Web and MAC Authentication
Configuring MAC Authentication on the Switch

HP Switch(config)# show port-access web-based config

Port Access Web-based Configuration
DHCP Base Address : 192.168.0.0
DHCP Subnet Mask : 255.255.248.0
DHCP Lease Length : 10 seconds
Allow RADIUS-assigned dynamic (GVRP) VLANs[No]: Yes
Access Denied Message : Custom:
   Please contact your system administrator to obtain authentication privileges.

<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Limit</th>
<th>Moves</th>
<th>Logoff</th>
<th>Re-auth</th>
<th>Unauth</th>
<th>Auth</th>
<th>Ctrl</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>60</td>
<td>1</td>
<td>2</td>
<td>both</td>
</tr>
<tr>
<td>A2</td>
<td>Yes</td>
<td>18</td>
<td>No</td>
<td>999999999</td>
<td>999999999</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>A3</td>
<td>Yes</td>
<td>22</td>
<td>No</td>
<td>999999999</td>
<td>999999999</td>
<td>4096</td>
<td>4096</td>
<td>both</td>
</tr>
</tbody>
</table>

Figure 3-14. Example of Output showing the Custom Access Denied Message

The example in Figure 3-15 shows the text of the Access Denied Message when the radius-response option is configured.

HP Switch(config)# show port-access web-based config

Port Access Web-based Configuration
DHCP Base Address : 192.168.0.0
DHCP Subnet Mask : 255.255.248.0
DHCP Lease Length : 10 seconds
Allow RADIUS-assigned dynamic (GVRP) VLANs[No]: Yes
Access Denied Message : Retrieved from Radius

<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Limit</th>
<th>Moves</th>
<th>Logoff</th>
<th>Re-auth</th>
<th>Unauth</th>
<th>Auth</th>
<th>Ctrl</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>60</td>
<td>1</td>
<td>2</td>
<td>both</td>
</tr>
<tr>
<td>A2</td>
<td>Yes</td>
<td>18</td>
<td>No</td>
<td>300</td>
<td>999999999</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>A3</td>
<td>Yes</td>
<td>22</td>
<td>No</td>
<td>300</td>
<td>999999999</td>
<td>4096</td>
<td>4096</td>
<td>both</td>
</tr>
</tbody>
</table>

Figure 3-15. Example of Access Denied Message when radius-response is Configured
Unauthenticated clients may be assigned to a specific static, untagged VLAN (unauth-vid), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients, the port is blocked and no network access is available.

**Web Page Display of Access Denied Message**

The web page in Figure 3-16 is an example of the denied access message that appears when unauth-vid is configured.

---

Invalid Credentials

Your credentials were not accepted. You may have limited network access. Please wait while the configuration completes.

Estimated time remaining: 35 seconds

Please contact your system administrator to obtain authentication privileges.

© 2009 Hewlett Packard Development Company, L.P.

---

Figure 3-16. Example of Web Page with Configured Access Denied Message When unauth-vid is Configured

Figure 3-17 shows an example of a web page displaying the access denied message when un auth-vid is not configured.
Invalid Credentials

Your credentials were not accepted. Please wait 96 seconds to retry. You will be redirected automatically to the login page.

Unauthorized access to this network is prohibited. Access to this network requires prior authorization from the System Administrator. Please obtain the credentials prior to logging in.

Please contact your system administrator to obtain authentication privileges.

The `show running-config` command displays the client’s information, including the configured access denied message.
Figure 3-18. Example of Running Configuration Output Displaying Access Denied Message
Web and MAC Authentication
Configuring MAC Authentication on the Switch

HP Switch(config)# show running-config

Running configuration:

; J8692A Configuration Editor; Created on release #W.15.xx

hostname "HP Switch"
web-management ssl
qos dscp-map 000000 priority 0
module 1 type J86xxA
module 3 type J8694A
no stack auto-join
vlan 1
  name "DEFAULT_VLAN"
    untagged 1-14,19-24,A1-A4
    ip address dhcp-bootp
    no untagged 15-18
    exit
vlan 100
  name "auth-vid"
    untagged 15-18
    ip address dhcp-bootp
    exit
radius-server host 10.0.13.118 key 'secret'
aaa authentication port-access eap-radius
snmp-server community "public" Unrestricted
aaa port-access web-based 5 auth-vid 100
aaa port-access web-based 5 unauth-vid 1
aaa port-access web-based dhcp-addr 172.18.0.0 255.255.255.0
aaa port-access web-based access-denied-message radius-response

Figure 3-19. Example of Running Configuration Output When RADIUS Response is Configured

Show Commands for MAC-Based Authentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show port-access mac-based [port-list]</td>
<td>3-43</td>
</tr>
<tr>
<td>show port-access mac-based clients [port-list]</td>
<td>3-44</td>
</tr>
<tr>
<td>show port-access mac-based clients &lt;port-list&gt; detailed</td>
<td>3-45</td>
</tr>
<tr>
<td>show port-access mac-based config [port-list]</td>
<td>3-46</td>
</tr>
<tr>
<td>show port-access mac-based config &lt;port-list&gt; detailed</td>
<td>3-47</td>
</tr>
<tr>
<td>show port-access mac-based config [port-list] auth-server</td>
<td>3-48</td>
</tr>
</tbody>
</table>
**Syntax:** show port-access mac-based [port-list]

Displays the status of all ports or specified ports that are enabled for MAC authentication. The information displayed for each port includes:

- Number of authorized and unauthorized clients
- VLAN ID number of the untagged VLAN used. If the switch supports MAC-based (untagged) VLANs, **MACbased** is displayed to show that multiple untagged VLANs are configured for authentication sessions.
- If tagged VLANs (statically configured or RADIUS-assigned) are used (Yes or No)
- If client-specific per-port CoS (Class of Service) values are configured (Yes or No) or the numerical value of the CoS (802.1p priority) applied to all inbound traffic. For client-specific per-port CoS values, enter the `show port-access web-based clients detailed` command.
- If per-port rate-limiting for inbound traffic is applied (Yes or No) or the percentage value of the port’s available bandwidth applied as a rate-limit value.
- If RADIUS-assigned ACLs are applied

Information on ports not enabled for MAC authentication is not displayed.

<table>
<thead>
<tr>
<th>Port</th>
<th>Auth Clients</th>
<th>Unauth Clients</th>
<th>Untagged VLAN</th>
<th>Tagged VLANs</th>
<th>Port COS</th>
<th>% In</th>
<th>RADIUS ACL</th>
<th>Control Dir</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2003</td>
<td>Yes</td>
<td>70000000</td>
<td>100</td>
<td>Yes</td>
<td>both</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>MACbased</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>both</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>both</td>
</tr>
</tbody>
</table>

Figure 3-20. Example of show port-access mac-based Command Output
Web and MAC Authentication
Configuring MAC Authentication on the Switch

**Syntax:** show port-access mac-based clients [port-list]

Displays the session status, name, and address for each MAC-authenticated client on the switch. The IP address displayed is taken from the DHCP binding table (learned through the DHCP Snooping feature).

If DHCP snooping is not enabled on the switch, n/a (not available) is displayed for a client's IP address.

If a MAC-authenticated client uses an IPv6 address, n/a - IPv6 is displayed.

If DHCP snooping is enabled but no MAC-to-IP address binding for a client is found in the DHCP binding table, n/a - no info is displayed.

```
HP Switch(config)# show port-access mac-based clients

Port Access MAC-Based Client Status

Port  MAC Address          IP Address                              Session Status
-----  -----------          --------------------------------------- -------------
 1     000000-111112       192.192.192.192                          authenticated
 2     000000-111111       n/a                                     authenticating
```

Figure 3-21. Example of show port-access mac-based clients Command Output
Syntax:  show port-access mac-based clients <port-list> detailed

Displays detailed information on the status of MAC-authenticated client sessions on specified ports. Show session status, name, and address for each MAC-authenticated client on the switch. The IP address displayed is taken from the DHCP binding table (learned through DHCP snooping). The following can appear if the client’s IP address is not available:

n/a—DHCP snooping is not enabled on the switch; n/a is displayed for a client’s IP address.

n/a-IPv6—a web-authenticated client uses an IPv6 address.

n/a-no info—DHCP snooping is enabled but no MAC-to-IP address binding for a client is found in the DHCP binding table.

HP Switch(config)# show port-access mac-based clients 1 detailed

Port Access MAC-Based Client Status Detailed

Client Base Details:
- Port : 1
- Session Status : authenticated
- Session Time(sec) : 6
- Username : client1
- MAC Address : 0010b5-891a9e
- IP : n/a

Access Policy Details:
- COS Map : 12345678
- In Limit % : 98
- Untagged VLAN : 4006
- Out Limit % : 100
- Tagged VLANs : 1, 3, 5, 6, 334, 4001

RADIUS-ACL List:
- deny in udp from any to 10.2.8.233 CNT
  Hit Count: 0
- permit in udp from any to 10.2.8.233 CNT
  Hit Count: 0
- deny in tcp from any to 10.2.8.233 CNT
  Hit Count: 0
- permit in tcp from any to 10.2.8.233 CNT
  Hit Count: 0
- permit in tcp from any to 0.0.0.0/0 CNT
  Hit Count: 0

Figure 3-22. Example of show port-access mac-based clients detail Command Output
Web and MAC Authentication
Configuring MAC Authentication on the Switch

**Syntax:**
```
show port-access mac-based config [port-list]
```

Displays the currently configured MAC Authentication settings for all switch ports or specified ports, including:
- MAC address format
- Support for RADIUS-assigned dynamic VLANs (Yes or No)
- Controlled directions setting for transmitting Wake-on-LAN traffic on egress ports
- Authorized and unauthorized VLAN IDs

If the authorized or unauthorized VLAN ID value is 0, the default VLAN ID is used unless overridden by a RADIUS-assigned value.

```
HP Switch(config)# show port-access mac-based config
```

<table>
<thead>
<tr>
<th>Port Access MAC-Based Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address Format : no-delimiter</td>
</tr>
<tr>
<td>Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Limit</th>
<th>Moves</th>
<th>Period</th>
<th>Re-Auth</th>
<th>Unauth</th>
<th>Auth</th>
<th>VLAN ID</th>
<th>VLAN ID</th>
<th>Ctrl</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>both</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>in</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3-23. Example of show port-access mac-based config Command Output**
Web and MAC Authentication
Configuring MAC Authentication on the Switch

Syntax: show port-access mac-based config <port-list> detailed

 Displays more detailed information on the currently configured MAC Authentication settings for specified ports.

HP Switch(config)# show port-access mac-based config 1 detailed

<table>
<thead>
<tr>
<th>Port Access MAC-Based Detailed Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port            : 1        Web-based enabled : Yes</td>
</tr>
<tr>
<td>Client Limit    : 1        Client Moves      : No</td>
</tr>
<tr>
<td>Logoff Period   : 300       Re-Auth Period    : 0</td>
</tr>
<tr>
<td>Unauth VLAN ID  : 0        Auth VLAN ID      : 0</td>
</tr>
<tr>
<td>Max Requests    : 3        Quiet Period      : 60</td>
</tr>
<tr>
<td>Server Timeout  : 30</td>
</tr>
</tbody>
</table>

Figure 3-24. Example of show port-access mac-based config detail Command Output
Web and MAC Authentication
Configuring MAC Authentication on the Switch

Syntax: show port-access mac-based config [port-list] auth-server

Displays the currently configured Web Authentication settings for all switch ports or specified ports and includes RADIUS server-specific settings, such as:
- Timeout waiting period
- Number of timeouts supported before authentication login fails
- Length of time (quiet period) supported between authentication login attempts

<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Client Limit</th>
<th>Client Moves</th>
<th>Logoff Period</th>
<th>Re-Auth Period</th>
<th>Max Req Period</th>
<th>Quiet Period</th>
<th>Server Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>3</td>
<td>60</td>
<td>30</td>
</tr>
<tr>
<td>2</td>
<td>No</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>3</td>
<td>60</td>
<td>30</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>1</td>
<td>No</td>
<td>300</td>
<td>0</td>
<td>3</td>
<td>60</td>
<td>30</td>
</tr>
</tbody>
</table>

Figure 3-25. Example of show port-access mac-based config auth-server Command Output
Client Status

The table below shows the possible client status information that may be reported by a Web-based or MAC-based `show clients` command.

<table>
<thead>
<tr>
<th>Reported Status</th>
<th>Available Network Connection</th>
<th>Possible Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>authenticated</td>
<td>Authorized VLAN</td>
<td>Client authenticated. Remains connected until logoff-period or reauth-period expires.</td>
</tr>
<tr>
<td>authenticating</td>
<td>Switch only</td>
<td>Pending RADIUS request.</td>
</tr>
<tr>
<td>rejected-no vlan</td>
<td>No network access</td>
<td>1. Invalid credentials supplied.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. RADIUS Server difficulties. See log file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. If unauth-vid is specified it cannot be successfully applied to the port. An authorized client on the port has precedence.</td>
</tr>
<tr>
<td>rejected-unauth vlan</td>
<td>Unauthorized VLAN only</td>
<td>1. Invalid credentials supplied.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. RADIUS Server difficulties. See log file.</td>
</tr>
<tr>
<td>timed out-no vlan</td>
<td>No network access</td>
<td>RADIUS request timed out. If unauth-vid is specified it cannot be successfully applied to the port. An authorized client on the port has precedence. Credentials resubmitted after quiet-period expires.</td>
</tr>
<tr>
<td>timed out-unauth vlan</td>
<td>Unauthorized VLAN only</td>
<td>RADIUS request timed out. After the quiet-period expires credentials are resubmitted when client generates traffic.</td>
</tr>
<tr>
<td>unauthenticated</td>
<td>Switch only</td>
<td>Waiting for user credentials.</td>
</tr>
</tbody>
</table>
Web and MAC Authentication
Client Status
TACACS+ Authentication

Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view the switch’s authentication configuration</td>
<td>n/a</td>
<td>—</td>
<td>page 4-8</td>
<td>—</td>
</tr>
<tr>
<td>view the switch’s TACACS+ server contact configuration</td>
<td>n/a</td>
<td>—</td>
<td>page 4-9</td>
<td>—</td>
</tr>
<tr>
<td>configure the switch’s authentication methods</td>
<td>disabled</td>
<td>—</td>
<td>page 4-10</td>
<td>—</td>
</tr>
<tr>
<td>configure the switch to contact TACACS+ server(s)</td>
<td>disabled</td>
<td>—</td>
<td>page 4-17</td>
<td>—</td>
</tr>
</tbody>
</table>

TACACS+ authentication enables you to use a central server to allow or deny access to the switches covered in this guide (and other TACACS-aware devices) in your network. This means that you can use a central database to create multiple unique username/password sets with associated privilege levels for use by individuals who have reason to access the switch from either the switch’s console port (local access) or Telnet (remote access).

Figure 4-1. Example of TACACS+ Operation
TACACS+ Authentication

Terminology Used in TACACS Applications:

TACACS+ in the switches covered in this guide manages authentication of logon attempts through either the Console port or Telnet. TACACS+ uses an authentication hierarchy consisting of (1) remote passwords assigned in a TACACS+ server and (2) local passwords configured on the switch. That is, with TACACS+ configured, the switch first tries to contact a designated TACACS+ server for authentication services. If the switch fails to connect to any TACACS+ server, it defaults to its own locally assigned passwords for authentication control if it has been configured to do so. For both Console and Telnet access you can configure a login (read-only) and an enable (read/write) privilege level access.

TACACS+ does not affect WebAgent access. See “Controlling WebAgent Access” on page 4-27.

---

Terminology Used in TACACS Applications:

- **NAS (Network Access Server):** This is an industry term for a TACACS-aware device that communicates with a TACACS server for authentication services. Some other terms you may see in literature describing TACACS operation are communication server, remote access server, or terminal server. These terms apply to a switch when TACACS+ is enabled on the switch (that is, when the switch is TACACS-aware).

- **TACACS+ Server:** The server or management station configured as an access control server for TACACS-enabled devices. To use TACACS+ with a switch covered in this guide and any other TACACS-capable devices in your network, you must purchase, install, and configure a TACACS+ server application on a networked server or management station in the network. The TACACS+ server application you install will provide various options for access control and access notifications. For more on the TACACS+ services available to you, see the documentation provided with the TACACS+ server application you will use.

- **Authentication:** The process for granting user access to a device through entry of a user name and password and comparison of this username/password pair with previously stored username/password data. Authentication also grants levels of access, depending on the privileges assigned to a user name and password pair by a system administrator.
• **Local Authentication:** This method uses username/password pairs configured locally on the switch; one pair each for manager-level and operator-level access to the switch. You can assign local usernames and passwords through the CLI or WebAgent. (Using the menu interface you can assign a local password, but not a username.) Because this method assigns passwords to the switch instead of to individuals who access the switch, you must distribute the password information on each switch to everyone who needs to access the switch, and you must configure and manage password protection on a per-switch basis. (For more on local authentication, refer to chapter 2, “Configuring Username and Password Security”.)

• **TACACS+ Authentication:** This method enables you to use a TACACS+ server in your network to assign a unique password, user name, and privilege level to each individual or group who needs access to one or more switches or other TACACS-aware devices. This allows you to administer primary authentication from a central server, and to do so with more options than you have when using only local authentication. (You will still need to use local authentication as a backup if your TACACS+ servers become unavailable.) This means, for example, that you can use a central TACACS+ server to grant, change, or deny access to a specific individual on a specific switch instead of having to change local user name and password assignments on the switch itself, and then have to notify other users of the change.
General System Requirements

To use TACACS+ authentication, you need the following:

- A TACACS+ server application installed and configured on one or more servers or management stations in your network. (There are several TACACS+ software packages available.)
- A switch configured for TACACS+ authentication, with access to one or more TACACS+ servers.

Notes

The effectiveness of TACACS+ security depends on correctly using your TACACS+ server application. For this reason, HP recommends that you thoroughly test all TACACS+ configurations used in your network.

TACACS-aware HP switches include the capability of configuring multiple backup TACACS+ servers. HP recommends that you use a TACACS+ server application that supports a redundant backup installation. This allows you to configure the switch to use a backup TACACS+ server if it loses access to the first-choice TACACS+ server.

TACACS+ does not affect WebAgent access. Refer to “Controlling WebAgent Access When Using TACACS+ Authentication” on page 4-27.

General Authentication Setup Procedure

It is important to test the TACACS+ service before fully implementing it. Depending on the process and parameter settings you use to set up and test TACACS+ authentication in your network, you could accidentally lock all users, including yourself, out of access to a switch. While recovery is simple, it may pose an inconvenience that can be avoided. To prevent an unintentional lockout on the switch, use a procedure that configures and tests TACACS+ protection for one access type (for example, Telnet access), while keeping the other access type (console, in this case) open in case the Telnet access fails due to a configuration problem. The following procedure outlines a general setup procedure.
If a complete access lockout occurs on the switch as a result of a TACACS+ configuration, see “Troubleshooting TACACS+ Operation” in the Troubleshooting chapter of the Management and Configuration Guide for your switch.

1. Familiarize yourself with the requirements for configuring your TACACS+ server application to respond to requests from the switch. (Refer to the documentation provided with the TACACS+ server software.) This includes knowing whether you need to configure an encryption key. (See “Using the Encryption Key” on page 4-25.)

2. Determine the following:

- The IP address(es) of the TACACS+ server(s) you want the switch to use for authentication. If you will use more than one server, determine which server is your first-choice for authentication services.
- The encryption key, if any, for allowing the switch to communicate with the server. You can use either a global key or a server-specific key, depending on the encryption configuration in the TACACS+ server(s).
- The number of log-in attempts you will allow before closing a log-in session. (Default: 3)
- The period you want the switch to wait for a reply to an authentication request before trying another server.
- The username/password pairs you want the TACACS+ server to use for controlling access to the switch.
- The privilege level you want for each username/password pair administered by the TACACS+ server for controlling access to the switch.
- The username/password pairs you want to use for local authentication (one pair each for Operator and Manager levels).

3. Plan and enter the TACACS+ server configuration needed to support TACACS+ operation for Telnet access (login and enable) to the switch. This includes the username/password sets for logging in at the Operator (read-only) privilege level and the sets for logging in at the Manager (read/write) privilege level.
TACACS+ Authentication
General Authentication Setup Procedure

Note on Privilege Levels
When a TACACS+ server authenticates an access request from a switch, it includes a privilege level code for the switch to use in determining which privilege level to grant to the terminal requesting access. The switch interprets a privilege level code of “15” as authorization for the Manager (read/write) privilege level access. Privilege level codes of 14 and lower result in Operator (read-only) access. Thus, when configuring the TACACS+ server response to a request that includes a username/password pair that should have Manager privileges, you must use a privilege level of 15. For more on this topic, refer to the documentation you received with your TACACS+ server application.

If you are a first-time user of the TACACS+ service, HP recommends that you configure only the minimum feature set required by the TACACS+ application to provide service in your network environment. After you have success with the minimum feature set, you may then want to try additional features that the application offers.

4. Ensure that the switch has the correct local username and password for Manager access. (If the switch cannot find any designated TACACS+ servers, the local manager and operator username/password pairs are always used as the secondary access control method.)

Caution
You should ensure that the switch has a local Manager password. Otherwise, if authentication through a TACACS+ server fails for any reason, then unauthorized access will be available through the console port or Telnet.

5. Using a terminal device connected to the switch’s console port, configure the switch for TACACS+ authentication only for telnet login access and telnet enable access. At this stage, do not configure TACACS+ authentication for console access to the switch, as you may need to use the console for access if the configuration for the Telnet method needs debugging.

6. Ensure that the switch is configured to operate on your network and can communicate with your first-choice TACACS+ server. (At a minimum, this requires IP addressing and a successful ping test from the switch to the server.)

7. On a remote terminal device, use Telnet to attempt to access the switch. If the attempt fails, use the console access to check the TACACS+ configuration on the switch. If you make changes in the switch configuration, check Telnet access again. If Telnet access still fails, check the
configuration in your TACACS+ server application for mis-configurations or missing data that could affect the server's interoperation with the switch.

8. After your testing shows that Telnet access using the TACACS+ server is working properly, configure your TACACS+ server application for console access. Then test the console access. If access problems occur, check for and correct any problems in the switch configuration, and then test console access again. If problems persist, check your TACACS+ server application for mis-configurations or missing data that could affect the console access.

9. When you are confident that TACACS+ access through both Telnet and the switch’s console operates properly, use the **write memory** command to save the switch’s running-config file to flash.

---

**Configuring TACACS+ on the Switch**

**Before You Begin**

If you are new to TACACS+ authentication, HP recommends that you read the “General Authentication Setup Procedure” on page 4-4 and configure your TACACS+ server(s) before configuring authentication on the switch.

The switch offers three command areas for TACACS+ operation:

- **show authentication** and **show tacacs**: Displays the switch’s TACACS+ configuration and status.
- **aaa authentication**: A command for configuring the switch’s authentication methods
- **tacacs-server**: A command for configuring the switch’s contact with TACACS+ servers
CLI Commands Described in this Section

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication</td>
<td>4-8</td>
</tr>
<tr>
<td>show tacacs</td>
<td>4-9</td>
</tr>
<tr>
<td>aaa authentication</td>
<td>4-10 through 4-16</td>
</tr>
</tbody>
</table>

- console
- Telnet
- `num-attempts <1-10>`

- tacacs-server 4-17
- `host <ip-addr>` 4-17
- `key` 4-21
- `timeout <1-255>` 4-23

Viewing the Switch’s Current Authentication Configuration

This command lists the number of login attempts the switch allows in a single login session, and the primary/secondary access methods configured for each type of access.

**Syntax:** show authentication

This example shows the default authentication configuration.
TACACS+ Authentication
Configuring TACACS+ on the Switch

Figure 4-2. Example Listing of the Switch's Authentication Configuration

Viewing the Switch’s Current TACACS+ Server Contact Configuration

This command lists the timeout period, encryption key, and the IP addresses of the first-choice and backup TACACS+ servers the switch can contact.

Syntax:

show tacacs

For example, if the switch was configured for a first-choice and two backup TACACS+ server addresses, the default timeout period, and "paris-1" for a (global) encryption key, show tacacs would produce a listing similar to the following:

Figure 4-3. Example of the Switch’s TACACS+ Configuration Listing
Configuring the Switch’s Authentication Methods

The **aaa authentication** command configures access control for the following access methods:

- Console
- Telnet
- SSH
- Web
- Port-access (802.1X)

However, TACACS+ authentication is only used with the console, Telnet, or SSH access methods. The command specifies whether to use a TACACS+ server or the switch’s local authentication, or (for some secondary scenarios) no authentication (meaning that if the primary method fails, authentication is denied). The command also reconfigures the number of access attempts to allow in a session if the first attempt uses an incorrect username/password pair.

Using the Privilege-Mode Option for Login

When using TACACS+ to control user access to the switch, you must first login with your username at the Operator privilege level using the password for Operator privileges, and then login again with the same username but using the Manager password to obtain Manager privileges. You can avoid this double login process by entering the `privilege-mode` option with the **aaa authentication login** command to enable TACACS+ for a single login. The switch authenticates your username/password, then requests the privilege level (Operator or Manager) that was configured on the TACACS+ server for this username/password. The TACACS+ server returns the allowed privilege level to the switch. You are placed directly into Operator or Manager mode, depending on your privilege level.

```
HP Switch(config) aaa authentication login privilege-mode
```

The **no** version of the above command disables TACACS+ single login capability.
TACACS+ Authentication
Configuring TACACS+ on the Switch

Syntax: aaa authentication

< console | telnet | ssh | web | port-access >

Selects the access method for configuration.

< enable>

The server grants privileges at the Manager privilege level.

< login [privilege-mode] >

The server grants privileges at the Operator privilege level. If the privilege-mode option is entered, TACACS+ is enabled for a single login. The authorized privilege level (Operator or Manager) is returned to the switch by the TACACS+ server.

Default: Single login disabled.

< local | tacacs | radius >

Selects the type of security access:

local — Authenticates with the Manager and Operator password you configure in the switch.

tacacs — Authenticates with a password and other data configured on a TACACS+ server.

radius — Authenticates with a password and other data configured on a RADIUS server.

[< local | none >]

If the primary authentication method fails, determines whether to use the local password as a secondary method or to disallow access.

aaa authentication num-attempts < 1-10 >

Specifies the maximum number of login attempts allowed in the current session. Default: 3
TACACS+ Authentication
Configuring TACACS+ on the Switch

Authentication Parameters

Table 4-1. AAA Authentication Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Range</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>console, Telnet, SSH, web or port-access</td>
<td>n/a</td>
<td>n/a</td>
<td>Specifies the access method used when authenticating. TACACS+ authentication only uses the console, Telnet or SSH access methods.</td>
</tr>
<tr>
<td>enable</td>
<td>n/a</td>
<td>n/a</td>
<td>Specifies the Manager (read/write) privilege level for the access method being configured.</td>
</tr>
<tr>
<td>login &lt;privilege-mode&gt;</td>
<td>privilege-mode disabled</td>
<td>n/a</td>
<td>login: Specifies the Operator (read-only) privilege level for the access method being configured. The privilege-mode option enables TACACS+ for a single login. The authorized privilege level (Operator or Manager) is returned to the switch by the TACACS+ server.</td>
</tr>
<tr>
<td>local - or - tacacs</td>
<td>local</td>
<td>n/a</td>
<td>Specifies the primary method of authentication for the access method being configured. local: Use the username/password pair configured locally in the switch for the privilege level being configured tacacs: Use a TACACS+ server.</td>
</tr>
<tr>
<td>local - or - none</td>
<td>none</td>
<td>n/a</td>
<td>Specifies the secondary (backup) type of authentication being configured. local: The username/password pair configured locally in the switch for the privilege level being configured none: No secondary type of authentication for the specified method/privilege path. (Available only if the primary method of authentication for the access being configured is local.) Note: If you do not specify this parameter in the command line, the switch automatically assigns the secondary method as follows: • If the primary method is tacacs, the only secondary method is local. • If the primary method is local, the default secondary method is none.</td>
</tr>
<tr>
<td>num-attempts</td>
<td>3</td>
<td>1 - 10</td>
<td>In a given session, specifies how many tries at entering the correct username/password pair are allowed before access is denied and the session terminated.</td>
</tr>
</tbody>
</table>

Configuring the TACACS+ Server for Single Login

In order for the single login feature to work correctly, you need to check some entries in the User Setup on the TACACS+ server.

In the User Setup, scroll to the Advanced TACACS+ Settings section. Make sure the radio button for “Max Privilege for any AAA Client” is checked and the level is set to 15, as shown in Figure 4-4. Privileges are represented by the
numbers 0 through 15, with zero allowing only Operator privileges (and requiring two logins) and 15 representing root privileges. The root privilege level is the only level that will allow Manager level access on the switch.

Figure 4-4. Advanced TACACS+ Settings Section of the TACACS+ Server User Setup

Then scroll down to the section that begins with “Shell” (See Figure 4-5). Check the Shell box.

Check the Privilege level box and set the privilege level to 15 to allow “root” privileges. This allows you to use the single login option.
As shown in the next table, login and enable access is always available locally through a direct terminal connection to the switch's console port. However, for Telnet access, you can configure TACACS+ to deny access if a TACACS+ server goes down or otherwise becomes unavailable to the switch.
## TACACS+ Authentication

### Configuring TACACS+ on the Switch

#### Table 4-2. Primary/Secondary Authentication Table

<table>
<thead>
<tr>
<th>Access Method and Privilege Level</th>
<th>Authentication Options</th>
<th>Effect on Access Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Primary</td>
<td>Secondary</td>
</tr>
<tr>
<td>Console — Login</td>
<td>local</td>
<td>none*</td>
</tr>
<tr>
<td></td>
<td>tacacs</td>
<td>local</td>
</tr>
<tr>
<td>Console — Enable</td>
<td>local</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>tacacs</td>
<td>local</td>
</tr>
<tr>
<td>Telnet — Login</td>
<td>local</td>
<td>none*</td>
</tr>
<tr>
<td></td>
<td>tacacs</td>
<td>local</td>
</tr>
<tr>
<td></td>
<td>tacacs</td>
<td>none</td>
</tr>
<tr>
<td>Telnet — Enable</td>
<td>local</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>tacacs</td>
<td>local</td>
</tr>
<tr>
<td></td>
<td>tacacs</td>
<td>none</td>
</tr>
</tbody>
</table>

#### Caution Regarding the Use of Local for Login Primary Access

During local authentication (which uses passwords configured in the switch instead of in a TACACS+ server), the switch grants read-only access if you enter the Operator password, and read-write access if you enter the Manager password. For example, if you configure authentication on the switch with Telnet Login Primary as Local and Telnet Enable Primary as Tacacs, when you attempt to Telnet to the switch, you will be prompted for a local password. If you enter the switch's local Manager password (or, if there is no local Manager password configured in the switch) you can bypass the TACACS+ server authentication for Telnet Enable Primary and go directly to read-write (Manager) access. Thus, for either the Telnet or console access method, configuring Login Primary for Local authentication while configuring Enable Primary for TACACS+ authentication is not recommended, as it defeats the purpose of using the TACACS+ authentication. If you want Enable Primary log-in attempts to go to a TACACS+ server, then you should configure both Login Primary and Enable Primary for Tacacs authentication instead of configuring Login Primary to Local authentication.
For example, here is a set of access options and the corresponding commands to configure them:

**Console Login (Operator or Read-Only) Access:** Primary using TACACS+ server. Secondary using Local.

```
HP Switch(config)# aaa authentication console login tacacs local
```

**Console Enable (Manager or Read/Write) Access:** Primary using TACACS+ server. Secondary using Local.

```
HP Switch(config)# aaa authentication console enable tacacs local
```

**Telnet Login (Operator or Read-Only) Access:** Primary using TACACS+ server. Secondary using Local.

```
HP Switch(config)# aaa authentication Telnet login tacacs local
```

**Telnet Enable (Manager or Read/Write Access:** Primary using TACACS+ server. Secondary using Local.

```
HP Switch(config)# aaa authentication telnet enable tacacs local
```

**Deny Access and Close the Session After Failure of Two Consecutive Username/Password Pairs:**

```
HP Switch(config)# aaa authentication num-attempts 2
```
Configuring the Switch’s TACACS+ Server Access

The tacacs-server command configures these parameters:

- **The host IP address(es)** for up to three TACACS+ servers; one first-choice and up to two backups. Designating backup servers provides for a continuation of authentication services in case the switch is unable to contact the first-choice server.

- **An optional encryption key.** This key helps to improve security, and must match the encryption key used in your TACACS+ server application. In some applications, the term “secret key” or “secret” may be used instead of “encryption key”. If you need only one encryption key for the switch to use in all attempts to authenticate through a TACACS+ server, configure a global key. However, if the switch is configured to access multiple TACACS+ servers having different encryption keys, you can configure the switch to use different encryption keys for different TACACS+ servers.

- **The timeout value** in seconds for attempts to contact a TACACS+ server. If the switch sends an authentication request, but does not receive a response within the period specified by the timeout value, the switch resends the request to the next server in its Server IP Addr list, if any. If the switch still fails to receive a response from any TACACS+ server, it reverts to whatever secondary authentication method was configured using the `aaa authentication` command (local or none; see “Configuring the Switch’s Authentication Methods” on page 4-10.)

---

**Note**

As described under “General Authentication Setup Procedure” on page 4-4, HP recommends that you configure, test, and troubleshoot authentication via Telnet access before you configure authentication via console port access. This helps to prevent accidentally locking yourself out of switch access due to errors or problems in setting up authentication in either the switch or your TACACS+ server.
TACACS+ Authentication
Configuring TACACS+ on the Switch

**Syntax:**
```
tacacs-server host <ip-addr> [key <key-string>]
```

Adds a TACACS+ server and optionally assigns a server-specific encryption key. If the switch is configured to access multiple TACACS+ servers having different encryption keys, you can configure the switch to use different encryption keys for different TACACS+ servers.

```
[no] tacacs-server host <ip-addr>
```

Removes a TACACS+ server assignment (including its server-specific encryption key, if any).

```
tacacs-server [key <key-string>]
```

Configures an optional global encryption key. Keys configured in the switch must exactly match the encryption keys configured in the TACACS+ servers that the switch will attempt to use for authentication.

```
[no] tacacs-server key
```

Removes the optional global encryption key. (Does not affect any server-specific encryption key assignments.)

```
tacacs-server timeout <1-255>
```

Changes the wait period for a TACACS server response.
( Default: 5 seconds.)
TACACS+ Authentication
Configuring TACACS+ on the Switch

### Name

<table>
<thead>
<tr>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>host &lt;ip-addr&gt; [key &lt;key-string&gt;]</td>
<td>none</td>
</tr>
</tbody>
</table>

Specifies the IP address of a device running a TACACS+ server application. Optionally, can also specify the unique, per-server encryption key to use when each assigned server has its own, unique key. For more on the encryption key, see “Using the Encryption Key” on page 4-25 and the documentation provided with your TACACS+ server application.

You can enter up to three IP addresses; one first-choice and two (optional) backups (one second-choice and one third-choice).

Use `show tacacs` to view the current IP address list.

If the first-choice TACACS+ server fails to respond to a request, the switch tries the second address, if any, in the `show tacacs` list. If the second address also fails, then the switch tries the third address, if any.

(See figure 4-3, “Example of the Switch’s TACACS+ Configuration Listing” on p. 4-9.)

The priority (first-choice, second-choice, and third-choice) of a TACACS+ server in the switch’s TACACS+ configuration depends on the order in which you enter the server IP addresses:

1. When there are no TACACS+ servers configured, entering a server IP address makes that server the first-choice TACACS+ server.

2. When there is one TACACS+ server already configured, entering another server IP address makes that server the second-choice (backup) TACACS+ server.

3. When there are two TACACS+ servers already configured, entering another server IP address makes that server the third-choice (backup) TACACS+ server.

- The above position assignments are fixed. Thus, if you remove one server and replace it with another, the new server assumes the priority position that the removed server had. For example, suppose you configured three servers, A, B, and C, configured in order:
  
  First-Choice: A  
  Second-Choice: B  
  Third-Choice: C  

  If you removed server B and then entered server X, the TACACS+ server order of priority would be:
  
  First-Choice: A  
  Second-Choice: X  
  Third-Choice: C  

- If there are two or more vacant slots in the TACACS+ server priority list and you enter a new IP address, the new address will take the vacant slot with the highest priority. Thus, if A, B, and C are configured as above and you (1) remove A and B, and (2) enter X and Y (in that order), then the new TACACS+ server priority list would be X, Y, and C.

- The easiest way to change the order of the TACACS+ servers in the priority list is to remove all server addresses in the list and then re-enter them in order, with the new first-choice server address first, and so on.

To add a new address to the list when there are already three addresses present, you must first remove one of the currently listed addresses.

See also “General Authentication Process Using a TACACS+ Server” on page 4-23.
TACACS+ Authentication
Configuring TACACS+ on the Switch

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>key &lt;key-string&gt;</td>
<td>none (null)</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Specifies the optional, global “encryption key” that is also assigned in the TACACS+ server(s) that the switch will access for authentication. This option is subordinate to any “per-server” encryption keys you assign, and applies only to accessing TACACS+ servers for which you have not given the switch a “per-server” key. (See the host <ip-addr> [key <key-string>] entry at the beginning of this table.)

You can configure a TACACS+ encryption key that includes a tilde (~) as part of the key, for example, “hp~switch”. It is not backward compatible; the “~” character is lost if you use a software version that does not support the “~” character. For more on the encryption key, see “Using the Encryption Key” on page 4-25 and the documentation provided with your TACACS+ server application.

| timeout <1 - 255> | 5 sec | 1 - 255 sec |

Specifies how long the switch waits for a TACACS+ server to respond to an authentication request. If the switch does not detect a response within the timeout period, it initiates a new request to the next TACACS+ server in the list. If all TACACS+ servers in the list fail to respond within the timeout period, the switch uses either local authentication (if configured) or denies access (if none configured for local authentication).

HP Switch(config)# tacacs-server host 10.10.10.2 key hp~switch

Figure 4-6. Example of Configuring a Host-Specific Key

Use the show running-config command to display the key information.

HP Switch(config)# show running-config

Running configuration:

; J8692A Configuration Editor; Created on release JW.15.xx
hostname "HP Switch"
module 1 type J86xxA
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address dhcp-bootp
exit
banner motd "good morning"
tacacs-server host 10.10.10.2 key "hp~switch"  Shows the key configured for a specific host.
snmp-server community "public" unrestricted

Figure 4-7. Example of the Running Configuration File Showing the Host-Specific Key for TACACS+ with the "~" Included
Adding, Removing, or Changing the Priority of a TACACS+ Server.

Suppose that the switch was already configured to use TACACS+ servers at 10.28.227.10 and 10.28.227.15. In this case, 10.28.227.15 was entered first, and so is listed as the first-choice server:

```
Figure 4-8. Example of the Switch with Two TACACS+ Server Addresses Configured
```

To move the “first-choice” status from the “15” server to the “10” server, use the `no tacacs-server host <ip-addr>` command to delete both servers, then use `tacacs-server host <ip-addr>` to re-enter the “10” server first, then the “15” server.

The servers would then be listed with the new “first-choice” server, that is:

```
Figure 4-9. Example of the Switch After Assigning a Different “First-Choice” Server
```

To remove the 10.28.227.15 device as a TACACS+ server, you would use this command:

```
HP Switch(config)# no tacacs-server host 10.28.227.15
```

Configuring an Encryption Key. Use an encryption key in the switch if the switch will be requesting authentication from a TACACS+ server that also uses an encryption key. (If the server expects a key, but the switch either does not provide one, or provides an incorrect key, then the authentication attempt will fail.) Use a `global encryption key` if the same key applies to all TACACS+ servers.
servers the switch may use for authentication attempts. Use a per-server encryption key if different servers the switch may use will have different keys. (For more details on encryption keys, see “Using the Encryption Key” on page 4-25.)

To configure north01 as a global encryption key:

HP Switch(config)# tacacs-server key north01

To configure north01 as a per-server encryption key:

HP Switch(config)# tacacs-server host 10.28.227.63 key north01

An encryption key can contain up to 100 characters, without spaces, and is likely to be case-sensitive in most TACACS+ server applications.

To delete a global encryption key from the switch, use this command:

HP Switch(config)# no tacacs-server key

To delete a per-server encryption key in the switch, re-enter the tacacs-server host command without the key parameter. For example, if you have north01 configured as the encryption key for a TACACS+ server with an IP address of 10.28.227.104 and you want to eliminate the key, you would use this command:

HP Switch(config)# tacacs-server host 10.28.227.104

---

**Note**

You can save the encryption key in a configuration file by entering this command:

HP Switch(config)# tacacs-server key <keystring>

The <keystring> parameter is the encryption key in clear text.

---

**Note**

The show tacacs command lists the global encryption key, if configured. However, to view any configured per-server encryption keys, you must use show config or show config running (if you have made TACACS+ configuration changes without executing write mem).
Configuring the Timeout Period. The timeout period specifies how long the switch waits for a response to an authentication request from a TACACS+ server before either sending a new request to the next server in the switch’s Server IP Address list or using the local authentication option. For example, to change the timeout period from 5 seconds (the default) to 3 seconds:

HP Switch(config)# tacacs-server timeout 3

How Authentication Operates
General Authentication Process Using a TACACS+ Server

Authentication through a TACACS+ server operates generally as described below. For specific operating details, refer to the documentation you received with your TACACS+ server application.

Using figure 4-10, above, after either switch detects an operator’s logon request from a remote or directly connected terminal, the following events occur:

1. The switch queries the first-choice TACACS+ server for authentication of the request.
   - If the switch does not receive a response from the first-choice TACACS+ server, it attempts to query a secondary server. If the switch does not receive a response from any TACACS+ server,
TACACS+ Authentication
How Authentication Operates

then it uses its own local username/password pairs to authenticate the logon request. (See “Local Authentication Process” on page 4-24.)

- If a TACACS+ server recognizes the switch, it forwards a username prompt to the requesting terminal via the switch.

2. When the requesting terminal responds to the prompt with a username, the switch forwards it to the TACACS+ server.

3. After the server receives the username input, the requesting terminal receives a password prompt from the server via the switch.

4. When the requesting terminal responds to the prompt with a password, the switch forwards it to the TACACS+ server and one of the following actions occurs:

- If the username/password pair received from the requesting terminal matches a username/password pair previously stored in the server, then the server passes access permission through the switch to the terminal.

- If the username/password pair entered at the requesting terminal does not match a username/password pair previously stored in the server, access is denied. In this case, the terminal is again prompted to enter a username and repeat steps 2 through 4. In the default configuration, the switch allows up to three attempts to authenticate a login session. If the requesting terminal exhausts the attempt limit without a successful TACACS+ authentication, the login session is terminated and the operator at the requesting terminal must initiate a new session before trying again.

Local Authentication Process

When the switch is configured to use TACACS+, it reverts to local authentication only if one of these two conditions exists:

- “Local” is the authentication option for the access method being used.

- TACACS+ is the primary authentication mode for the access method being used. However, the switch was unable to connect to any TACACS+ servers (or no servers were configured) AND Local is the secondary authentication mode being used.

(For a listing of authentication options, see table 4-2, “Primary/Secondary Authentication Table” on 4-15.)
For local authentication, the switch uses the operator-level and manager-level username/password set(s) previously configured locally on the switch. (These are the usernames and passwords you can configure using the CLI password command, the WebAgent, or the menu interface—which enables only local password configuration).

- If the operator at the requesting terminal correctly enters the username/password pair for either access level, access is granted.

- If the username/password pair entered at the requesting terminal does not match either username/password pair previously configured locally in the switch, access is denied. In this case, the terminal is again prompted to enter a username/password pair. In the default configuration, the switch allows up to three attempts. If the requesting terminal exhausts the attempt limit without a successful authentication, the login session is terminated and the operator at the requesting terminal must initiate a new session before trying again.

**Note**

The switch’s menu allows you to configure only the local Operator and Manager passwords, and not any usernames. In this case, all prompts for local authentication will request only a local password. However, if you use the CLI or the WebAgent to configure usernames for local access, you will see a prompt for both a local username and a local password during local authentication.

**Using the Encryption Key**

**General Operation**

When used, the encryption key (sometimes termed “key”, “secret key”, or “secret”) helps to prevent unauthorized intruders on the network from reading username and password information in TACACS+ packets moving between the switch and a TACACS+ server. At the TACACS+ server, a key may include both of the following:

- **Global key**: A general key assignment in the TACACS+ server application that applies to all TACACS-aware devices for which an individual key has not been configured.

- **Server-Specific key**: A unique key assignment in the TACACS+ server application that applies to a specific TACACS-aware device.
**TACACS+ Authentication**  
**How Authentication Operates**

---

**Note**

Configure a key in the switch only if the TACACS+ server application has this exact same key configured for the switch. That is, if the key parameter in switch “X” does not exactly match the key setting for switch “X” in the TACACS+ server application, then communication between the switch and the TACACS+ server will fail.

Thus, on the TACACS+ server side, you have a choice as to how to implement a key. On the switch side, it is necessary only to enter the key parameter so that it exactly matches its counterpart in the server. For information on how to configure a general or individual key in the TACACS+ server, refer to the documentation you received with the application.

**Encryption Options in the Switch**

When configured, the encryption key causes the switch to encrypt the TACACS+ packets it sends to the server. When left at “null”, the TACACS+ packets are sent in clear text. The encryption key (or just "key") you configure in the switch must be identical to the encryption key configured in the corresponding TACACS+ server. If the key is the same for all TACACS+ servers the switch will use for authentication, then configure a global key in the switch. If the key is different for one or more of these servers, use “server-specific” keys in the switch. (If you configure both a global key and one or more per-server keys, the per-server keys will override the global key for the specified servers.)

For example, you would use the next command to configure a global encryption key in the switch to match a key entered as `north40campus` in two target TACACS+ servers. (That is, both servers use the same key for your switch.) Note that you do not need the server IP addresses to configure a global key in the switch:

```bash
HP Switch(config)# tacacs-server key north40campus
```

Suppose that you subsequently add a third TACACS+ server (with an IP address of 10.28.227.87) that has `south10campus` for an encryption key. Because this key is different than the one used for the two servers in the previous example, you will need to assign a server-specific key in the switch that applies only to the designated server:

```bash
HP Switch(config)# tacacs-server host 10.28.227.87 key south10campus
```

With both of the above keys configured in the switch, the `south10campus` key overrides the `north40campus` key only when the switch tries to access the TACACS+ server having the 10.28.227.87 address.
Controlling WebAgent Access When Using TACACS+ Authentication

Configuring the switch for TACACS+ authentication does not affect WebAgent access. To prevent unauthorized access through the WebAgent, do one or more of the following:

- Configure local authentication (a Manager user name and password and, optionally, an Operator user name and password) on the switch.

- Configure the switch’s Authorized IP Manager feature to allow WebAgent access only from authorized management stations. (The Authorized IP Manager feature does not interfere with TACACS+ operation.)

- Disable WebAgent access to the switch by going to the System Information screen in the Menu interface and configuring the Web Agent Enabled parameter to No.
### Messages Related to TACACS+ Operation

The switch generates the CLI messages listed below. However, you may see other messages generated in your TACACS+ server application. For information on such messages, refer to the documentation you received with the application.

<table>
<thead>
<tr>
<th>CLI Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting to Tacacs server</td>
<td>The switch is attempting to contact the TACACS+ server identified in the switch's <code>tacacs-server</code> configuration as the first-choice (or only) TACACS+ server.</td>
</tr>
<tr>
<td>Connecting to secondary Tacacs server</td>
<td>The switch was not able to contact the first-choice TACACS+ server, and is now attempting to contact the next (secondary) TACACS+ server identified in the switch's <code>tacacs-server</code> configuration.</td>
</tr>
<tr>
<td>Invalid password</td>
<td>The system does not recognize the username or the password or both. Depending on the authentication method (tacacs or local), either the TACACS+ server application did not recognize the username/password pair or the username/password pair did not match the username/password pair configured in the switch.</td>
</tr>
<tr>
<td>No Tacacs servers responding</td>
<td>The switch has not been able to contact any designated TACACS+ servers. If this message is followed by the Username prompt, the switch is attempting local authentication.</td>
</tr>
<tr>
<td>Not legal combination of authentication methods</td>
<td>For console access, if you select tacacs as the primary authentication method, you must select local as the secondary authentication method. This prevents you from being locked out of the switch if all designated TACACS+ servers are inaccessible to the switch.</td>
</tr>
<tr>
<td>Record already exists</td>
<td>When resulting from a <code>tacacs-server host &lt;ip addr&gt;</code> command, indicates an attempt to enter a duplicate TACACS+ server IP address.</td>
</tr>
</tbody>
</table>
Operating Notes

- If you configure Authorized IP Managers on the switch, it is not necessary to include any devices used as TACACS+ servers in the authorized manager list. That is, authentication traffic between a TACACS+ server and the switch is not subject to Authorized IP Manager controls configured on the switch. Also, the switch does not attempt TACACS+ authentication for a management station that the Authorized IP Manager list excludes because, independent of TACACS+, the switch already denies access to such stations.

- When TACACS+ is not enabled on the switch—or when the switch’s only designated TACACS+ servers are not accessible—setting a local Operator password without also setting a local Manager password does not protect the switch from manager-level access by unauthorized persons.

- When using the copy command to transfer a configuration to a TFTP server, any optional, server-specific and global encryption keys (page 4-17) in the TACACS configuration will not be included in the transferred file. Otherwise, a security breach could occur, allowing access to the TACACS+ username/password information.
TACACS+ Authentication
Operating Notes
RADIUS Authentication, Authorization, and Accounting

Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>WebAgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring RADIUS Authentication</td>
<td>None</td>
<td>n/a</td>
<td>5-7</td>
<td>n/a</td>
</tr>
<tr>
<td>Configuring RADIUS Accounting</td>
<td>None</td>
<td>n/a</td>
<td>5-47</td>
<td>n/a</td>
</tr>
<tr>
<td>Configuring RADIUS Authorization</td>
<td>None</td>
<td>n/a</td>
<td>5-33</td>
<td>n/a</td>
</tr>
<tr>
<td>Viewing RADIUS Statistics</td>
<td>n/a</td>
<td>n/a</td>
<td>5-62</td>
<td>n/a</td>
</tr>
</tbody>
</table>

RADIUS (Remote Authentication Dial-In User Service) enables you to use up to fifteen servers and maintain separate authentication and accounting for each RADIUS server employed. For authentication, this allows a different password for each user instead of having to rely on maintaining and distributing switch-specific passwords to all users. For accounting, this can help you track network resource usage.

Authentication Services

You can use RADIUS to verify user identity for the following types of primary password access to the HP switch:

- Serial port (Console)
- Telnet
- SSH
- SFTP/SCP
- Web Agent
- Port-Access (802.1X)
RADIUS Authentication, Authorization, and Accounting

Overview

The switch also supports RADIUS accounting for Web Authentication and MAC authentication sessions.

Note

The switch does not support RADIUS security for SNMP (network management) access. For information on blocking access through the WebAgent, refer to “Controlling WebAgent Access” on page 5-32.

Accounting Services

RADIUS accounting on the switch collects resource consumption data and forwards it to the RADIUS server. This data can be used for trend analysis, capacity planning, billing, auditing, and cost analysis.

Accounting support is provided for Web Agent sessions on the switch. The service types supported are Exec accounting and Commands accounting.

RADIUS-Administered CoS and Rate-Limiting

The switches covered in this guide take advantage of vendor-specific attributes (VSAs) applied in a RADIUS server to support these optional, RADIUS-assigned attributes:

- 802.1p (CoS) priority assignment to inbound traffic on the specified port(s) (port-access authentication only)
- Per-Port Rate-Limiting on a port with an active link to an authenticated client (port-access authentication only)

RADIUS-Administered Commands Authorization

This feature enables RADIUS server control of an authenticated client’s access to CLI commands on the switch. Refer to “Commands Authorization” on page 5-33.
SNMP Access to the Switch’s Authentication Configuration MIB

The switch’s default configuration allows SNMP access to the hpSwitchAuth MIB (Management Information Base). A management station running an SNMP networked device management application such as HP PCM+ or HP OpenView can access the switch’s MIB for read access to the switch’s status and read/write access to the switch’s configuration. For more information, including the CLI command to use for disabling this feature, refer to “Using SNMP To View and Configure Switch Authentication Features” on page 5-27.
Terminology

**AAA**: Authentication, Authorization, and Accounting groups of services provided by the carrying protocol.

**CHAP (Challenge-Handshake Authentication Protocol)**: A challenge-response authentication protocol that uses the Message Digest 5 (MD5) hashing scheme to encrypt a response to a challenge from a RADIUS server.

**CoS (Class of Service)**: Support for priority handling of packets traversing the switch, based on the IEEE 802.1p priority carried by each packet. (For more on this topic, refer to the “Overview” section in the “Quality of Service (QoS)” chapter in the *Advanced Traffic Management Guide* for your switch.)

**EAP (Extensible Authentication Protocol)**: A general PPP authentication protocol that supports multiple authentication mechanisms. A specific authentication mechanism is known as an EAP type, such as MD5-Challenge, Generic Token Card, and TLS (Transport Level Security).

**EXEC Session**: a service (EXEC shell) granted to the authenticated login user for doing management operations on the HP device.

**Host**: See RADIUS Server.

**NAS (Network Access Server)**: In this case, a HP switch configured for RADIUS security operation.

**RADIUS (Remote Authentication Dial In User Service)**: a protocol for carrying authentication, authorization, and accounting information between a Network Access Server and shared AAA servers in a distributed dial-in networking environment.

**RADIUS Client**: The device that passes user information to designated RADIUS servers.

**RADIUS Host**: See RADIUS server.

**RADIUS Server**: A server running the RADIUS application you are using on your network. This server receives user connection requests from the switch, authenticates users, and then returns all necessary information to the switch. For the HP switch, a RADIUS server can also perform accounting functions. Sometimes termed a *RADIUS host.*
RADIUS Authentication, Authorization, and Accounting

Switch Operating Rules for RADIUS

**Shared Secret Key:** A text value used for encrypting data in RADIUS packets. Both the RADIUS client and the RADIUS server have a copy of the key, and the key is never transmitted across the network.

**Vendor-Specific Attribute:** A vendor-defined value configured in a RADIUS server to specify an optional switch feature assigned by the server during an authenticated client session.

---

Switch Operating Rules for RADIUS

- You must have at least one RADIUS server accessible to the switch.
- The switch supports authentication and accounting using up to fifteen RADIUS servers. The switch accesses the servers in the order in which they are listed by `show radius` (page 5-62). If the first server does not respond, the switch tries the next one, and so on. (To change the order in which the switch accesses RADIUS servers, refer to “Changing RADIUS-Server Access Order” on page 5-67.)
- You can select RADIUS as the primary authentication method for each type of access. (Only one primary and one secondary access method is allowed for each access type.)
- In the HP switch, EAP RADIUS uses MD5 and TLS to encrypt a response to a challenge from a RADIUS server.
- When primary/secondary authentication is set to Radius/Local (for either Login or Enable) and the RADIUS server fails to respond to a client attempt to authenticate, the failure is noted in the Event Log with the message `radius: Can't reach RADIUS server < server-ip-addr >`. When this type of failure occurs, the switch prompts the client again to enter a username and password. In this case, use the local username (if any) and password configured on the switch itself.
- Zero-length usernames or passwords are not allowed for RADIUS authentication, even though allowed by some RADIUS servers.
- TACACS+ is not supported for the WebAgent access.
General RADIUS Setup Procedure

Preparation:

1. Configure one to fifteen RADIUS servers to support the switch. Refer to the documentation provided with the RADIUS server application.

2. Before configuring the switch, collect the information outlined below.

Table 5-1. Preparation for Configuring RADIUS on the Switch

- Determine the access methods (console, Telnet, Port-Access (802.1X), WebAgent and/or SSH) for which you want RADIUS as the primary authentication method. Consider both Operator (login) and Manager (enable) levels, as well as which secondary authentication methods to use (local or none) if the RADIUS authentication fails or does not respond.

```
HP Switch(config)# show authentication
Status and Counters - Authentication Information
Login Attempts : 3
Respect Privilege : Disabled

<table>
<thead>
<tr>
<th>Login</th>
<th>Login</th>
<th>Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Task</td>
<td>Primary</td>
<td>Server Group</td>
</tr>
<tr>
<td>Console</td>
<td>Local</td>
<td>Local</td>
</tr>
<tr>
<td>Telnet</td>
<td>Local</td>
<td>None</td>
</tr>
<tr>
<td>Port-Access</td>
<td>Local</td>
<td>None</td>
</tr>
<tr>
<td>Webui</td>
<td>Local</td>
<td>None</td>
</tr>
<tr>
<td>SSH</td>
<td>Local</td>
<td>None</td>
</tr>
<tr>
<td>Web-Auth</td>
<td>ChapRadius radius</td>
<td>None</td>
</tr>
<tr>
<td>MAC-Auth</td>
<td>ChapRadius radius</td>
<td>None</td>
</tr>
<tr>
<td>SNMP</td>
<td>Local</td>
<td>None</td>
</tr>
</tbody>
</table>

| Access Task | Primary | Server Group | Secondary |
| Console | Local | None | |
| Telnet | Local | None | |
| Webui | Local | None | |
| SSH | Local | None | |
```

Note: The WebAgent access task shown in this figure is available only on the switches covered in this guide.

Console access requires Local as secondary method to prevent lockout if the primary RADIUS access fails due to loss of RADIUS server access or other problems with the server.

Figure 5-1. Example of Possible RADIUS Access Assignments
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

- Determine the IP address(es) of the RADIUS server(s) you want to support the switch. (You can configure the switch for up to fifteen RADIUS servers.)
- If you need to replace the default UDP destination port (1812) the switch uses for authentication requests to a specific RADIUS server, select it before beginning the configuration process.
- If you need to replace the default UDP destination port (1813) the switch uses for accounting requests to a specific Radius server, select it before beginning the configuration process.
- Determine whether you can use one, global encryption key for all RADIUS servers or if unique keys will be required for specific servers. With multiple RADIUS servers, if one key applies to two or more of these servers, then you can configure this key as the global encryption key. For any server whose key differs from the global key you are using, you must configure that key in the same command that you use to designate that server’s IP address to the switch.
- Determine an acceptable timeout period for the switch to wait for a server to respond to a request. HP recommends that you begin with the default (five seconds).
- Determine how many times you want the switch to try contacting a RADIUS server before trying another RADIUS server or quitting. (This depends on how many RADIUS servers you have configured the switch to access.)
- Determine whether you want to bypass a RADIUS server that fails to respond to requests for service. To shorten authentication time, you can set a bypass period in the range of 1 to 1440 minutes for non-responsive servers. This requires that you have multiple RADIUS servers accessible for service requests.
- Optional: Determine whether the switch access level (Manager or Operator) for authenticated clients can be set by a Service Type value the RADIUS server includes in its authentication message to the switch. (Refer to “2. Enable the (Optional) Access Privilege Option” on page 5-12.)
- Configure RADIUS on the server(s) used to support authentication on the switch.

## Configuring the Switch for RADIUS Authentication

<table>
<thead>
<tr>
<th>RADIUS Authentication Commands</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication</td>
<td>5-9</td>
</tr>
<tr>
<td>console</td>
<td>telnet</td>
</tr>
<tr>
<td>web-based</td>
<td>mac-based</td>
</tr>
<tr>
<td>[ local</td>
<td>none</td>
</tr>
<tr>
<td>[login privilege-mode]*</td>
<td>5-12</td>
</tr>
<tr>
<td>[no] radius-server host &lt; IP-address &gt;</td>
<td>5-14</td>
</tr>
<tr>
<td>[auth-port &lt; port-number &gt;]</td>
<td>5-14</td>
</tr>
<tr>
<td>[acct-port &lt; port-number &gt;]</td>
<td>5-14, 5-53</td>
</tr>
<tr>
<td>[dyn-authorization]</td>
<td>5-15</td>
</tr>
<tr>
<td>[key &lt; server-specific key-string &gt;]</td>
<td>5-14</td>
</tr>
<tr>
<td>[no] radius-server key &lt; global key-string &gt;</td>
<td>5-18</td>
</tr>
</tbody>
</table>
### Outline of the Steps for Configuring RADIUS Authentication

There are three main steps to configuring RADIUS authentication:

1. Configure RADIUS authentication for controlling access through one or more of the following:
   - Serial port
   - Telnet
   - SSH
   - Port-Access (802.1X)
   - WebAgent

2. Enable RADIUS authentication on the switch to override the default authentication operation of automatically assigning an authenticated client to the Operator privilege level. This optional feature applies the privilege level specified by the Service Type value received from the RADIUS server. (Refer to “1. Configure Authentication for the Access Methods You Want RADIUS To Protect” on page 5-9.)

3. Configure the switch for accessing one or more RADIUS servers (one primary server and up to two backup servers):

   **Note**

   This step assumes you have already configured the RADIUS server(s) to support the switch. Refer to the documentation provided with the RADIUS server documentation.

   - Server IP address
   - (Optional) UDP destination port for authentication requests (default: 1812; recommended)
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

- (Optional) UDP destination port for accounting requests (default: 1813; recommended)
- (Optional) encryption key for use during authentication sessions with a RADIUS server. This key overrides the global encryption key you can also configure on the switch, and must match the encryption key used on the specified RADIUS server. (Default: null)

4. Configure the global RADIUS parameters.
- **Server Key:** This key must match the encryption key used on the RADIUS servers the switch contacts for authentication and accounting services unless you configure one or more per-server keys. (Default: null.)
- **Timeout Period:** The timeout period the switch waits for a RADIUS server to reply. (Default: 5 seconds; range: 1 to 15 seconds.)
- **Retransmit Attempts:** The number of retries when there is no server response to a RADIUS authentication request. (Default: 3; range of 1 to 5.)
- **Server Dead-Time:** The period during which the switch will not send new authentication requests to a RADIUS server that has failed to respond to a previous request. This avoids a wait for a request to time out on a server that is unavailable. If you want to use this feature, select a dead-time period of 1 to 1440 minutes. (Default: 0—disabled; range: 1 - 1440 minutes.) If your first-choice server was initially unavailable, but then becomes available before the dead-time expires, you can nullify the dead-time by resetting it to zero and then trying to log on again. As an alternative, you can reboot the switch, (thus resetting the dead-time counter to assume the server is available) and then try to log on again.
- **Number of Login Attempts:** This is actually an aaa authentication command. It controls how many times per session a RADIUS client (and clients using other forms of access) can try to log in with the correct username and password. (Default: Three times per session.)

(For RADIUS accounting features, refer to “Accounting Services” on page 5-47.)

1. Configure Authentication for the Access Methods You Want RADIUS To Protect

This section describes how to configure the switch for RADIUS authentication through the following access methods:

- **Console:** Either direct serial-port connection or modem connection.
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

- **Telnet**: Inbound Telnet must be enabled (the default).

- **SSH**: To use RADIUS for SSH access, first configure the switch for SSH operation. Refer to chapter 7, “Configuring Secure Shell (SSH)”.

- **WebAgent**: You can enable RADIUS authentication for WebAgent access to the switch.

You can configure RADIUS as the primary password authentication method for the above access methods. You also need to select either local, none, or authorized as a secondary, or backup, method. Note that for console access, if you configure radius (or tacacs) for primary authentication, you must configure local for the secondary method. This prevents the possibility of being completely locked out of the switch in the event that all primary access methods fail.

**Syntax:**
```
aaa authentication < console | telnet | ssh | web | < enable | login <local | radius>> web-based | mac-based <chap-radius | peap-radius>>
```

Configures RADIUS as the primary password authentication method for console, Telnet, SSH, and/or the WebAgent. (The default primary < enable | login > authentication is local.)

```
<console | telnet | ssh | web>

[< local | none | authorized >]
```

Provides options for secondary authentication (default: none). Note that for console access, secondary authentication must be local if primary access is not local. This prevents you from being locked out of the switch in the event of a failure in other access methods.

```
<<web-based | mac-based > login> <chap-radius | peap-mschapv2>:
```
Password authentication for web-based or mac-based port access to the switch. Use peap-mschapv2 when you want password verification without requiring access to a plain text password; it is more secure.

Default: chap-radius

```
[none | authorized]: Provides options for secondary authentication. The none option specifies that a backup authentication method is not used. The authorized option allows access without authentication. (default: none).
```

In certain situations, RADIUS servers can become isolated from the network. Users are not able to access the network resources configured with RADIUS access protection and are rejected. To address this situation, configuring the
authorized secondary authentication method allows users unconditional access to the network when the primary authentication method fails because the RADIUS servers are unreachable.

**Caution**

Configuring **authorized** as the secondary authentication method used when there is a failure accessing the RADIUS servers allows clients to access the network unconditionally. Use this method with care.

Figure 5-2 shows an example of the **show authentication** command displaying **authorized** as the secondary authentication method for port-access, Web-auth access, and MAC-auth access. Since the configuration of **authorized** means no authentication will be performed and the client has unconditional access to the network, the “Enable Primary” and “Enable Secondary” fields are not applicable (N/A).

---

```
HP Switch(config)# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled

<table>
<thead>
<tr>
<th>Access Task</th>
<th>Primary</th>
<th>Server Group</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Port-Access</td>
<td>Local</td>
<td>Authorized</td>
<td></td>
</tr>
<tr>
<td>Webui</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Web-Auth</td>
<td>ChapRadius</td>
<td>radius</td>
<td>Authorized</td>
</tr>
<tr>
<td>MAC-Auth</td>
<td>ChapRadius</td>
<td>radius</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Task</th>
<th>Primary</th>
<th>Server Group</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Webui</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 5-2. Example of AAA Authentication Using Authorized for the Secondary Authentication Method
RADIUS Authentication, Authorization, and Accounting

Configuring the Switch for RADIUS Authentication

Suppose you already configured local passwords on the switch, but want RADIUS to protect primary Telnet and SSH access without allowing a secondary Telnet or SSH access option (the switch's local passwords):

```
HP Switch(config)# aaa authentication telnet login radius none
HP Switch(config)# aaa authentication telnet enable radius none
HP Switch(config)# aaa authentication ssh login radius none
HP Switch(config)# aaa authentication ssh enable radius none
HP Switch(config)# show authentication
```

Status and Counters - Authentication Information

<table>
<thead>
<tr>
<th>Login Attempts</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respect Privilege</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Task</th>
<th>Primary</th>
<th>Server Group</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Radius</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Port-Access</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Webui</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Radius</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Web-Auth</td>
<td>ChapRadius</td>
<td>radius</td>
<td>None</td>
</tr>
<tr>
<td>MAC-Auth</td>
<td>ChapRadius</td>
<td>radius</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Task</th>
<th>Primary</th>
<th>Server Group</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Radius</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Webui</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Radius</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

If you configure the Login Primary method as `local` instead of `radius` (and local passwords are configured on the switch), then clients connected to your network can gain access to either the Operator or Manager level without encountering the RADIUS authentication specified for Enable Primary. Refer to “Local Authentication Process” on page 5-31.

2. Enable the (Optional) Access Privilege Option

In the default RADIUS operation, the switch automatically admits any authenticated client to the Login (Operator) privilege level, even if the RADIUS server specifies Enable (Manager) access for that client. Thus, an authenticated user
authorized for the Manager privilege level must authenticate again to change
privilege levels. Using the optional `login privilege-mode` command overrides
this default behavior for clients with Enable (manager) access. That is, with
`privilege-mode` enabled, the switch immediately allows Enable (Manager)
access to a client for whom the RADIUS server specifies this access level.

**Syntax:** `[no] aaa authentication login privilege-mode`

When enabled, the switch reads the Service-Type field in the
client authentication received from a RADIUS server. The
following table describes the applicable Service-Type values
and corresponding client access levels the switch allows upon
authentication by the server.

<table>
<thead>
<tr>
<th>Service-Type</th>
<th>Value</th>
<th>Client Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative-User</td>
<td>6</td>
<td>Manager</td>
</tr>
<tr>
<td>NAS-Prompt-User</td>
<td>7</td>
<td>Operator</td>
</tr>
<tr>
<td>Any Other Type</td>
<td>Any Value Except 6 or 7</td>
<td>Access Denied</td>
</tr>
</tbody>
</table>

This feature applies to console (serial port), Telnet, SSH, and
WebAgent access to the switch. It does not apply to 802.1X
port-access.

**Notes:** While this option is enabled, a Service-Type value
other than 6 or 7, or an unconfigured (null) Service-Type
causes the switch to deny access to the requesting client.

The `no` form of the command returns the switch to the default
RADIUS authentication operation. The default behavior for
most interfaces is that a client authorized by the RADIUS
server for Enable (Manager) access will be prompted twice,
once for Login (Operator) access and once for Enable access.
In the default RADIUS authentication operation, the
WebAgent requires only one successful authentication
request. For more information on configuring the Service
Type in your RADIUS application, refer to the documentation
provided with the application.
3. Configure the Switch To Access a RADIUS Server

This section describes how to configure the switch to interact with a RADIUS server for both authentication and accounting services.

Note

If you want to configure RADIUS accounting on the switch, go to page 5-47: “Accounting Services” instead of continuing here.

Syntax:  
\[
\text{[no]} \text{ radius-server host } < \text{ip-address} >
\]

Adds a server to the RADIUS configuration or (with no) deletes a server from the configuration. You can configure up to three RADIUS server addresses. You can configure up to 15 RADIUS server addresses. (See “Using Multiple RADIUS Server Groups” on page 5-22 for information about grouping multiple RADIUS servers.)

The switch uses the first server it successfully accesses. (Refer to “Changing the RADIUS Server Access Order” on page 5-67.)

[auth-port < port-number>]

Optional. Changes the UDP destination port for authentication requests to the specified RADIUS server (host). If you do not use this option with the radius-server host command, the switch automatically assigns the default authentication port number. The auth-port number must match its server counterpart. (Default: 1812)

[acct-port < port-number>]

Optional. Changes the UDP destination port for accounting requests to the specified RADIUS server. If you do not use this option with the radius-server host command, the switch automatically assigns the default accounting port number. The acct-port number must match its server counterpart. (Default: 1813)
[dyn-authorization]

*Enables or disables the processing of Disconnect and Change of Authorization messages from this host. When enabled, the RADIUS server can dynamically terminate or change the authorization parameters (such as VLAN assignment) used in an active client session on the switch. The UDP port specified in the `radius-server dyn-autz-port` command (defaults to 3799) is the port used to listen for Change of Authorization messages (CoA) or Disconnect messages (DM). See Change-of-Authorization on page 5-44.*

Default: Disabled

[key < key-string>]

*Optional. Specifies an encryption key for use during authentication (or accounting) sessions with the specified server. This key must match the encryption key used on the RADIUS server. Use this command only if the specified server requires a different encryption key than configured for the global encryption key.*

*Note: Formerly, when you saved the configuration file using Xmodem or TFTP, the RADIUS encryption key information was not saved in the file. This caused RADIUS authentication to break when the startup configuration file was loaded back onto the switch. You now can save the configured RADIUS shared secret (encryption) key to a configuration file by entering the following commands:*

`include-credentials`  
`write memory`

*For more information, see “Saving Security Credentials in a Config File” on page 2-10 in this guide.*
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

[time-window <0-65535>]

The time window in seconds within which the received
dynamic authorization requests are considered to be cur-
rent and accepted for processing. A zero value means there
is no time limit. A non-zero value indicates that the even-
timestamp attribute is expected as part of all Change of
Authorization and Disconnect request messages. If the
timestamp attribute is not present the message is dropped.

Default: 300 seconds.

no radius-server host <ip-address> key

Use the no form of the command to remove the key for a
specified server.

For example, suppose you have configured the switch as shown in figure 5-4
and you now need to make the following changes:

1. Change the encryption key for the server at 10.33.18.127 to “source0127”.
2. Add a RADIUS server with an IP address of 10.33.18.119 and a server-
specific encryption key of “source0119”.

HP Switch(config)# radius-server host 10.33.18.127 key source0127
HP Switch(config)# radius-server host 10.33.18.119 key source0119

HP Switch# show radius

Status and Counters - General RADIUS Information

Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key :
Dynamic Authorization UDP Port : 3799
Source IP Selection : Outgoing Interface

<table>
<thead>
<tr>
<th>Auth Acct DM/ Time</th>
<th>Server IP Addr</th>
<th>Port</th>
<th>Port</th>
<th>CoA</th>
<th>Window</th>
<th>Encryption Key</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.33.18.127</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>TempKey01</td>
</tr>
</tbody>
</table>

Figure 5-4. Sample Configuration for RADIUS Server Before Changing the Key and Adding Another Server

To make the changes listed prior to figure 5-4, you would do the following:
4. Configure the Switch’s Global RADIUS Parameters

You can configure the switch for the following global RADIUS parameters:

- **Number of login attempts**: In a given session, specifies how many tries at entering the correct username and password pair are allowed before access is denied and the session terminated. (This is a general `aaa authentication` parameter and is not specific to RADIUS.)

- **Global server key**: The server key the switch will use for contacts with all RADIUS servers for which there is not a server-specific key configured by `radius-server host <ip-address> key <key-string>`. This key is optional if you configure a server-specific key for each RADIUS server entered in the switch. (Refer to “3. Configure the Switch To Access a RADIUS Server” on page 5-14.)

- **Server timeout**: Defines the time period in seconds for authentication attempts. If the timeout period expires before a response is received, the attempt fails.

- **Server dead time**: Specifies the time in minutes during which the switch avoids requesting authentication from a server that has not responded to previous requests.
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

- **Retransmit attempts**: If the first attempt to contact a RADIUS server fails, specifies how many retries you want the switch to attempt on that server.

- **Change of Authorization port**: The `dyn-autz-port` parameter specifies the UDP port number that listens for the Change of Authorization and Disconnect messages. The UDP port range is 1024-49151. The default port is 3799.

**Syntax**: 
```
aaa authentication num-attempts < 1 - 10 >
```

Specifies how many tries for entering the correct username and password before shutting down the session due to input errors. (Default: 3; Range: 1 - 10).

```
[no] radius-server
key < global-key-string >
```

Specifies the global encryption key the switch uses with servers for which the switch does not have a server-specific key assignment. This key is optional if all RADIUS server addresses configured in the switch include a server-specific encryption key. (Default: Null.)

```
dead-time < 1 - 1440 >
```

Optional. Specifies the time in minutes during which the switch will not attempt to use a RADIUS server that has not responded to an earlier authentication attempt. (Default: 0; Range: 1 - 1440 minutes)

```
dyn-autz-port <1024-49151>
```

Specifies the UDP port number that listens for Change of Authorization or Disconnect messages. The range of ports is 1024-49151. See Change-of-Authorization on page 5-44.
Default: 3799
radius-server timeout < 1 - 15 >

Specifies the maximum time the switch waits for a response to an authentication request before counting the attempt as a failure. (Default: 3 seconds; Range: 1 - 15 seconds)

radius-server retransmit < 1 - 5 >

If a RADIUS server fails to respond to an authentication request, specifies how many retries to attempt before closing the session. Default: 3; Range: 1 - 5)

Note

Where the switch has multiple RADIUS servers configured to support authentication requests, if the first server fails to respond, then the switch tries the next server in the list, and so-on. If none of the servers respond, then the switch attempts to use the secondary authentication method configured for the type of access being attempted (console, Telnet, or SSH). If this occurs, refer to “RADIUS-Related Problems” in the Troubleshooting chapter of the Management and Configuration Guide for your switch.

For example, suppose that your switch is configured to use three RADIUS servers for authenticating access through Telnet and SSH. Two of these servers use the same encryption key. In this case your plan is to configure the switch with the following global authentication parameters:

- Allow only two tries to correctly enter username and password.
- Use the global encryption key to support the two servers that use the same key. (For this example, assume that you did not configure these two servers with a server-specific key.)
- Use a dead-time of five minutes for a server that fails to respond to an authentication request.
- Allow three seconds for request timeouts.
- Allow two retries following a request that did not receive a response.
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

```
HP Switch(config)# aaa authentication num-attempts 2
HP Switch(config)# radius-server key My-Global-KEY-1099
HP Switch(config)# radius-server dead-time 5
HP Switch(config)# radius-server timeout 3
HP Switch(config)# radius-server retransmit 2
HP Switch(config)# write mem
```

Figure 5-6. Example of Global Configuration Exercise for RADIUS Authentication
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

Figure 5-7. Listings of Global RADIUS Parameters Configured In Figure 5-6

<table>
<thead>
<tr>
<th>Access Task</th>
<th>Primary Login</th>
<th>Server Group Secondary Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Local</td>
<td>None</td>
</tr>
<tr>
<td>Telnet</td>
<td>Radius</td>
<td>None</td>
</tr>
<tr>
<td>Port-Access</td>
<td>Local</td>
<td>Authorized</td>
</tr>
<tr>
<td>Webui</td>
<td>Local</td>
<td>None</td>
</tr>
<tr>
<td>SSH</td>
<td>Radius</td>
<td>None</td>
</tr>
<tr>
<td>Web-Auth</td>
<td>ChapRadius</td>
<td>Authorized</td>
</tr>
<tr>
<td>MAC-Auth</td>
<td>ChapRadius</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Task</th>
<th>Primary Login</th>
<th>Server Group Secondary Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Local</td>
<td>None</td>
</tr>
<tr>
<td>Telnet</td>
<td>Radius</td>
<td>None</td>
</tr>
<tr>
<td>Webui</td>
<td>Local</td>
<td>None</td>
</tr>
<tr>
<td>SSH</td>
<td>Radius</td>
<td>None</td>
</tr>
</tbody>
</table>

Global RADIUS parameters from figure 5-6.

Server-specific encryption key for the RADIUS server that will not use the global encryption key.

Global RADIUS parameters from figure 5-6.

These two servers will use the global encryption key.

After two attempts failing due to username or password entry errors, the switch will terminate the session.

Figure 5-7. Listings of Global RADIUS Parameters Configured In Figure 5-6
Using Multiple RADIUS Server Groups

The authentication and accounting features on the switch can use up to fifteen RADIUS servers. This option allows the RADIUS servers to be put into groups. Up to 5 groups of 3 RADIUS servers each can be configured. The authentication and accounting features can choose which RADIUS server group to communicate with. End-user authentication methods (802.1X, MAC-based and web-based) can authenticate with different RADIUS servers from the management interface authentication methods (console, telnet, ssh, web).

Commands

Several commands are used to support the RADIUS server group option. The RADIUS server must be configured before it can be added to a group. See “Configuring the Switch for RADIUS Authentication” on page 5-7 for more information about configuring RADIUS servers.

```
HP Switch(config)# radius-server host 10.33.18.151 acct-port 1750 key source0151
HP Switch(config)# write mem
HP Switch(config)# show radius
```

Status and Counters - General RADIUS Information

- Deadtime(min) : 0
- Timeout(secs) : 5
- Retransmit Attempts : 3
- Global Encryption Key :
- Dynamic Authorization UDP Port : 3799

<table>
<thead>
<tr>
<th>Server IP Addr</th>
<th>Port</th>
<th>Port CoA Window Encryption Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.33.18.151</td>
<td>1812</td>
<td>1750 No 10 source0151</td>
</tr>
</tbody>
</table>

Because the radius-server command includes an acct-port keyword with a non-default UDP port number of 1750, the switch assigns this value as the UDP accounting port.

**Syntax:** `[no] radius-server host <ip-address>`

- Adds a server to the RADIUS configuration or (with no) deletes a server from the configuration. You can configure up to fifteen RADIUS server addresses. The switch uses the first server it successfully accesses.
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

Syntax:   aaa server-group radius <group-name> host <ip-addr>
          no aaa server-group radius <group-name> host <ip-addr>

Associates a RADIUS server with a server group. Each group can contain up to 3 RADIUS servers. The default group (called ‘radius’) can only contain the first three RADIUS servers. The default group cannot be edited.

The no form of the command removes the RADIUS server with the indicated IP address from the server group. If that server was the last entry in the group, the group is removed.

radius <group-name>: The group name of the RADIUS server group. The name has a maximum length of 12 characters. Up to five groups can be configured with a a maximum of three RADIUS servers in each group. The first group slot is used by the default group.

host <ip-addr>: The IP address of the RADIUS server to be used.

Enhanced Commands
The following commands have the server-group option. If no server-group is specified, the default RADIUS group is used. The server group must have already been configured.

Note
The last RADIUS server in a server group cannot be deleted if an authentication or accounting method is using the server group.

Syntax:   aaa authentication <console | telnet | ssh | web> < enable | login <local | radius [server-group <group-name> | local | none | authorized]>>

Configures the primary password authentication method for console, Telnet, SSH, and/or the WebAgent.

<enable | login>: Primary authentication method.
Default: local

<local | radius>: Use either the local switch user/password database or a RADIUS server for authentication.

<server-group <group-name>>: Specifies the server group to use.
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

[local | none | authorized]: Provides options for secondary authentication (default: none). Note that for console access, secondary authentication must be local if primary access is not local. This prevents you from being locked out of the switch in the event of a failure in other access methods.

**Syntax:**
```
aaa authentication <port-access <local | eap-radius | chap-radius> |<mac-based | web-based <chap-radius | peap-mschapv2> [none | authorized | server-group <group-name>] >
```

Configures the primary authentication method for port-access, MAC-based, or web-based access.

```
mac-based | web-based <chap-radius | peap-mschapv2>: Password authentication for web-based or MAC-based port access to the switch. Use peap-mschapv2 when you want password verification without requiring access to a plain text password; it is more secure. Default: chap-radius

port-access <local | eap-radius | chap-radius>: Configures local, chap-radius (MD5), or eap-radius as the primary password authentication method for port-access. The default primary authentication is local. (Refer to the documentation for your RADIUS server application.)
```

[none | authorized | server-group <group-name>]

- **none:** No backup authentication method is used.
- **authorized:** Allow access without authentication
- **server-group <group-name>** Specifies the server group to use with RADIUS.

**Syntax:**
```
aaa accounting <exec | network | system | commands | <start-stop | stop-only> radius [server-group <group-name>]
```

Configures accounting type and how data will be sent to the RADIUS server.

```
radius: Uses RADIUS protocol as accounting method.

server-group <group-name>: Specifies the server group to use with RADIUS.
```
Displaying the RADIUS Server Group Information

The **show server-group radius** command displays the same information as the **show radius** command, but displays the servers in their server groups.

<table>
<thead>
<tr>
<th>Server IP Addr</th>
<th>Port</th>
<th>Port</th>
<th>CoA</th>
<th>Window</th>
<th>Encryption Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.3</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>default_key</td>
</tr>
<tr>
<td>192.168.3.3</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp2_key</td>
</tr>
<tr>
<td>192.172.4.5</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp2_key</td>
</tr>
<tr>
<td>192.173.6.7</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp2_key</td>
</tr>
<tr>
<td>192.168.30.3</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp3_key</td>
</tr>
<tr>
<td>192.172.40.5</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp3_key</td>
</tr>
<tr>
<td>192.173.60.7</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp3_key</td>
</tr>
</tbody>
</table>

Group Name: group2

<table>
<thead>
<tr>
<th>Server IP Addr</th>
<th>Port</th>
<th>Port</th>
<th>CoA</th>
<th>Window</th>
<th>Encryption Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.3.3</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp2_key</td>
</tr>
<tr>
<td>192.172.4.5</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp2_key</td>
</tr>
<tr>
<td>192.173.6.7</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp2_key</td>
</tr>
</tbody>
</table>

Group Name: group3

<table>
<thead>
<tr>
<th>Server IP Addr</th>
<th>Port</th>
<th>Port</th>
<th>CoA</th>
<th>Window</th>
<th>Encryption Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.30.3</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp3_key</td>
</tr>
<tr>
<td>192.172.40.5</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp3_key</td>
</tr>
<tr>
<td>192.173.60.7</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>grp3_key</td>
</tr>
</tbody>
</table>

Figure 5-9. Example of Output from show server-group radius Command
RADIUS Authentication, Authorization, and Accounting
Configuring the Switch for RADIUS Authentication

**Figure 5-10. Example of Output from show authentication Command**

```
HP Switch(config)# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled

| Access Task | Primary | Server Group | Secondary |
|-------------+---------+--------------+-----------|
| Console     | Local   | radius       | None      |
| Telnet      | Local   | radius       | None      |
| Port-Access | Local   |              | None      |
| Webui       | Local   |              | None      |
| SSH         | Local   |              | None      |
| Web-Auth    | ChapRadius group3 | None       |
| MAC-Auth    | ChapRadius group3 | None       |

| Enable | Enable | Enable |
|--------+--------+--------|
| Console | Local   | radius | None |
| Telnet  | Radius  | group2 | None |
| Webui   | Local   |        | None |
| SSH     | Local   |        | None |
```

**Figure 5-11. Example of Output from show accounting Command**

```
HP Switch(config)# show accounting

Status and Counters - Accounting Information

Interval(min) : 0
Suppress Empty User : No
Sessions Identification : Unique

| Type     | Method Mode | Server Group       |
|----------+-------------+--------------------|
| Network  | None        |                    |
| Exec     | Radius Start-Stop | group2         |
| System   | Radius Stop-Only | group2        |
| Commands | Radius Start-Stop | radius       |
```

5-26
Using SNMP To View and Configure Switch Authentication Features

SNMP MIB object access is available for switch authentication configuration (hpSwitchAuth) features. This means that the switches covered by this Guide allow, by default, manager-only SNMP read/write access to a subset of the authentication MIB objects for the following features:

- number of primary and secondary login and enable attempts
- TACACS+ server configuration and status
- RADIUS server configuration
- selected 802.1X settings
- key management subsystem chain configuration
- key management subsystem key configuration
- local switch operator and manager usernames and passwords

With SNMP access to the hpSwitchAuth MIB enabled, a device with management access to the switch can view the configuration for the authentication features listed above (excluding usernames, passwords, and keys). Using SNMP sets, a management device can change the authentication configuration (including changes to usernames, passwords, and keys). Operator read/write access to the authentication MIB is always denied.

Security Notes

All usernames, passwords, and keys configured in the hpSwitchAuth MIB are not returned via SNMP, and the response to SNMP queries for such information is a null string. However, SNMP sets can be used to configure username, password, and key MIB objects.

To help prevent unauthorized access to the switch’s authentication MIB, HP recommends following the “SNMP Security Guidelines” on page 1-13.

If you do not want to use SNMP access to the switch’s authentication configuration MIB, then use the `snmp-server mib hpswitchauthmib excluded` command to disable this access, as described in the next section.

If you choose to leave SNMP access to the security MIB open (the default setting), HP recommends that you configure the switch with the SNMP version 3 management and access security feature, and disable SNMP version 2c access. (Refer to “Access Security Features” on page 1-2.)
Changing and Viewing the SNMP Access Configuration

**Syntax:** snmp-server mib hpswitchauthmib < excluded | included >

- **included:** Enables manager-level SNMP read/write access to the switch's authentication configuration (hpSwitchAuth) MIB.
- **excluded:** Disables manager-level SNMP read/write access to the switch's authentication configuration (hpSwitchAuth) MIB.
  (Default: included)

**Syntax:** show snmp-server

The output for this command has been enhanced to display the current access status of the switch's authentication configuration MIB in the Excluded MIBs field.

For example, to disable SNMP access to the switch's authentication MIB and then display the result in the Excluded MIB field, you would execute the following two commands.
RADIUS Authentication, Authorization, and Accounting
Using SNMP To View and Configure Switch Authentication Features

**Figure 5-12. Disabling SNMP Access to the Authentication MIB and Displaying the Result**

<table>
<thead>
<tr>
<th>SNMP Communities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Name</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>public</td>
</tr>
<tr>
<td>test</td>
</tr>
</tbody>
</table>

**Trap Receivers**

<table>
<thead>
<tr>
<th>Link-Change Traps Enabled on Ports [All] : All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traps Category</td>
</tr>
<tr>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>SNMP Authentication</td>
</tr>
<tr>
<td>Password change</td>
</tr>
<tr>
<td>Login failures</td>
</tr>
<tr>
<td>Port-Security</td>
</tr>
<tr>
<td>Authorization Server Contact</td>
</tr>
<tr>
<td>DHCP-Snooping</td>
</tr>
<tr>
<td>Dynamic ARP Protection</td>
</tr>
<tr>
<td>Dynamic IP Lockdown</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
<th>Community</th>
<th>Events</th>
<th>Type</th>
<th>Retry</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.255.131.57</td>
<td>public</td>
<td>None</td>
<td>trap</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>192.169.1.106</td>
<td>public</td>
<td>None</td>
<td>trap</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>15.255.135.68</td>
<td>public</td>
<td>None</td>
<td>trap</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>15.255.135.235</td>
<td>public</td>
<td>None</td>
<td>trap</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>15.255.135.222</td>
<td>public</td>
<td>None</td>
<td>trap</td>
<td>3</td>
<td>15</td>
</tr>
</tbody>
</table>

**Excluded MIBs**

- hpSwitchAuthenticationMIB

**Snmp Response Pdu Source-IP Information**

- Selection Policy : rfc1517

**Trap Pdu Source-IP Information**

- Selection Policy : rfc1517
An alternate method of determining the current Authentication MIB access state is to use the `show run` command.

```
HP Switch(config)# show run

Running configuration:

; J9091A Configuration Editor; Created on release #W.15.01.000x

hostname "HP Switch"
ip default-gateway 10.10.24.55
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A24,B1-B4
  ip address 10.10.24.100 255.255.255.0
exit
snmp-server community "public" Operator
snmp-server mib hpSwitchAuthMIB excluded
password manager
```

Figure 5-13. Using the `show run` Command to View the Current Authentication MIB Access State
Local Authentication Process

When the switch is configured to use RADIUS, it reverts to local authentication only if one of these two conditions exists:

- **Local** is the authentication option for the access method being used.
- The switch has been configured to query one or more RADIUS servers for a primary authentication request, but has not received a response, and **Local** is the configured secondary option.

For local authentication, the switch uses the Operator-level and Manager-level username/password set(s) previously configured locally on the switch. (These are the usernames and passwords you can configure using the CLI password command, the WebAgent, or the menu interface—which enables only local password configuration).

- If the operator at the requesting terminal correctly enters the username/password pair for either access level (Operator or Manager), access is granted on the basis of which username/password pair was used. For example, suppose you configure Telnet primary access for RADIUS and Telnet secondary access for local. If a RADIUS access attempt fails, then you can still get access to either the Operator or Manager level of the switch by entering the correct username/password pair for the level you want to enter.

- If the username/password pair entered at the requesting terminal does not match either local username/password pair previously configured in the switch, access is denied. In this case, the terminal is again prompted to enter a username/password pair. In the default configuration, the switch allows up to three attempts. If the requesting terminal exhausts the attempt limit without a successful authentication, the login session is terminated and the operator at the requesting terminal must initiate a new session before trying again.
Controlling WebAgent Access

To help prevent unauthorized access through the WebAgent, do one or more of the following:

- Configure the switch to support RADIUS authentication for WebAgent access (Web Authentication, Chapter 6).

- Options for the switches covered in this guide:
  - Configure local authentication (a Manager user name and password and, optionally, an Operator user name and password) on the switch.
  - Configure the switch's Authorized IP Manager feature to allow WebAgent access only from authorized management stations. (The Authorized IP Manager feature does not interfere with TACACS+ operation.)
  - Use one of the following methods to disable WebAgent access to the switch via http (Port 80):
    
    **CLI:** no web-management

    Menu Interface—From the Main menu, select the following:
    
    2. Switch Configuration
    1. System Information
    Web Agent Enabled: No
Commands Authorization

The RADIUS protocol combines user authentication and authorization steps into one phase. The user must be successfully authenticated before the RADIUS server will send authorization information (from the user's profile) to the Network Access Server (NAS). After user authentication has occurred, the authorization information provided by the RADIUS server is stored on the NAS for the duration of the user's session. Changes in the user's authorization profile during this time will not be effective until after the next authentication occurs.

You can limit the services for a user by enabling AAA RADIUS authorization. The NAS uses the information set up on the RADIUS server to control the user's access to CLI commands.

The authorization type implemented on the switches covered in this guide is the “commands” method. This method explicitly specifies on the RADIUS server which commands are allowed on the client device for authenticated users. This is done on a per-user or per-group basis.

**Note**

The commands authorization will only be executed for commands entered from Telnet, SSH, or console sessions. The Web management interface is not supported.

By default, all users may execute a minimal set of commands regardless of their authorization status, for example, “exit” and “logout”. This minimal set of commands can prevent deadlock on the switch due to an error in the user's authorization profile on the RADIUS server.
Enabling Authorization

To configure authorization for controlling access to the CLI commands, enter this command at the CLI.

Syntax: [no] aaa authorization <commands> <local | radius | none>

Configures authorization for controlling access to CLI commands. When enabled, the switch checks the list of commands supplied by the RADIUS server during user authentication to determine if a command entered by the user can be executed.

local: Use local groups as the authorization method.

radius: The NAS requests authorization information from the RADIUS server. Authorization rights are assigned by user or group.

none: The NAS does not request authorization information.

For example, to enable the RADIUS protocol as the authorization method:

HP Switch(config)# aaa authorization commands radius

When the NAS sends the RADIUS server a valid username and password, the RADIUS server sends an Access-Accept packet that contains two attributes—the command list and the command exception flag. When an authenticated user enters a command on the switch, the switch examines the list of commands delivered in the RADIUS Access-Accept packet as well as the command exception flag, which indicates whether the user has permission to execute the commands in the list. See Configuring the RADIUS Server on page 5-35.

After the Access-Accept packet is deliver, the command list resides on the switch. Any changes to the user's command list on the RADIUS server are not seen until the user is authenticated again.
RADIUS Authentication, Authorization, and Accounting

Commands Authorization

Displaying Authorization Information

You can show the authorization information by entering this command:

**Syntax:** show authorization

*Configures authorization for controlling access to CLI commands. When enabled, the switch checks the list of commands supplied by the RADIUS server during user authentication to determine if a command entered by the user can be executed.*

An example of the output is shown.

```plaintext
HP Switch(config)# show authorization

Status and Counters - Authorization Information

<table>
<thead>
<tr>
<th>Type</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands</td>
<td>RADIUS</td>
</tr>
</tbody>
</table>
```

**Figure 5-14. Example of Show Authorization Command**

Configuring Commands Authorization on a RADIUS Server

Using Vendor Specific Attributes (VSAs)

Some RADIUS-based features implemented on HP switches use HP VSAs for information exchange with the RADIUS server. RADIUS Access-Accept packets sent to the switch may contain the vendor-specific information.

The list of commands that are permitted (or denied) execution by the user are called regular expressions. The system compares those regular expressions against the full command name to determine whether the user is allowed to execute the command. For example, assume a RADIUS user is defined as follows:

User1    User-Password = “hpswitch”
          Service-Type = Administrative-User,
          HP-Command-Exception = 1, # Deny_list
          HP-Command-String = “config”
User1 is blocked from executing all commands that contain “config” in the name, which includes the following commands:

configure
show running-config (sh run)
show config

To block User 1 from executing only the “configure” command, the regular expression would be:

User1 User-Password = “hpswitch”
Service-Type = Administrative-User,
HP-Command-Exception = 1, # Deny_list
HP-Command-String = “^configure$”

The ^ metacharacter defines the start of the string and the $ character defines the end of the string. Do not leave a space between the semi-colon and the start of the next regular expression. So the HP-Command-String with more than one regular expression defined may look as follows:

HP-Command-String = “^configure$;^show running-config$”.

In this case, User1 is blocked from executing the commands “configure” and “show running-config” but is able to execute the “show config” command.

The attributes supported with commands authorization are:

- HP-Command-String: List of commands (regular expressions) that are permitted (or denied) execution by the user. The commands are delimited by semi-colons and must be between 1 and 249 characters in length. Multiple instances of this attribute may be present in Access-Accept packets. (A single instance may be present in Accounting-Request packets.)

- HP-Command-Exception: A flag that specifies whether the commands indicated by the HP-Command-String attribute are permitted or denied to the user. A zero (0) means permit all listed commands and deny all others; a one (1) means deny all listed commands and permit all others.

The results of using the HP-Command-String and HP-Command-Exception attributes in various combinations are shown below.
### RADIUS Authentication, Authorization, and Accounting

#### Commands Authorization

<table>
<thead>
<tr>
<th>HP-Command-String</th>
<th>HP-Command-Exception</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not present</td>
<td>Not present</td>
<td>If command authorization is enabled and the RADIUS server does not provide any authorization attributes in an Access-Accept packet, the user is denied access to the server. This message appears: “Access denied: no user’s authorization info supplied by the RADIUS server.”</td>
</tr>
<tr>
<td>Not present</td>
<td>DenyList-PermitOthers(1)</td>
<td>Authenticated user is allowed to execute all commands available on the switch.</td>
</tr>
<tr>
<td>Not present</td>
<td>PermitList-DenyOthers(0)</td>
<td>Authenticated user can only execute a minimal set of commands (those that are available by default to any user).</td>
</tr>
<tr>
<td>Commands List</td>
<td>DenyList-PermitOthers(1)</td>
<td>Authenticated user may execute all commands except those in the Commands list.</td>
</tr>
<tr>
<td>Commands List</td>
<td>PermitList-DenyOthers(0)</td>
<td>Authenticated user can execute only those commands provided in the Commands List, plus the default commands.</td>
</tr>
<tr>
<td>Commands List</td>
<td>Not present</td>
<td>Authenticated user can only execute commands from the Commands List, plus the default commands.</td>
</tr>
<tr>
<td>Empty Commands List</td>
<td>Not present</td>
<td>Authenticate user can only execute a minimal set of commands (those that are available by default to any user).</td>
</tr>
<tr>
<td>Empty Commands List</td>
<td>DenyList-PermitOthers(1)</td>
<td>Authenticated user is allowed to execute all commands available on the switch.</td>
</tr>
<tr>
<td>Empty Commands List</td>
<td>PermitList-DenyOthers(0)</td>
<td>Authenticated user can only execute a minimal set of commands (those that are available by default to any user).</td>
</tr>
</tbody>
</table>

You must configure the RADIUS server to provide support for the HP VSAs. There are multiple RADIUS server applications; the two examples below show how a dictionary file can be created to define the VSAs for that RADIUS server application.
Example Configuration on Cisco Secure ACS for MS Windows

It is necessary to create a dictionary file that defines the VSAs so that the RADIUS server application can determine which VSAs to add to its user interface. The VSAs will appear below the standard attributes that can be configured in the application.

The dictionary file must be placed in the proper directory on the RADIUS server. Follow these steps.

1. Create a dictionary file (for example, hp.ini) containing the HP VSA definitions, as shown in the example below.

```ini
;[User Defined Vendor]
;
; The Name and IETF vendor code and any VSAs MUST be unique.
;
; One or more VSAs named (max 255)
;
; Each named VSA requires a definition section...
;
; Types are STRING, INTEGER, IPADDR
;
; The profile specifies usage, IN for accounting, OUT for authorization,
; MULTI if more than a single instance is allowed per RADIUS message.
; Combinations are allowed, e.g. "IN", "MULTI OUT", "MULT IN OUT"
;
; Enumerations are optional for INTEGER attribute types

[User Defined Vendor]
Name=HP
IETF Code=11
VSA 2=Hp-Command-String
VSA 3=Hp-Command-Exception

[Hp-Command-String]
Type=STRING
Profile=IN OUT

[Hp-Command-Exception]
Type=INTEGER
```
RADIUS Authentication, Authorization, and Accounting
Commands Authorization

Profile=IN OUT
Enums=Hp-Command-Exception-Types

[Hp-Command-Exception-Types]
0=PermitList
1=DenyList

2. Copy the hp.ini dictionary file to c:\program files\cisco acs 3.2\utils (or the \utils directory wherever acs is installed).

3. From the command prompt execute the following command:
   c:\Program files\CiscoSecure ACS v3.2\utils>
csutil -addudv 0 hp.ini

   The zero (0) is the slot number. You will see some processing messages:

   Adding or removing vendors requires ACS services to be re-started. Please make sure regedit is not running as it can prevent registry backup/restore operations.

   Are you sure you want to proceed?  (Y or N) y

   Parsing [\hp.ini] for addition at UDV slot [0]
   Stopping any running services
   Creating backup of current config
   Adding Vendor [HP} added as [RADIUS (HP)]

   Done
   Checking new configuration...
   New configuration OK
   Re-starting stopped services

4. Start the registry editor (regedit) and browse to
   HKEY_LOCAL_MACHINE\software\cisco\CiscoAAA v3.2\NAS Vendors tree.

   Cisco adds the entry into this tree for each custom vendor. The id is 100 + the slot number used in the previous command (100 + 0, as it was added in slot 0). Look in the key to verify the vendor name and id.

5. Go to:
   HKEY_LOCAL_MACHINE\software\cisco\CiscoAAAv3.2\CSRADIUS\ExtensionPoints\002\AssociatedWithVendors
RADIUS Authentication, Authorization, and Accounting

Commands Authorization

6. Right click and then select **New > key**. Add the vendor Id number that you determined in step 4 (100 in the example).

7. Restart all Cisco services.

8. The newly created HP RADIUS VSA appears only when you configure an AAA client (NAS) to use the HP VSA RADIUS attributes. Select Network Configuration and add (or modify) an AAA entry. In the Authenticate Using field choose RADIUS(HP) as an option for the type of security control protocol.

9. Select **Submit + Restart** to effect the change. The HP RADIUS VSA attributes will appear in Cisco ACS configurations, for example, “Interface Configuration”, “Group Setup”, “User Setup”.

To enable the processing of the HP-Command-String VSA for RADIUS accounting:

1. Select **System Configuration**.

2. Select **Logging**.

3. Select **CSV RADIUS Accounting**. In the Select Columns to Log section, add the HP-Command-String attribute to the Logged Attributes list.

4. Select **Submit**.

5. Select **Network Configuration**. In the AAA Clients section, select an entry in the AAA Client Hostname column. You will go to the AAA Client Setup screen.

6. Check the box for **Log Update/Watchdog Packets from this AAA Client**.

7. Click **Submit + Restart**. You should be able to see the HP-Command-String attribute in the RADIUS accounting reports.

You can enter the commands you wish to allow or deny with the special characters used in standard regular expressions (c, ., \ [list], [^list], *, ^, $). Commands must be between 1-249 characters in length.
Example Configuration Using FreeRADIUS

1. Create a dictionary file (for example, dictionary.hp) containing HP VSA definitions. An example file is:

```plaintext
# dictionary.hp
#
# As posted to the list by User <user_email>
#
# Version: $Id: dictionary.hp, v 1.0 2006/02/23 17:07:07
#
VENDOR Hp 11

# HP Extensions

ATTRIBUTE Hp-Command-String 2 string Hp
ATTRIBUTE Hp-Command-Exception 3 integer Hp

# Hp-Command-Exception Attribute Values
VALUE Hp-Command-Exception Permit-List 0
VALUE Hp-Command-Exception Deny-List 1
```

2. Find the location of the dictionary files used by FreeRADIUS (try /usr/local/share/freeradius).

3. Copy dictionary.hp to that location. Open the existing dictionary file and add this entry:

   `$ INCLUDE dictionary.hp`

4. You can now use HP VSAs with other attributes when configuring user entries.
VLAN Assignment in an Authentication Session

A switch supports concurrent 802.1X and either Web- or MAC-authentication sessions on a port (with up to 32 clients allowed). If you have configured RADIUS as the primary authentication method for a type of access, when a client authenticates on a port, the RADIUS server assigns an untagged VLAN that is statically configured on the switch for use in the authentication session. (For information on how to configure a user profile on a RADIUS server with the VLAN to be assigned for 802.1X, Web, or MAC authentication, refer to the documentation provided with the RADIUS server application.)

If a switch port is configured to accept multiple 802.1X and/or Web- or MAC-Authentication client sessions, all authenticated clients must use the same port-based, untagged VLAN membership assigned for the earliest, currently active client session. On a port where one or more authenticated client sessions are already running, all clients are on the same untagged VLAN (unless MAC-based VLANs are enabled. Please see “MAC-Based VLANs” on page 5-46). If the RADIUS server subsequently authenticates a new client, but attempts to re-assign the port to a different, untagged VLAN than the one already in use for the previously existing, authenticated client sessions, the connection for the new client will fail.

Tagged and Untagged VLAN Attributes

When you configure a user profile on a RADIUS server to assign a VLAN to an authenticated client, you can use either the VLAN’s name or VLAN ID (VID) number. For example, if a VLAN configured in the switch has a VID of 100 and is named vlan100, you could configure the RADIUS server to use either “100” or “vlan100” to specify the VLAN.

After the RADIUS server validates a client’s username and password, the RADIUS server returns an Access-Accept packet that contains the VLAN assignment and the following attributes for use in the authentication session:

- **Egress-VLANID**: Configures an optional, egress VLAN ID for either tagged or untagged packets (RFC 4675).
- **Egress-VLAN-Name**: Configures an optional, egress VLAN for either tagged or untagged packets when the VLAN ID is not known (RFC 4675).
Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID: Tunnel attributes that specify an untagged VLAN assignment (RFC 3580).

Tunnel (untagged VLAN) attributes may be included in the same RADIUS packet as the Egress-VLANID and Egress-VLAN-Name attributes. These attributes are not mutually exclusive.

The switch processes the VLAN information returned from the remote RADIUS server for each successfully 802.1X-, Web-, and MAC-authenticated client (user). The VLAN information is part of the user’s profile stored in the RADIUS server’s database and is applied if the VLANs exist on the switch.

The support for RADIUS-assigned tagged and untagged VLAN configuration on an authenticated port allows you to use IDM to dynamically configure tagged and untagged VLANs as required for different client devices, such as PCs and IP phones, that share the same switch port.

Additional RADIUS Attributes

The following attributes are included in Access-Request and Access-Accounting packets sent from the switch to the RADIUS server to advertise switch capabilities, report information on authentication sessions, and dynamically reconfigure authentication parameters:

- MS-RAS-Vendor (RFC 2548): Allows HP switches to inform a Microsoft RADIUS server that the switches are from HP Networking. This feature assists the RADIUS server in its network configuration.

- HP-capability-advert: An HP proprietary RADIUS attribute that allows a switch to advertise its current capabilities to the RADIUS server for port-based (MAC, Web, or 802.1X) authentication; for example, HP VSAs for port QoS, ingress rate-limiting, IDM filter rules, RFC 4675 QoS and VLAN attributes, and RFC 3580 VLAN-related attributes.

  The RADIUS server uses this information to make a more intelligent policy decision on the configuration settings to return to the switch for a client session.

- HP-acct-terminate-cause: An HP proprietary RADIUS accounting attribute that allows a switch to report to the RADIUS server why an authentication session was terminated. This information allows customers to diagnose network operational problems and generate
reports on terminated sessions. This attribute provides extended
information on the statistics provided by the acct-terminate-cause
attribute.

- Change-of-Authorization (CoA) (RFC 3576: Dynamic Authorization
  Extensions to RADIUS): A mechanism that allows a RADIUS server
to dynamically disconnect messages (DM) or change the authoriza-
tion parameters (such as VLAN assignment) used in an active client
session on the switch. The switch (NAS) does not have to initiate the
exchange.

For example, for security reasons you may want to limit the network
services granted to an authenticated user. In this case, you can change the
user profile on the RADIUS server and have the new authorization settings
take effect immediately in the active client session. The Change-of-AUTH-
ORIZATION attribute provides the mechanism to dynamically update an active
client session with a new user policy that is sent in RADIUS packets. See
figures 5-15 and 5-16. See “3. Configure the Switch To Access a RADIUS
Server” on page 5-14 for configuration commands for dynamic authoriza-

```
HP Switch(config)# show radius dyn-authorization

Status and Counters - RADIUS Dynamic Authorization Information

NAS Identifier : LAB-8212
Invalid Client Addresses (CoA-Reqs) : 0
Invalid Client Addresses (Disc-Reqs) : 0

<table>
<thead>
<tr>
<th>Client IP Addr</th>
<th>Disc Reqs</th>
<th>Disc ACKs</th>
<th>Disc NAKs</th>
<th>CoA Reqs</th>
<th>CoA ACKs</th>
<th>CoA NAKs</th>
</tr>
</thead>
<tbody>
<tr>
<td>154.34.23.106</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>154.45.234.12</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Figure 5-15. Example of Output for Dynamic Authorization Configuration
HP Switch(config)# show radius host 154.23.45.111 dyn-authorization

<table>
<thead>
<tr>
<th>Status and Counters - RADIUS Dynamic Authorization Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Client IP Address : 154.23.45.111</td>
</tr>
<tr>
<td>Unknown PKT Types Received : 0</td>
</tr>
<tr>
<td>Disc-reqs : 2</td>
</tr>
<tr>
<td>Disc-reqs Authorize Only : 0</td>
</tr>
<tr>
<td>Disc-ACKs : 2</td>
</tr>
<tr>
<td>Disc-NAKs : 0</td>
</tr>
<tr>
<td>Disc-NAKs Authorize Only : 0</td>
</tr>
<tr>
<td>Disc-reqs Ses. Removed : 0</td>
</tr>
<tr>
<td>Disc-reqs Malformed : 0</td>
</tr>
<tr>
<td>Disc-reqs Bad Authentic. : 0</td>
</tr>
<tr>
<td>Disc-reqs Dropped : 0</td>
</tr>
<tr>
<td>CoA-reqs : 1</td>
</tr>
<tr>
<td>CoA-reqs Authorize Only : 0</td>
</tr>
<tr>
<td>CoA-ACKs : 1</td>
</tr>
<tr>
<td>CoA-NAKs : 0</td>
</tr>
<tr>
<td>CoA-NAKs Authorize Only : 0</td>
</tr>
<tr>
<td>CoA-reqs Ses. Changed : 0</td>
</tr>
<tr>
<td>CoA-reqs Malformed : 0</td>
</tr>
<tr>
<td>CoA-reqs Bad Authentic. : 0</td>
</tr>
<tr>
<td>CoA-reqs Dropped : 0</td>
</tr>
</tbody>
</table>

Figure 5-16. Example of Output Showing Dynamic Authorization Statistics
MAC-Based VLANs

MAC-Based VLANs (MBVs) allow multiple clients on a single switch port to receive different untagged VLAN assignments. VLAN assignment of untagged traffic is based on the source MAC address rather than the port. Clients receive their untagged VLAN assignment from the RADIUS server. This feature adheres to the requirement that if all known IDM attributes for a given client cannot be applied the authentication request for that client must be rejected.

Both authenticated and unauthenticated clients can reside on the same port on different VLANs, but only if the mixed-mode configuration is enabled. This is not the default behavior. The normal operating behavior is to not allow unauthenticated clients on the port when at least one authenticated client is present on the port. If an unauthenticated client is present on the unauth VLAN and another client successfully authenticates on that port, the unauthenticated client is kicked off the port.

When a MBV cannot be applied due to a conflict with another client on that port a message indicating VID arbitration error is logged.

When a MBV cannot be applied due to lack of resources a message indicating lack of resources is logged.

There is no command line support for this feature. The decision to use a MBV is made automatically if the hardware is capable and if the situation necessitates. If multiple clients authenticate on different untagged VLANs on hardware that does not support MBVs, the switch will reject all clients authorized on a VLAN different from the first client’s VLAN - the first authenticated client sets the Port VID (PVID).

This feature has the side effect of allowing egress traffic from one client’s VLAN to be accepted by all untagged clients on that port. For example, suppose that clients A and B are both located on the same switch port, but on two different VLANs. If client A is subscribing to a multicast stream, then client B also receives that multicast traffic.
Accounting Services

RADIUS accounting collects data about user activity and system events and sends it to a RADIUS server when specified events occur on the switch, such as a logoff or a reboot.

Accounting Service Types

The switch supports four types of accounting services:

- **Network accounting:** Provides records containing the information listed below on clients directly connected to the switch and operating under Port-Based Access Control (802.1X):
  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Acct-Input-Packets
  - Acct-Output-Packets
  - Acct-Input-Octets
  - Acct-Output-Octets
  - Acct-Session-Time
  - User-Name
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Calling-Station-Id
  - MS-RAS-Vendor

- **Exec accounting:** Provides records holding the information listed below about login sessions (console, Telnet, and SSH) on the switch:
  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Acct-Session-Time
  - Acct-Input-Packets
  - Acct-Output-Packets
  - Acct-Input-Octets
  - Acct-Output-Octets
  - User-Name
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Calling-Station-Id
  - MS-RAS-Vendor

- **System accounting:** Provides records containing the information listed below when system events occur on the switch, including system reset, system boot, and enabling or disabling of system accounting:
  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Username
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Calling-Station-Id
  - Acct-Session-Time
  - MS-RAS-Vendor
Commands accounting: Provides records containing information on CLI command execution during user sessions.

- Acct-Session-Id
- Acct-Status-Type
- Service-Type
- Acct-Authentic
- User-Name
- NAS-IP-Address
- NAS-Identifier
- NAS-Port-Type
- Calling-Station-Id
- HP-Command-String
- Acct-Delay-Time

RADIUS accounting with IP attribute: The RADIUS Attribute 8 (Framed-IP-Address) feature provides the RADIUS server with information about the client’s IP address after the client is authenticated. DHCP snooping is queried for the IP address of the client, so DHCP snooping must be enabled for the VLAN of which the client is a member.

When the switch begins communications with the RADIUS server it sends the IP address of the client requesting access to the RADIUS server as RADIUS Attribute 8 (Framed-IP-Address) in the RADIUS accounting request. The RADIUS server can use this information to build a map of usernames and addresses.

It may take a minute or longer for the switch to learn the IP address and then send the accounting packet with the Framed-IP-Address attribute to the RADIUS server. If the switch does not learn the IP address after a minute, it sends the accounting request packet to the RADIUS server without the Framed-IP-Address attribute. If the IP address is learned at a later time, it will be included in the next accounting request packet sent.

The switch forwards the accounting information it collects to the designated RADIUS server, where the information is formatted, stored, and managed by the server. For more information on this aspect of RADIUS accounting, refer to the documentation provided with your RADIUS server.

Operating Rules for RADIUS Accounting

- You can configure up to four types of accounting to run simultaneously: exec, system, network, and command.
- RADIUS servers used for accounting are also used for authentication.
- The switch must be configured to access at least one RADIUS server.
- RADIUS servers are accessed in the order in which their IP addresses were configured in the switch. Use show radius to view the order. As long as the first server is accessible and responding to authentication
requests from the switch, a second or third server will not be
accessed. (For more on this topic, refer to “Changing RADIUS-Server
Access Order” on page 5-67.)

- If access to a RADIUS server fails during a session, but after the client
  has been authenticated, the switch continues to assume the server is
  available to receive accounting data. Thus, if server access fails during
  a session, it will not receive accounting data transmitted from the
  switch.

**Acct-Session-ID Options in a Management Session**

The switch can be configured to support either of the following options for
the accounting service types used in a management session. (Refer to
“Accounting Service Types” on page 5-47.)

- unique Acct-Session-ID for each accounting service type used in the
  same management session (the default)

- same Acct-Session-ID for all accounting service types used in the
  same management session

**Unique Acct-Session-ID Operation**

In the Unique mode (the default), the various service types running in a
management session operate as parallel, independent processes. Thus, during
a specific management session, a given service type has the same Acct-
Session-ID for all accounting actions for that service type. However, the Acct-
Session-ID for each service type differs from the ID for the other types.

**Note**

In Unique Acct-Session-ID operation, the Command service type is a special
case in which the Acct-Session-ID for each executed CLI command in the
session is different from the IDs for other service types used in the session
and also different for each CLI command executed during the session. That
is, the ID for each successive CLI command in the session is sequentially
incremented from the ID value assigned to the immediately preceding CLI
command in that session.
Figure 5-17 shows *Unique mode* accounting operation for a new session in which two commands are executed, and then the session is closed.

User “fred” starts Exec Accounting session "003300000008".

User “fred” then executes `show ip`, which results in this accounting entry. Notice the session ID (003300000009) assigned to this accounting entry incrementally follows the preceding Acct-Session-Id. This incrementing of the session ID is normal operation for command accounting in the (default) Unique mode.

User “fred” executes the *logout* command. The session ID (00330000000A) assigned to this accounting entry incrementally follows the preceding Acct-Session-Id. This is another instance of normal Command accounting operation in the Unique mode.

Terminate Exec Accounting Session "003300000008".

Figure 5-17. Example of Accounting in the (Default) Unique Mode
Common Acct-Session-ID Operation

In this case, all service types running in a given management session operate as subprocesses of the same parent process, and the same Acct-Session-ID is used for accounting of all service types, including successive CLI commands.

| User “fred” starts Exec Accounting session “00330000000B”. | Acct-Session-Id = "00330000000B"
Acct-Status-Type = Start
Service-Type = NAS-Prompt-User
Acct-Authentic = RADIUS
NAS-IP-Address = 10.1.242.15
NAS-Identifier = "gsf_dosx_15"
User-Name = "fred"
Calling-Station-Id = "172.22.17.101"
Acct-Delay-Time = 0 |
| --- | --- |

| User “fred” then executes show ip, which results in this command accounting entry. Because this example assumes Common Mode configuration, the session ID (00330000000B) assigned to this accounting entry is identical to the session ID assigned when the session was opened. No incrementing of the session ID is done for individual commands. | Acct-Session-Id = "00330000000B"
Acct-Status-Type = Stop
Service-Type = NAS-Prompt-User
Acct-Authentic = RADIUS
User-Name = "fred"
NAS-IP-Address = 10.1.242.15
NAS-Identifier = "gsf_dosx_15"
NAS-Port-Type = Virtual
Calling-Station-Id = "172.22.17.101"
HP-Command-String = "show ip"
Acct-Delay-Time = 0 |
| --- | --- |

| User “fred” executes the logout command. The session ID (00330000000B) used for the earlier Exec and Command accounting entries continues to be the same as was originally assigned to the session. | Acct-Session-Id = "00330000000B"
Acct-Status-Type = Stop
Service-Type = NAS-Prompt-User
Acct-Authentic = RADIUS
User-Name = "fred"
NAS-IP-Address = 10.1.242.15
NAS-Identifier = "gsf_dosx_15"
NAS-Port-Type = Virtual
Calling-Station-Id = "172.22.17.101"
HP-Command-String = "logout"
Acct-Delay-Time = 0 |
| --- | --- |

| Terminate Exec Accounting Session "00330000000B" | Acct-Session-Id = "00330000000B"
Acct-Status-Type = Stop
Service-Type = NAS-Prompt-User
Acct-Authentic = RADIUS
NAS-IP-Address = 10.1.242.15
NAS-Identifier = "gsf_dosx_15"
User-Name = "fred"
Calling-Station-Id = "172.22.17.101"
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 29
Acct-Delay-Time = 0 |
| --- | --- |

Figure 5-18. Example of Accounting in Common Mode (Same Session ID Throughout)
Configuring RADIUS Accounting

### Note

This section assumes you have already:

- Configured RADIUS authentication on the switch for one or more access methods
- Configured one or more RADIUS servers to support the switch

If you have not already done so, refer to “General RADIUS Setup Procedure” in the “RADIUS Authentication and Accounting” chapter of the Access Security Guide for your switch.

### Steps for Configuring RADIUS Accounting

1. Configure the switch for accessing a RADIUS server.

   You can configure a list of up to three RADIUS servers (one primary, two backup). The switch operates on the assumption that a server can operate in both accounting and authentication mode. (Refer to the documentation for your RADIUS server application.)

   - Use the same `radius-server host` command that you would use to configure RADIUS authentication. Refer to “1. Configure the Switch To Access a RADIUS Server” on page 5-53.

---

**RADIUS Accounting Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] radius-server host &lt; ip-address &gt;</td>
<td>5-53</td>
</tr>
<tr>
<td>[acct-port &lt; port-number &gt;]</td>
<td>5-53</td>
</tr>
<tr>
<td>[key &lt; key-string &gt;]</td>
<td>5-53</td>
</tr>
<tr>
<td>[no] aaa accounting &lt; exec</td>
<td>network</td>
</tr>
<tr>
<td>[no] aaa accounting commands &lt; stop-only</td>
<td>interim-update &gt; radius</td>
</tr>
<tr>
<td>aaa accounting session-id &lt; unique</td>
<td>common &gt;</td>
</tr>
<tr>
<td>[no] aaa accounting update</td>
<td>5-61</td>
</tr>
<tr>
<td>periodic &lt; 1 - 525600 &gt; (in minutes)</td>
<td></td>
</tr>
<tr>
<td>[no] aaa accounting suppress null-username</td>
<td>5-61</td>
</tr>
<tr>
<td>show accounting</td>
<td>5-66</td>
</tr>
<tr>
<td>show accounting sessions</td>
<td>5-67</td>
</tr>
<tr>
<td>show radius accounting</td>
<td>5-67</td>
</tr>
</tbody>
</table>
• Provide the following:
  – A RADIUS server IP address.
  – Optional—a UDP destination port for authentication requests. Otherwise the switch assigns the default UDP port (1812; recommended).
  – Optional—if you are also configuring the switch for RADIUS authentication, and need a unique encryption key for use during authentication sessions with the RADIUS server you are designating, configure a server-specific key. This key overrides the global encryption key you can also configure on the switch, and must match the encryption key used on the specified RADIUS server. For more information, refer to the key <key-string> parameter on page 5-14. (Default: null)

2. (Optional) Reconfigure the desired Acct-Session-ID operation.
  • Unique (the default setting): Establishes a different Acct-Session-ID value for each service type, and incrementing of this ID per CLI command for the Command service type. (Refer to “Unique Acct-Session-ID Operation” on page 5-49.)
  • Common: Establishes the same Acct-Session-ID value for all service types, including successive CLI commands in the same management session.

3. Configure accounting types and the controls for sending reports to the RADIUS server.
  • Accounting types:
    – exec (page 5-47)
    – network (page 5-47)
    – system (page 5-47)
    – commands (page 5-48)
  • Trigger for sending accounting reports to a RADIUS server: At session start and stop or only at session stop

4. (Optional) Configure session blocking and interim updating options
  • Updating: Periodically update the accounting data for sessions-in-progress.
  • Suppress accounting: Block the accounting session for any unknown user with no username access to the switch.

1. Configure the Switch To Access a RADIUS Server

Before you configure the actual accounting parameters, you should first configure the switch to use a RADIUS server. This is the same as the process described on page 5-14. You need to repeat this step here only if you have not
yet configured the switch to use a RADIUS server, your server data has
time, or you need to specify a non-default UDP destination port for
accounting requests. Note that switch operation expects a RADIUS server to
accommodate both authentication and accounting.

**Syntax:**

```
[no] radius-server host <ip-address>
```

*Adds a server to the RADIUS configuration or (with no) deletes a server from the configuration.*

```
[acct-port <port-number>]
```

*Optional. Changes the UDP destination port for accounting requests to the specified RADIUS server. If you do not use this option, the switch automatically assigns the default accounting port number. (Default: 1813)*

```
[key <key-string>]
```

*Optional. Specifies an encryption key for use during accounting or authentication sessions with the specified server. This key must match the encryption key used on the RADIUS server. Use this command only if the specified server requires a different encryption key than configured for the global encryption key.*

*Note:* If you save the config file using Xmodem or TFTP, the key information is not saved in the file. This causes RADIUS authentication to fail when the config file is loaded back onto the switch.

For example, suppose you want the switch to use the RADIUS server described below for both authentication and accounting purposes.

- IP address: 10.33.18.151
- A non-default UDP port number of 1750 for accounting.
- An encryption key of “source0151” for accounting sessions.

For this example, assume that all other RADIUS authentication parameters for accessing this server are acceptable at their default settings, and that RADIUS is already configured as an authentication method for one or more types of access to the switch (Telnet, Console, etc.).
The radius-server command as shown in figure 5-19, above, configures the switch to use a RADIUS server at IP address 10.33.18.151, with a (non-default) UDP accounting port of 1750, and a server-specific key of “source0151”.

2. (Optional) Reconfigure the Acct-Session-ID Operation

**Syntax:**

```
aaa accounting session-id < unique | common >
```

Optional command to reconfigure the Acct-Session-ID mode to apply to the accounting service type records for a given management session.

- **unique:** Configures the switch to use a different Acct-Session-ID for each accounting service type. (Default setting)
- **common:** Configures the switch to apply the same Acct-Session-ID to all accounting service types in the same management session.

For more on these options, refer to “Acct-Session-ID Options in a Management Session” on page 5-49.
3. Configure Accounting Types and the Controls for Sending Reports to the RADIUS Server

**Accounting Service Types.** Configure one or more accounting service types to track:

- **Exec:** Use `exec` if you want to collect accounting information on login sessions on the switch via the console, Telnet, or SSH. (See also “Accounting Service Types” on page 5-56.)

- **System:** Use `system` if you want to collect accounting data when:
  - A system boot or reload occurs
  - System accounting is turned on or off

  Note that there is no time span associated with using the `system` option. It simply causes the switch to transmit whatever accounting data it currently has when one of the above events occurs.

- **Network:** Use `network` if you want to collect accounting information on 802.1X port-based-access to the network by users connected to the physical ports on the switch. (See also “Accounting Service Types” on page 5-56.) For information on this feature, refer to the chapter titled “Configuring Switch Ports as 802.1X Authenticators” in the *Access Security Guide* for your switch.

- **Commands:** When commands accounting is enabled, an accounting notice record is sent after the execution of each command.

---

**Example of common Session ID Configuration**

```text
HP Switch(config)# aaa accounting session-id common
HP Switch(config)# show accounting
Status and Counters - Accounting Information
Interval (min) : 0
Suppress Empty User : No
Sessions Identification : Common

<table>
<thead>
<tr>
<th>Type</th>
<th>Method Mode</th>
<th>Server Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Exec</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Commands</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 5-20. Accounting Configured for the Common Option
Accounting Controls. These options are enabled separately, and define how the switch will send accounting data to a RADIUS server:

- **Start-Stop**: Applies to the **exec**, **network**, and **system** accounting service types:
  - Send a “start record accounting” notice at the beginning of the accounting session and a “stop record notice” at the end of the session. Both notices include the latest data the switch has collected for the requested accounting type.
  - Do not wait for an acknowledgement.

- **Stop-Only**: Applies to the **network**, **exec**, **system**, and **command** service types, as described below:
  - Send a stop record accounting notice at the end of the accounting session. The notice includes the latest data the switch has collected for the requested accounting type (**network**, **exec**, or **system** service types). For the **commands** service type, sends the “Stop” accounting notice after execution of each CLI command.
  - Do not wait for an acknowledgment.

- **Interim-Update**: Applies only to the **command** service type, and is intended for use when the optional **common** session ID is configured. Enabling **interim-update** in this case results in the command accounting records appearing as enclosed sub-parts of the **exec** service type record for a given management session. (Using interim-update when the **unique** session ID is configured has no effect because in this case, the different service types appear as separate accounting processes with separate Acct-Session-ID values.

---

**Note**

Configuring **interim-update** for Command accounting results in all commands being reported as “update” records, regardless of whether common or unique is configured for the accounting session ID (page 5-55).
Syntax: [no] aaa accounting < exec | network | system > < start-stop | stop-only > < radius | syslog>
[no] aaa accounting command < stop-only | interim-only > < radius | syslog>

Configures RADIUS accounting service type and how data will be sent to the RADIUS server.

< exec | network | system | command >: Specifies an accounting service type to configure. Refer to “Accounting Service Types” on page 5-56.

- **start-stop:** Applies to exec, network, and system accounting service types. Refer to “Accounting Controls” on page 5-57.
- **stop-only:** Applies to all accounting service types. Refer to “Accounting Controls” on page 5-57.
- **radius:** Uses RADIUS as the accounting protocol.
- **syslog:** Uses syslog as the accounting protocol.
- **interim-update:** Applies to the commands accounting service type. Refer to “Accounting Controls” on page 5-57.

Example. To configure RADIUS accounting on the switch with **start-stop** for Exec functions, **stop-only** for system functions, and **interim-update** for commands functions. This example continues from figure 5-20, where the session ID was configured as **common**.
Example. If the switch is configured with RADIUS accounting on the switch to use **start-stop** for Exec, System, and Command functions, as shown in figure 5-22, there will be an “Accounting-On” record when the switch boots up and an “Accounting-Off” record when the switch reboots or reloads. (Assume that Acct-Session-Id is configured for **common**.)
Figure 5-22. Example of Accounting Session Operation with “start-stop” Enabled
4. (Optional) Configure Session Blocking and Interim Updating Options

These optional parameters give you additional control over accounting data.

- **Updates:** In addition to using a Start-Stop or Stop-Only trigger, you can optionally configure the switch to send periodic accounting record updates to a RADIUS server.

- **Suppress:** The switch can suppress accounting for an unknown user having no user name.

**Syntax:**  
`[no] aaa accounting update periodic < 1 - 525600 >`  
Sets the accounting update period for all accounting sessions on the switch. (The *no* form disables the update function and resets the value to zero.) (Default: zero; disabled)

**Syntax:**  
`[no] aaa accounting suppress null-username`  
Disables accounting for unknown users having no username. (Default: suppression disabled)

To continue the example in figure 5-21, suppose that you wanted the switch to:

- Send updates every 10 minutes on in-progress accounting sessions.
- Block accounting for unknown users (no username).

```
HP Switch(config)# aaa accounting update periodic 10
HP Switch(config)# aaa accounting suppress null-username
HP Switch(config)# show accounting
Status and Counters - Accounting Information
Interval(min) : 10
Suppress Empty User : Yes
Sessions Identification : Common

<table>
<thead>
<tr>
<th>Type</th>
<th>Method</th>
<th>Server Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Exec</td>
<td>Radius Start-Stop</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Radius Stop-Only</td>
<td></td>
</tr>
<tr>
<td>Commands</td>
<td>Radius Interim-Update</td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 5-23. Example of Optional Accounting Update Period and Accounting Suppression on Unknown User
RADIUS Authentication, Authorization, and Accounting

Viewing RADIUS Statistics

General RADIUS Statistics

Syntax:  show radius [host < ip-addr>]

Shows general RADIUS configuration, including the server IP addresses. Optional form shows data for a specific RADIUS host. To use show radius, the server's IP address must be configured in the switch, which requires prior use of the radius-server host command. (See “Accounting Services” on page 5-47.)

HP Switch# show radius

Status and Counters - General RADIUS Information

Deadtime(min) : 5
Timeout(secs) : 10
Retransmit Attempts : 2
Global Encryption Key : myg10balkey
Dynamic Authorization UDP Port : 3799
Source IP Selection : Outgoing Interface

<table>
<thead>
<tr>
<th>Server IP Addr</th>
<th>Port</th>
<th>Port</th>
<th>CoA</th>
<th>Window</th>
<th>Encryption Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.33.12.65</td>
<td>1812</td>
<td>1813</td>
<td>No</td>
<td>300</td>
<td>my65key</td>
</tr>
</tbody>
</table>

Figure 5-24. Example of General RADIUS Information from Show Radius Command
**Table 5-2. Values for Show Radius Host Output (Figure 5-25)**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round Trip Time</td>
<td>The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.</td>
</tr>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.</td>
</tr>
<tr>
<td>Retransmissions</td>
<td>The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.</td>
</tr>
<tr>
<td>Malformed Responses</td>
<td>The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.</td>
</tr>
<tr>
<td>Bad Authenticators</td>
<td>The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.</td>
</tr>
<tr>
<td>Unknown Types</td>
<td>The number of RADIUS packets of unknown type which were received from this server on the accounting port.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.</td>
</tr>
</tbody>
</table>
### RADIUS Authentication, Authorization, and Accounting

#### Viewing RADIUS Statistics

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Requests</td>
<td>The number of RADIUS Access-Requests the switch has sent since it was last rebooted. (Does not include retransmissions.)</td>
</tr>
<tr>
<td>Accounting Requests</td>
<td>The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.</td>
</tr>
<tr>
<td>Access Challenges</td>
<td>The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.</td>
</tr>
<tr>
<td>Access Accepts</td>
<td>The number of RADIUS Access-Accept packets (valid or invalid) received from this server.</td>
</tr>
<tr>
<td>Access Rejects</td>
<td>The number of RADIUS Access-Reject packets (valid or invalid) received from this server.</td>
</tr>
<tr>
<td>Responses</td>
<td>The number of RADIUS packets received on the accounting port from this server.</td>
</tr>
</tbody>
</table>

### RADIUS Authentication Statistics

**Syntax:**  
`show authentication`

*Displays the primary and secondary authentication methods configured for the Console, Telnet, Port-Access (802.1X), and SSH methods of accessing the switch. Also displays the number of access attempts currently allowed in a session.*

`show radius authentication`

*Displays NAS identifier and data on the configured RADIUS server and the switch’s interactions with this server. (Requires prior use of the radius-server host command to configure a RADIUS server IP address in the switch. See “Accounting Services” on page 5-47.)*
RADIUS Authentication, Authorization, and Accounting

Viewing RADIUS Statistics

HP Switch(config)# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled

| Access Task | Primary  Login | Server Group | Secondary Login |
|-------------+------------+-------------+----------------|
| Console     | Local      | None        |                |
| Telnet      | Radius     | None        |                |
| Port-Access | Local      | None        |                |
| Webui       | Local      | None        |                |
| SSH         | Radius     | None        |                |
| Web-Auth    | ChapRadius | None        |                |
| MAC-Auth    | ChapRadius | None        |                |
|             | Enable     | Enable      | Enable         |

HP Switch(config)# show radius authentication

Status and Counters - RADIUS Authentication Information

NAS Identifier : HP_switch
Invalid Server Addresses : 0

<table>
<thead>
<tr>
<th>UDP</th>
<th>Server IP Addr</th>
<th>Port</th>
<th>Timeouts</th>
<th>Requests</th>
<th>Challenges</th>
<th>Accepts</th>
<th>Rejects</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.33.12.65</td>
<td>1812</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 5-26. Example of Login Attempt and Primary/Secondary Authentication Information from the Show Authentication Command

Figure 5-27. Example of RADIUS Authentication Information from a Specific Server
RADIUS Accounting Statistics

Syntax:  show accounting

Lists configured accounting interval, “Empty User” suppression status, session ID, accounting types, methods, and modes.

show radius accounting

Lists accounting statistics for the RADIUS server(s) configured in the switch (using the radius-server host command).

show accounting sessions

Lists the accounting sessions currently active on the switch.

HP Switch(config)# show accounting

Status and Counters - Accounting Information

  Interval(min) : 5
  Suppress Empty User : No
  Sessions Identification : Common

| Type     | Method Mode       | Server Group
|----------+------------------|--------------|
| Network  | None              |              |
| Exec     | Radius Start-Stop |              |
| System   | Radius Stop-Only  |              |
| Commands | Radius Interim-Update |     |

Figure 5-28. Listing the Accounting Configuration in the Switch
Changing RADIUS-Server Access Order

The switch tries to access RADIUS servers according to the order in which their IP addresses are listed by the `show radius` command. Also, when you add a new server IP address, it is placed in the highest empty position in the list.

Adding or deleting a RADIUS server IP address leaves an empty position, but does not change the position of any other server addresses in the list. For example, if you initially configure three server addresses, they are listed in the order in which you entered them. However, if you subsequently remove the second server address in the list and add a new server address, the new address will be placed second in the list.

Thus, to move a server address up in the list, you must delete it from the list, ensure that the position to which you want to move it is vacant, and then re-enter it. For example, suppose you have already configured the following three RADIUS server IP addresses in the switch:

<table>
<thead>
<tr>
<th>Server IP Addr</th>
<th>Port</th>
<th>Timeouts</th>
<th>Requests</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.33.12.65</td>
<td>1813</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Changing RADIUS-Server Access Order

To exchange the positions of the addresses so that the server at 10.10.10.3 will be the first choice and the server at 10.10.10.1 will be the last, you would do the following:

1. Delete 10.10.10.3 from the list. This opens the third (lowest) position in the list.
2. Delete 10.10.10.1 from the list. This opens the first (highest) position in the list.
3. Re-enter 10.10.10.3. Because the switch places a newly entered address in the highest-available position, this address becomes first in the list.
4. Re-enter 10.10.10.1. Because the only position open is the third position, this address becomes last in the list.

Note: If the switch successfully accesses the first server, it does not try to access any other servers in the list, even if the client is denied access by the first server.

Figure 5-31. Search Order for Accessing a RADIUS Server

To exchange the positions of the addresses so that the server at 10.10.10.3 will be the first choice and the server at 10.10.10.1 will be the last, you would do the following:

1. Delete 10.10.10.3 from the list. This opens the third (lowest) position in the list.
2. Delete 10.10.10.1 from the list. This opens the first (highest) position in the list.
3. Re-enter 10.10.10.3. Because the switch places a newly entered address in the highest-available position, this address becomes first in the list.
4. Re-enter 10.10.10.1. Because the only position open is the third position, this address becomes last in the list.
RADIUS Authentication, Authorization, and Accounting
Changing RADIUS-Server Access Order

HP Switch(config)# no radius host 10.10.10.1
HP Switch(config)# radius host 10.10.10.3
HP Switch(config)# radius host 10.10.10.1
HP Switch# show radius

Status and Counters - General RADIUS Information

| Deadtime(min) : 0 |
| Timeout(secs) : 5 |
| Retransmit Attempts : 3 |
| Global Encryption Key : |
| Dynamic Authorization UDP Port : 3799 |
| Source IP Selection : Outgoing Interface |

<table>
<thead>
<tr>
<th>Auth Acct DM/ Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP Addr Port Port CoA Window Encryption Key</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>10.10.10.3 1812 1813 No 300</td>
</tr>
<tr>
<td>10.10.10.2 1812 1813 No 300</td>
</tr>
<tr>
<td>10.10.10.1 1812 1813 No 300</td>
</tr>
</tbody>
</table>

Figures 5-32. Example of New RADIUS Server Search Order

Removes the “3” and “1” addresses from the RADIUS server list.

Inserts the “3” address in the first position in the RADIUS server list, and inserts the “1” address in the last position in the list.

Shows the new order in which the switch searches for a RADIUS server.
Creating Local Privilege Levels

This feature allows more granular localized control over user access when accessing the switch through the console or by telnet or SSH. Instead of allowing access to all commands with the “manager” command, or very restricted access with the “operator” command, the local access can be customized to allow the commands that the local account is authorized to execute. The new local accounts are in addition to and independent of the existing manager and operator accounts, with the exception that if a username is set for a manager or operator account, that name cannot be the same as any of the local user account names.

To do this, groups are created that contain up to 16 user accounts. The group has a list of match commands that determine if that user is authorized to execute that command. Up to 100 local user accounts are supported. The local user accounts are stored in the configuration as an SHA1 hash, which is only displayed if “include-credentials” is enabled. A password is required for the local user accounts, but nothing else.

There is one default group—operator. Users assigned to the operator group have only operator privileges.

Applying the authorization group to a local user account only occurs if the user logs in using local as the primary authentication method and the aaa authorization commands local command has been executed. Authorization groups are not supported when the login method is set as secondary local authentication.

These commands are authorized at all access levels:

- exit
- logout
- page
- redo
- repeat
- end
Configuring Groups for Local Authorization

You must create a group for local authorization before you can assign local users to it. When creating the group, at least one command is created as part of that group. Typically, multiple commands are assigned to a group. To create a group, enter this command.

**Syntax:**

```
[no] aaa authorization group <group-name> <1-2147483647> match-command <command-string> <permit | deny> [log]
```

Create a local authorization group with the specified name. The name is case-sensitive and may not contain spaces. Duplicate names are not allowed. You can create a maximum of 16 groups. The name of the group can have a maximum of 16 characters.

**<1-2147483647>:** The evaluation order for the match commands.

**match-command <command-string>:** The command string is the CLI command. It must be surrounded in double quotes if it contains any spaces, for example, "vlan *". The <command-string> is a POSIX regular expression and follows POSIX matching rules. For example, the "*" character means match the preceding character zero or more times, so ab*c will match "ac", "abe", "abbc", etc. The "." character means match any character, so ".*" would match anything, while the command string "aaa.*" would match commands that have "aaa" followed by zero or more characters. The "^" character means match to the beginning of the string, so "^aaa.*" would mean the string must start with "aaa" and can have anything after that.

**<permit | deny>:** Either permit or deny execution of the command.

**[log]:** Optional. Indicates the matching of such commands will generate an event log entry for either permitted or denied.

Typically multiple commands are assigned to a group. Each command is entered on a separate line. Commands are evaluated in numerical order of the sequence number until a match is found, then the permit or deny action for that command is executed.
**RADIUS Authentication, Authorization, and Accounting**

**Creating Local Privilege Levels**

**Note**

Commands are expanded before the comparison is done, for example, `sh ver` would be expanded to `show version` and then this command is compared against the command strings of the authorization group.

```plaintext
HP Switch(config)# aaa authorization group Bluegroup 100 match-command configure permit
HP Switch(config)# aaa authorization group Bluegroup 200 match-command telnet permit
HP Switch(config)# aaa authorization group Bluegroup 300 match-command menu permit
```

**Figure 5-33. Example of Creating a Local Authorization Group and Assigning the Commands that are Authorized for the Group**

When a command must be preceded by the execution of another command, then both commands need to be permitted for the command authorization group. For example, you must execute the `configure` command before you can enter the `vlan` context, so both commands must be permitted.

```plaintext
HP Switch(config)# aaa authorization group Redgroup 100 match-command configure permit
HP Switch(config)# aaa authorization group Redgroup 200 match-command "vlan *" permit
```

**Figure 5-34. Example of Configuring Authorized Commands for a Group in the Correct Order**

Some commands cause the switch CLI to enter a special context, such as test mode, and the input is not processed by the normal CLI. Keyboard input is not checked against the command authorization group. If these special contexts are permitted, the user can proceed outside the control and logging of the command group configuration.

**Configuring a Local User for a Group**

Local manager user logins and authorized command configuration are mutually exclusive with RADIUS or TACACS authentication and with RADIUS authorization and accounting.
To create a local user enter this command for the group with the appropriate authorizations.

**Syntax:**  
```plaintext  
[no] aaa authentication local-user <username> group <group-name>  
password <plaintext | sha1 <password>>  
```

Defines a local user for a defined group.

- **local-user <username>**: The local user being added to the authorization group. The username can have a maximum of 16 characters. It must not contain spaces and is case-sensitive.

- **group <group-name>**: The authorization group the local user belongs to. The group must have been created already.

- **password <plaintext | sha1 <password>>**: The plaintext password string can have a maximum of 16 characters. It must not contain spaces and is case-sensitive.

**Note:** You are not allowed to actually enter the plaintext password in-line as part of the command; you will be prompted for it. The password is obscured when you enter it. This is similar to entering the password for the manager or operator.

If include-credentials is enabled, displaying the configuration shows the user passwords as SHA1 hash. If include-credentials is not enabled, then no password information is shown.

If a user is assigned to a command group and the group is subsequently deleted, the user will have operator privileges.

```
HP Switch(config)# aaa authentication local-user User1 group Redgroup password plaintext
New password for User1: ********
Please retype new password for User1: ********
HP Switch(config)#
```

**Figure 5-35. Example of Creating a Local User for a Group**
Displaying Command Authorization Information

To display information about users and command authorization for command groups, enter this command.

**Syntax:**  
show authorization group [group-name]

*Displays information about users and command authorization for command groups.*

*Specifying the group parameter without any group names displays information for all configured groups.*

![Example Showing Command Information for all Groups](image)

---

**Figure 5-36. Example Showing Command Information for all Groups**

---

5-74
Dynamic Removal of Authentication Limits

Overview

In some situations, it is desirable to configure RADIUS attributes for downstream supplicant devices that allow dynamic removal of the 802.1X, MAC, and Web authentication limits on the associated port of the authenticator switch. This eliminates the need to manually reconfigure ports associated with downstream 802.1X-capable devices, and MAC relay devices such as IP phones, on the authenticator switches. When the RADIUS authentication ages out, the authentication limits are dynamically restored. This enhancement allows a common port policy to be configured on all access ports by creating new RADIUS HP vendor-specific attributes (VSAs) that will dynamically override the authentication limits. The changes are always applied to the port on the authenticator switch associated with the supplicant being authenticated.

Note

All the changes requested by the VSAs must be valid for the switch configuration. For example, if either MAC-based or Web-based port access is configured while 802.1X port access is in client mode, a RADIUS client with a VSA to change the 802.1X port access to port-based mode is not allowed. 802.1X in port-based mode is not allowed with MAC-based or web-based port access types. However, if the authenticating client has VSAs to disable MAC-based and Web-based authentication in conjunction with changing 802.1X to port-based mode, then client authentication is allowed.

Configuring the RADIUS VSAs

Only RADIUS authenticated port-access clients will be able to dynamically change the port access settings using the new proprietary RADIUS VSAs. The settings that can be overridden are:

- Client limit (address limit with mac-based port access)
- Disabling the port-access types
- Setting the port mode in which 802.1X is operating
If the VSA client limit decreases the switch’s configured client limit, all clients except the client that is overriding the settings is deauthenticated. Only one client session at a time can override the port-access settings on a port. When the client session is deauthenticated, the port resets itself to the configured settings. This port reset causes the deauthentication of all clients for the port-access authentication types that had their settings changed dynamically.

The new VSAs are:

- **HP-Port-Client-Limit-Dot1x**: This VSA temporarily alters the 802.1X authentication client limit to the value contained in the VSA. Values range from 0 to 32 clients. A zero client limit means this VSA is disabled. This is an HP proprietary VSA with a value of 10.

- **HP-Port-Client-Limit-MA**: This VSA temporarily alters the MAC authentication client limit to the value contained in the VSA. Values range from 0 to 256 clients. A zero client limit means this VSA is disabled. This is an HP proprietary VSA with a value of 11.

- **HP-Port-Client-Limit-WA**: This VSA temporarily alters the Web authentication client limit to the value contained in the VSA. Values range from 0 to 256 clients. A zero client limit means this VSA is disabled. This is an HP proprietary VSA with a value of 12.

- **HP-Port-Auth-Mode-Dot1x**: This VSA temporarily alters the 802.1X authentication mode to be either port-based or user-based depending on the value in the VSA. A port-based VSA is set with a value of 1; a user-based VSA is set with a value of 2. This is an HP proprietary VSA with a value of 13.

  If an 802.1X port is operating in port-based mode, it is invalid to set the 802.1X client limit using the HP-Port-Client-Limit VSA.

**Note**

The changing of the client limits for a port using VSAs is temporary. The running configuration file is not changed and still displays the client limit and address limit settings.

Each authentication type may have a unique value for the client limit. If the value of the VSA is zero, the authentication type corresponding to that VSA will be disabled.
Settings for these VSAs are in effect for the duration of the authenticated session of the downstream supplicant switch. If for any reason there is a loss of the session (link loss between authenticator switch and supplicant switch, or authentication failure during reauthentication), the originally configured 802.1X and MAC authentication limits are restored.

Displaying the Port-access Information

The `show port-access summary` command displays the dynamically changed client limit settings.

**Syntax:** `show port-access summary [radius-overridden]`

*Displays summary configuration information for all ports, including the ports that have client limits set by RADIUS VSAs.*

**radius-overridden**: *Displays only the ports with client limits that are overridden by RADIUS attributes.*

**Note**

If the command `no aaa port-access authentication <port-list> client-limit` is executed, the port access is in port-mode. If the 802.1X client-limit is configured with a value from 1-32, the port access is in user-mode.

---

<table>
<thead>
<tr>
<th>Port</th>
<th>Authenticator</th>
<th>Web Auth</th>
<th>MAC Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enabled Mode Limit</td>
<td>Enabled Limit</td>
<td>Enabled Limit</td>
</tr>
<tr>
<td>1</td>
<td>Yes</td>
<td>user*</td>
<td>1*</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>user 32</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>port 1</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>port 1</td>
<td>No*</td>
</tr>
</tbody>
</table>

**Figure 5-37. Example of Summary Configuration Information Showing RADIUS Overridden Client Limits**
To display the configuration information for just those ports that are dynamically overridden by RADIUS attributes, use the `show port-access summary radius-overridden` command.

```
HP Switch(config)# show port-access summary radius-overridden
```

<table>
<thead>
<tr>
<th>Authenticator</th>
<th>Web Auth</th>
<th>MAC Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enabled</td>
<td>Mode</td>
</tr>
<tr>
<td>1</td>
<td>Yes</td>
<td>user*</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>user</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>port</td>
</tr>
</tbody>
</table>

**Figure 5-38. Example of Output for Client-limit Values that are RADIUS Overridden**

**Operating Notes**

- Only RADIUS authentication supports the new VSAs. Other authentication types, such as TACACS, are not supported.

- The new VSAs are not supported in IDM and they cannot be specified in the configurations. The new VSAs must be configured manually.

- If the RADIUS server delivers a new VSA to an authenticator switch that does not understand it, the Access-Accept message is rejected.
## Messages Related to RADIUS Operation

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can’t reach RADIUS server &lt; x.x.x.x &gt;.</td>
<td>A designated RADIUS server is not responding to an authentication request. Try pinging the server to determine whether it is accessible to the switch. If the server is accessible, then verify that the switch is using the correct encryption key and that the server is correctly configured to receive an authentication request from the switch.</td>
</tr>
<tr>
<td>No server(s) responding.</td>
<td>The switch is configured for and attempting RADIUS authentication, however it is not receiving a response from a RADIUS server. Ensure that the switch is configured to access at least one RADIUS server. (Use <code>show radius</code>.) If you also see the message Can’t reach RADIUS server &lt; x.x.x.x &gt;, try the suggestions listed for that message.</td>
</tr>
<tr>
<td>Not legal combination of authentication methods.</td>
<td>Indicates an attempt to configure <code>local</code> as both the primary and secondary authentication methods. If <code>local</code> is the primary method, then <code>none</code> must be the secondary method.</td>
</tr>
</tbody>
</table>
Configuring RADIUS Server Support for Switch Services

Overview

This chapter provides information that applies to setting up a RADIUS server to configure the following switch features on ports supporting RADIUS-authenticated clients:

- CoS
- Rate-Limiting
- ACLS

Optional Network Management Applications. Per-port CoS and rate-limiting assignments through a RADIUS server are also supported in the PCM+ application. Per-port ACLs through a RADIUS server can also be augmented using the Identity-Driven Management (IDM) application available for use with PCM+. However, the features described in this chapter can be used without PCM+ or IDM support, if desired.

For information on configuring client authentication on the switch, refer to the chapter 5, “RADIUS Authentication, Authorization, and Accounting”.

Optional PCM+ and IDM Applications. PCM+ is a Windows-based network management solution for all manageable HP devices. It provides network: mapping and polling capabilities, device auto-discovery and topology, tools for device configuration and management, monitoring network traffic, and alerts and troubleshooting information for HP networks.

Identity Driven Manager (IDM) is an add-on module to the PCM+ application. IDM extends the functionality of PCM+ to include authorization control features for edge devices in networks using RADIUS servers and Web-Authentication, MAC-Authentication, or 802.1X security protocols.
RADIUS Server Configuration for Per-Port CoS (802.1p Priority) and Rate-Limiting

This section provides general guidelines for configuring a RADIUS server to dynamically apply CoS (Class of Service) and Rate-Limiting for inbound traffic on ports supporting authenticated clients. To configure support for these services on a specific RADIUS server application, refer to the documentation provided with the application. (If multiple clients are authenticated on a port where inbound CoS and Rate-Limiting values have been imposed by a RADIUS server, the CoS and Rate-Limiting applied to all clients on the port are those that are assigned by RADIUS for the most recently authenticated client.

<table>
<thead>
<tr>
<th>Service</th>
<th>Control Method and Operating Notes:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.1p (CoS) Priority Assignments on Inbound Traffic</strong></td>
<td>Vendor-Specific Attribute configured in the RADIUS server.</td>
</tr>
<tr>
<td>This feature assigns a RADIUS-specified 802.1p priority to all inbound packets received on a port supporting an authenticated client.</td>
<td>HP vendor-specific ID:11</td>
</tr>
<tr>
<td>VSA: 40 (string = HP)</td>
<td>Setting: HP-COS = xxxxxxxx where: x = desired 802.1p priority</td>
</tr>
<tr>
<td>Note: This is typically an eight-octet field. Enter the same x-value in all eight octets</td>
<td>Requires a port-access (802.1X Web Auth, or MAC Auth) authentication method configured on the client's port on the HP switch.</td>
</tr>
<tr>
<td>For more on 802.1p priority levels, refer to the section titled “Overview” in the “Quality of Service (QoS)” chapter of the Advanced Traffic Management Guide for your switch.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring RADIUS Server Support for Switch Services

RADIUS Server Configuration for Per-Port CoS (802.1q Priority) and Rate-Limiting

<table>
<thead>
<tr>
<th>Service</th>
<th>Control Method and Operating Notes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate-Limiting on inbound traffic</td>
<td>Vendor-Specific Attribute configured in the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>HP vendor-specific ID:11</td>
</tr>
<tr>
<td></td>
<td>VSA: 46 (integer = HP)</td>
</tr>
<tr>
<td></td>
<td>Setting: HP-RATE-LIMIT = &lt; bandwidth-in-Kbps &gt;</td>
</tr>
<tr>
<td>Note:</td>
<td>The CLI command for configuring a rate-limit on a port uses a percentage value.</td>
</tr>
<tr>
<td></td>
<td>However, using a VSA on a RADIUS server to specify a rate-limit requires the actual Kbps to which</td>
</tr>
<tr>
<td></td>
<td>you want to limit inbound traffic volume. Thus, to limit in-bound traffic on a gigabit port to</td>
</tr>
<tr>
<td></td>
<td>50% of the port’s bandwidth capacity requires a VSA setting of 500000 (1,000,000 x 0.5).</td>
</tr>
<tr>
<td></td>
<td>Requires a port-access (802.1X, Web Auth, or MAC Auth) authentication method configured on the</td>
</tr>
<tr>
<td></td>
<td>client’s port on the HP switch.</td>
</tr>
<tr>
<td></td>
<td>For more on Rate-Limiting, refer to “Rate-Limiting” in the “Port Traffic Controls” chapter of the</td>
</tr>
<tr>
<td></td>
<td>Management and Configuration Guide for your switch.</td>
</tr>
</tbody>
</table>

Applied Rates for RADIUS-Assigned Rate Limits

On the switches covered by this guide, rate limits are applied incrementally, as determined by the RADIUS-applied rate. For any given bandwidth assignment, the switch applies the nearest rate increment that does not exceed the assigned value. The increments are in graduated steps, as described in table 6-1.

Table 6-1. RADIUS-Assigned Rate-Limit Increments

<table>
<thead>
<tr>
<th>RADIUS-Assigned Rate-Limit Increments</th>
<th>Applied Rate-Limiting Increment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 10,999,999</td>
<td>100 Kbps</td>
</tr>
<tr>
<td>11,000,000 - 100,999,999</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>101,000,000 - 999,999,999</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>1,000,000,000 - 10 Gbps</td>
<td>100 Mbps</td>
</tr>
</tbody>
</table>

For example, some of the following RADIUS-assigned rates fall between their respective incremental values, resulting in applied rates lower than the RADIUS-assigned rates. However, others match their respective incremental values, resulting in no difference between the RADIUS-assigned rate limits and the applied rate limits.
Table 6-2. Examples of Assigned and Applied Rate Limits

<table>
<thead>
<tr>
<th>RADIUS-Assigned Bandwidth (Kbps)</th>
<th>Applied Increments</th>
<th>Applied Rate Limit (Kbps)</th>
<th>Difference/Kbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,250</td>
<td>100 Kbps</td>
<td>5,200</td>
<td>50 Kbps</td>
</tr>
<tr>
<td>50,250</td>
<td>1 Mbps</td>
<td>50,000</td>
<td>250 Kbps</td>
</tr>
<tr>
<td>51,000</td>
<td>1 Mbps</td>
<td>51,000</td>
<td>0 Kbps</td>
</tr>
<tr>
<td>525,000</td>
<td>10 Mbps</td>
<td>520,000</td>
<td>5,000 Kbps</td>
</tr>
<tr>
<td>530,000</td>
<td>10 Mbps</td>
<td>530,000</td>
<td>0 Kbps</td>
</tr>
<tr>
<td>1,250,000</td>
<td>100 Mbps</td>
<td>1,200,000</td>
<td>50,000 Kbps</td>
</tr>
<tr>
<td>1,300,000</td>
<td>100 Mbps</td>
<td>1,300,000</td>
<td>0 Kbps</td>
</tr>
</tbody>
</table>

Viewing the Currently Active Per-Port CoS and Rate-Limiting Configuration Specified by a RADIUS Server

While a port-access authenticated client session is active, any RADIUS-imposed port settings override their counterparts in the port’s configuration. For example, if the switch configuration allows port B1 a rate-limit of 80% of the port’s available bandwidth, but the RADIUS server specifies a rate-limit of 50% for a given authenticated client, then the switch shows the RADIUS-imposed rate-limit for that port as long as the authenticated client session is active.
Configuring RADIUS Server Support for Switch Services
RADIUS Server Configuration for Per-Port CoS (802.1p Priority) and Rate-Limiting

Syntax:
show port-access authenticator [port-list]
show rate-limit all
show qos port-priority

These commands display the CoS and Rate-Limiting settings specified by the RADIUS server used to grant authentication for a given client on a given port. When the authenticated client session closes, the switch resets these fields to the values to which they are configured in the switch’s running-config file.

show port-access authenticator [port-list] displays, for 802.1X authentication, the status of RADIUS-imposed overrides of the switch’s per-port CoS and Rate-Limiting configuration.

show rate-limit all displays, for all port-access authentication methods (802.1X, Web-Auth, and MAC-Auth), the status of RADIUS-imposed overrides of the switch’s per-port Rate-Limiting configuration.

show qos port-priority displays, for all port-access authentication methods (802.1X, Web-Auth, and MAC-Auth), the status of RADIUS-imposed overrides of the switch’s per-port CoS (802.1p) priority for inbound packets.

<table>
<thead>
<tr>
<th>Port</th>
<th>Limit</th>
<th>Mode</th>
<th>Radius Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No-override</td>
</tr>
<tr>
<td>2</td>
<td>500 kbps</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>50 %</td>
<td>Disabled</td>
<td>No-override</td>
</tr>
<tr>
<td>4</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No-override</td>
</tr>
<tr>
<td>5</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No-override</td>
</tr>
<tr>
<td>6</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No-override</td>
</tr>
<tr>
<td>7</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No-override</td>
</tr>
</tbody>
</table>

Port 2 has a rate limit of 500 Kbps with no RADIUS override.
Port 3 has a 50 percent rate limit, which is 50% of the port’s available bandwidth.
The 80 in the Radius Override field indicates that there is an active client session in which the RADIUS server used to authenticate the most recent client has imposed an inbound bandwidth limit of 80%.

Disabled indicates that there is no default rate-limit configured for the port. No-override indicates that there is currently no RADIUS-imposed rate-limit on the associated ports.

Figure 6-1. Example of Displaying Inbound Rate-Limiting Imposed by a RADIUS Session
Configuring RADIUS Server Support for Switch Services
RADIUS Server Configuration for Per-Port CoS (802.1p Priority) and Rate-Limiting

HP Switch(config)# show qos port-priority

Port priorities

<table>
<thead>
<tr>
<th>Port</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
<th>Radius Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>Priority</td>
<td>3</td>
<td>3</td>
<td>No-override</td>
</tr>
<tr>
<td>B2</td>
<td>No-override</td>
<td>No-override</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>B3</td>
<td>No-override</td>
<td>No-override</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>B4</td>
<td>DSCP</td>
<td>001010</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>B5</td>
<td>No-override</td>
<td>No-override</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>B6</td>
<td>No-override</td>
<td>No-override</td>
<td>No-override</td>
<td></td>
</tr>
</tbody>
</table>

Note

Where multiple clients are currently authenticated on a given port where inbound CoS and Rate-Limiting values have been imposed by a RADIUS server, the port operates with the inbound CoS priority and rate-limit assigned by RADIUS for the most recently authenticated client. Any earlier CoS or rate-limit values on the same port for authenticated client sessions that are still active are overwritten by the most recent RADIUS-imposed values. For example, if client “X” is authenticated with a CoS of 5 and a rate-limit of 75%, and client “Y” later becomes authenticated with a CoS of 3 and a rate-limit of 50% while the session for client “X” is still active, then the port will operate with a CoS of 3 and a rate-limit of 50% for both clients.
Configuring and Using RADIUS-Assigned Access Control Lists

Introduction

A RADIUS-assigned ACL is configured on a RADIUS server and dynamically assigned by the server to filter traffic entering the switch through a specific port after the client is authenticated by the server. Note that client authentication can be enhanced by using PCM+ with the optional IDM application.

The information in this section describes how to apply RADIUS-assigned ACLs on the switch, and assumes a general understanding of ACL structure and operation. If you need information on ACL filtering criteria, design, and operation, please refer to chapter 9, “IPv4 Access Control Lists (ACLs)”.

Terminology

ACE: See Access Control Entry, below.

Access Control Entry (ACE): An ACE is a policy consisting of a packet-handling action and criteria to define the packets on which to apply the action. For RADIUS-assigned ACLs, the elements composing the ACE include:

- **permit** or **drop** (action)
- **in** < *ip-packet-type* > from any (source)
- **to** < *ip-address* [/ *mask* ] | any > (destination)
- [ *port-* ] (optional TCP or UDP application port numbers used when the packet type is TCP or UDP)

ACL: See Access Control List, below.

Access Control List (ACL): A list (or set) consisting of one or more explicitly configured Access Control Entries (ACEs) and terminating with an implicit “deny” default which drops any IP packets that do not have a match with any explicit ACE in the named ACL. An ACL can be “standard” or “extended”. See “Standard ACL” and “Extended ACL”. Both can be applied in any of the following ways:

- **Static Port ACL**: an ACL assigned to filter inbound traffic on a specific switch port
RADIUS-assigned ACL: dynamic ACL assigned to a port by a RADIUS server to filter inbound traffic from an authenticated client on that port.

An ACL can be configured on an interface as a static port ACL. (RADIUS-assigned ACLs are configured on a RADIUS server.)

ACL Mask: Follows a destination IP address listed in an ACE. Defines which bits in a packet's corresponding IP addressing must exactly match the IP addressing in the ACE, and which bits need not match (wildcards).

DA: The acronym for Destination IP Address. In an IP packet, this is the destination IP address carried in the header, and identifies the destination intended by the packet's originator.

Deny: An ACE configured with this action causes the switch to drop a packet for which there is a match within an applicable ACL.

Deny Any Any: An abbreviated form of deny in ip from any to any, which denies any inbound IP traffic from any source to any destination.

Dynamic Port ACL: See RADIUS-Assigned ACL.

Implicit Deny: If the switch finds no matches between an inbound packet and the configured criteria in an applicable ACL, then the switch denies (drops) the packet with an implicit “deny IP any/any” operation. You can preempt the implicit “deny IP any/any” in a given ACL by configuring permit in ip from any to any as the last explicit ACE in the ACL. Doing so permits any inbound IP packet that is not explicitly permitted or denied by other ACEs configured sequentially earlier in the ACL. Unless otherwise noted, “implicit deny IP any” refers to the “deny” action enforced by both standard and extended ACLs.

Inbound Traffic: For the purpose of defining where the switch applies ACLs to filter traffic, inbound traffic is any IP packet that enters the switch from a given client on a given port.

NAS (Network Attached Server): In this context, refers to a HP switch configured for RADIUS operation.

Outbound Traffic: For defining the points where the switch applies an ACL to filter traffic, outbound traffic is routed traffic leaving the switch through a VLAN interface (or a subnet in a multinetted VLAN). “Outbound traffic” can also apply to switched traffic leaving the switch on a VLAN interface.
**Permit:** An ACE configured with this action allows the switch to forward an inbound packet for which there is a match within an applicable ACL.

**Permit Any Any:** An abbreviated form of `permit in ip from any to any`, which permits any inbound IP traffic from any source to any destination.

**RADIUS-Assigned ACL:** An ACL application type in which the ACL is assigned by a RADIUS server to a port to filter inbound IP traffic from a specific client authenticated by the server for that port.

**Static Port ACL:** An ACL statically configured on a specific port, group of ports, or trunk. A static port ACL filters all incoming traffic on the port, regardless of whether it is switched or routed.

**VSA (Vendor-Specific-Attribute):** A value used in a RADIUS-based configuration to uniquely identify a networking feature that can be applied to a port on a given vendor's switch during an authenticated client session.

**Wildcard:** The part of a mask that indicates the bits in a packet's IP addressing that do not need to match the corresponding bits specified in an ACL. See also [ACL Mask](#) on page 6-8.
Overview of RADIUS-Assigned, Dynamic ACLs

RADIUS-assigned ACLs enhance network and switch management access security and traffic control by permitting or denying authenticated client access to specific network resources and to the switch management interface. This includes preventing clients from using TCP or UDP applications (such as Telnet, SSH, Web browser, and SNMP) if you do not want their access privileges to include these capabilities.

This feature is designed for use on the network edge to accept RADIUS-assigned, per-port ACLs for Layer-3 filtering of IP traffic entering the switch from authenticated clients. A given RADIUS-assigned ACL is identified by a unique username/password pair or client MAC address, and applies only to IP traffic entering the switch from clients that authenticate with the unique credentials. The switch allows multiple RADIUS-assigned ACLs on a given port, up to the maximum number of authenticated clients allowed on the port.

A RADIUS-assigned ACL filters IP traffic entering the switch from the client whose authentication initiated the ACL assignment. Filtering criteria is based on destination and/or IP traffic type (such as TCP and UDP traffic) and traffic counter options. Implementing the feature requires:

- RADIUS authentication using the 802.1X, Web authentication, or MAC authentication services available on the switch to provide client authentication services
- configuring the ACLs on the RADIUS server (instead of the switch), and assigning each ACL to the username/password pair or MAC address of the clients you want the ACLs to support

Using RADIUS to dynamically apply per-port ACLs to edge ports enables the switch to filter IP traffic coming from outside the network, thus removing unwanted IP traffic as soon as possible and helping to improve system performance.
A RADIUS-assigned ACL assignment filters all inbound IP traffic from an authenticated client on a port, regardless of whether the client’s IP traffic is to be switched or routed.

RADIUS-assigned ACLs can be used either with or without PCM+ and IDM support. (Refer to “Optional PCM+ and IDM Applications” on page 6-1.)

ACLs enhance network security by blocking selected IP traffic, and can serve as one aspect of network security. However, because ACLs do not protect from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete edge security solution.

The ACLs described in this section do not screen non-IP traffic such as AppleTalk and IPX.

### Contrasting Dynamic (RADIUS-Assigned) and Static ACLs

Table 6-3 highlights several key differences between the static ACLs configurable on switch ports, and the RADIUS-assigned ACLs that can be assigned to individual ports by a RADIUS server.

<table>
<thead>
<tr>
<th>RADIUS-assigned ACLs</th>
<th>Static Port ACLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured in client accounts on a RADIUS server.</td>
<td>Configured on switch ports.</td>
</tr>
<tr>
<td>Designed for use on the edge of the network where filtering of IP traffic entering the switch from individual, authenticated clients is most important and where clients with differing access requirements are likely to use the same port.</td>
<td>Designed for use where the filtering needs focus on static configurations covering:</td>
</tr>
<tr>
<td>Implementation requires client authentication.</td>
<td>• switched or routed IP traffic entering the switch from multiple sources or from unauthenticated sources</td>
</tr>
<tr>
<td>Identified by the credentials (username/password pair or the MAC address) of the specific client the ACL is intended to service.</td>
<td>• IP traffic from multiple sources and having a destination on the switch itself</td>
</tr>
<tr>
<td>Supports dynamic assignment to filter only the IP traffic entering the switch from an authenticated client on the port to which the client is connected. (IP traffic can be routed or switched, and includes IP traffic having a DA on the switch itself.)</td>
<td>Supports static assignments to filter switched or routed IP traffic entering the switch, or routed IP traffic leaving the switch.</td>
</tr>
<tr>
<td>When the authenticated client session ends, the switch removes the RADIUS-assigned ACL from the client port.</td>
<td>Remains statically assigned to the port.</td>
</tr>
</tbody>
</table>
Configuring RADIUS Server Support for Switch Services
Configuring and Using RADIUS-Assigned Access Control Lists

### RADIUS-assigned ACLs

<table>
<thead>
<tr>
<th>Allows one RADIUS-assigned ACL per authenticated client on a port. (Each such ACL filters traffic from a different, authenticated client.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: The switch provides ample resources for supporting RADIUS-assigned ACLs and other features. However, the actual number of ACLs supported depends on the switch's current feature configuration and the related resource requirements. For more information, refer to the appendix titled &quot;Monitoring Resources&quot; in the Management and Configuration Guide for your switch.</td>
</tr>
<tr>
<td>Supports only extended ACLs. (Refer to Terminology.)</td>
</tr>
<tr>
<td>A given RADIUS-assigned ACL filters only the IP traffic entering the switch from the authenticated client corresponding to that ACL, and does not filter IP traffic inbound from other authenticated clients. (The traffic source is not a configurable setting.)</td>
</tr>
<tr>
<td>A given RADIUS-assigned ACL operates on a port to filter only the IP traffic entering the switch from the authenticated client corresponding to the ACL, and does not filter IP traffic inbound from other authenticated clients. (The traffic source is not a configurable setting.)</td>
</tr>
<tr>
<td>ACEs allow a counter (cnt) option that causes a counter to increment when there is a packet match.</td>
</tr>
</tbody>
</table>

### Static Port ACLs

<table>
<thead>
<tr>
<th>Supports static ACLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports standard and extended ACLs</td>
</tr>
<tr>
<td>A static port ACL applied on a port filters all traffic entering the switch through that port.</td>
</tr>
<tr>
<td>No client authentication requirement.</td>
</tr>
<tr>
<td>ACEs allow a log option that generates a log message whenever there is a packet match with a “deny” ACE.</td>
</tr>
</tbody>
</table>

### Caution Regarding the Use of Source Routing

Source routing is enabled by default on the switch and can be used to override ACLs. For this reason, if you are using ACLs to enhance network security, the recommended action is to use the `no ip source-route` command to disable source routing on the switch. (If source routing is disabled in the running-config file, the `show running` command includes “no ip source-route” in the running-config file listing.)

### How a RADIUS Server Applies a RADIUS-Assigned ACL to a Switch Port

A RADIUS-assigned ACL configured on a RADIUS server is identified and invoked by the unique credentials (username/password pair or a client MAC address) of the specific client the ACL is designed to service. Where the username/password pair is the selection criteria, the corresponding ACL can also be used for a group of clients that all require the same ACL policy and use...
Configuring RADIUS Server Support for Switch Services
Configuring and Using RADIUS-Assigned Access Control Lists

the same username/password pair. Where the client MAC address is the selection criteria, only the client having that MAC address can use the corresponding ACL. When a RADIUS server authenticates a client, it also assigns the ACL configured with that client’s credentials to the port. The ACL then filters the client’s inbound IP traffic and denies (drops) any such traffic that is not explicitly permitted by the ACL. (Every ACL ends with an implicit **deny in ip from any to any** (“deny any any”) ACE that denies IP traffic not specifically permitted by the ACL.) When the client session ends, the switch removes the RADIUS-assigned ACL from the client port.

**Notes**

Included in any RADIUS-assigned ACL, there is an implicit **deny in ip from any to any** (“deny any any”) command that results in a default action to deny any inbound IP traffic that is not specifically permitted by the ACL. To override this default, use an explicit **permit in ip from any to any** (“permit any any”) as the last ACE in the ACL. This will only apply to the authenticated client; the default **ip deny any any** applies to all other IPv4 traffic.

On a given port, RADIUS-assigned ACL filtering applies to all IPv4 traffic once a client is authenticated.

**Multiple Clients Sharing the Same RADIUS-Assigned ACL.** When multiple clients supported by the same RADIUS server use the same credentials, they will all be serviced by different instances of the same ACL. (The actual IP traffic inbound from any client on the switch carries a source MAC address unique to that client. The RADIUS-assigned ACL uses this MAC address to identify the traffic to be filtered.)

**Multiple ACL Application Types on an Interface.** The switch allows simultaneous use of all supported ACL application types on an interface.

**General ACL Features, Planning, and Configuration**

These steps suggest a process for using RADIUS-assigned ACLs to establish access policies for client IP traffic.

1. Determine the policies you want to enforce for authenticated client traffic inbound on the switch.

2. Plan ACLs to execute traffic policies:
   - Apply ACLs on a per-client basis where individual clients need different traffic policies or where each client must have a different username/password pair or will authenticate using MAC authentication.
   - Apply ACLs on a client group basis where all clients in a given group can use the same traffic policy and the same username/password pair.
3. Configure the ACLs on a RADIUS server accessible to the intended clients.

4. Configure the switch to use the desired RADIUS server and to support the desired client authentication scheme. Options include 802.1X, Web authentication, or MAC authentication. (Note that the switch supports the option of simultaneously using 802.1X with either Web or MAC authentication.)

5. Test client access on the network to ensure that your RADIUS-assigned ACL application is properly enforcing your policies.

For further information common to all ACL applications, refer to the following sections in chapter 9, “IPv4 Access Control Lists (ACLs)”:  
- “Features Common to All ACL Applications” on page 9-13  
- “General Steps for Planning and Configuring ACLs” on page 9-15  
- “General Steps for Planning and Configuring ACLs” on page 9-15

**The Packet-filtering Process**

Packet-filtering in an applied ACL is sequential, from the first ACE in the ACL to the implicit “deny any” following the last explicit ACE. This operation is the same regardless of whether the ACL is applied dynamically from a RADIUS server or statically in the switch configuration. For details of this process, refer to “IPv4 Static ACL Operation” in chapter 9, “IPv4 Access Control Lists (ACLs)”.

---

**Note**  
If a RADIUS-assigned ACL permits an authenticated client's inbound IP packet, but the client port is also configured with a static port ACL, then the packet will also be filtered by these other ACLs. If there is a match with a deny ACE in any of these ACLs, the switch drops the packet.

---

**Caution**  
ACLs can enhance network security by blocking selected IP traffic, and can serve as one aspect of maintaining network security. However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete security solution.
Operating Rules for RADIUS-Assigned ACLs

- **Relating a Client to a RADIUS-Assigned ACL:** A RADIUS-assigned ACL for a particular client must be configured in the RADIUS server under the authentication credentials the server should expect for that client. (If the client must authenticate using 802.1X and/or Web Authentication, the username/password pair forms the credential set. If authentication is through MAC Authentication, then the client MAC address forms the credential set.) For more on this topic, refer to “Configuring an ACL in a RADIUS Server” on page 6-15.

- **Multiple Clients Using the Same Username/Password Pair:** Multiple clients using the same username/password pair will use duplicate instances of the same ACL.

- **Limits for ACEs in RADIUS-assigned ACLs:** The switch supports up to 80 characters in a single ACE. Exceeding this limit causes the related client authentication to fail.

- **Effect of RADIUS-assigned ACLs on Inbound Traffic for Two Clients on the Same Port:** On a port configured for 802.1X user-based access where up to two clients are connected, if a given client’s authentication results in a RADIUS-assigned ACL assignment, then the authentication of the other client concurrently using the port must also include a RADIUS-assigned ACL assignment. Thus, if a RADIUS server is configured to assign a RADIUS-assigned ACL when client “X” authenticates, but is not configured to do the same for client “Y”, then traffic from client “Y” will be blocked whenever client “X” is authenticated on the port (and client “Y” will be deauthenticated). For this reason, if two clients are authenticated on a port, a separate RADIUS-assigned ACL must be assigned by a RADIUS server for each authenticated client. Inbound IP traffic from a client whose authentication does not result in a RADIUS-assigned ACL assignment will be blocked and the client will be deauthenticated. Also, if 802.1X port-based access is configured on the port, only one client can be authenticated on the port at any given time. In this case, no other inbound client traffic is allowed.

Configuring an ACL in a RADIUS Server

This section provides general guidelines for configuring a RADIUS server to specify RADIUS-assigned ACLs. Also included is an example configuration for a FreeRADIUS server application. However, to configure support for these services on a specific RADIUS server application, please refer to the documentation provided with the application.
Elements in a RADIUS-assigned ACL Configuration. A RADIUS-assigned ACL configuration in a RADIUS server has the following elements:

- **vendor and ACL identifiers:**
  - HP Vendor-Specific ID: 11
  - Vendor-Specific Attribute for ACLs: 61 (string = HP-IP-FILTER-RAW)
  - Setting: HP-IP-FILTER-RAW = < “permit” or “deny” ACE >
  (Note that the “string” value and the “Setting” specifier are identical.)

- **ACL configuration, including:**
  - one or more explicit “permit” and/or “deny” ACEs created by the system operator
  - implicit deny any any ACE automatically active after the last operator-created ACE

Nas-Filter-Rule-Options

Table 6-4. Nas-Filter-Rule Attribute Options

<table>
<thead>
<tr>
<th>Service</th>
<th>Control Method and Operating Notes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLs Applied to Client Traffic Inbound to the Switch</td>
<td><strong>Standard Attribute: 92</strong>&lt;br&gt;This is the preferred attribute for use in RADIUS-assigned ACLs to configure ACEs to filter IPv4 traffic.</td>
</tr>
<tr>
<td>Assigns a RADIUS-configured ACL to filter inbound packets received from a specific client authenticated on a switch port.</td>
<td><strong>Entry for IPv4-Only ACE To Filter Client Traffic:</strong>&lt;br&gt;<strong>Nas-filter-Rule = “&lt; permit or deny ACE &gt;”</strong> (Standard Attribute 92)</td>
</tr>
<tr>
<td>For example:</td>
<td><strong>Nas-filter-Rule=“permit in tcp from any to any”</strong></td>
</tr>
</tbody>
</table>

| ACLs Applied to Client Traffic Inbound to the Switch | **HP-Nas-Filter-Rule (Vendor-Specific Attribute): 61**<br>This attribute is maintained for legacy purposes to support ACEs in RADIUS-assigned ACLs. However, for new or updated configurations HP recommends using the Standard Attribute (92) described earlier in this table instead of the HP-Nas-filter-Rule attribute described here. |
| Assigns a RADIUS-configured IPv4 ACL to filter inbound IPv4 packets received from a specific client authenticated on a switch port. | **HP vendor-specific ID: 11** <br>VSA: 61 (string = HP-Nas-Filter-Rule) <br>**Setting:** HP-Nas-filter-Rule = “< permit or deny ACE >” |
Configuring RADIUS Server Support for Switch Services

Configuring and Using RADIUS-Assigned Access Control Lists

Configuring ACE Syntax in RADIUS Servers

The following syntax and operating information applies to ACLs configured in a RADIUS server.

ACE Syntax
(Standard Attribute-92)

Nas-filter-Rule ="< permit | deny > in <ip | ip-protocol-value > from any to
< any | ip-addr | ipv4-addr/mask > [ < tcp/udp-port | tcp/udp-port range > | icmp-type ] [cnt ]"

ACE Syntax
(Legacy VSA-61)

HP-Nas-filter-Rule="< permit | deny > in <ip | ip-protocol-value > from any to
< any | ip-addr | ipv4-addr/mask > [ < tcp/udp-port | tcp/udp-port range > | icmp-type ] [cnt ]"

Nas-filter-Rule =: Standard attribute for filtering inbound IPv4 traffic from an authenticated client. Refer also to table 6-4, “Nas-Filter-Rule Attribute Options” on page 6-16.

HP-Nas-filter-Rule =: Legacy HP VSA for filtering inbound IPv4 traffic from an authenticated client. Refer also to table 6-4, “Nas-Filter-Rule Attribute Options” on page 6-16.

"...": Must be used to enclose and identifies a complete permit or deny ACE syntax statement. For example: Nas-filter-Rule="deny in tcp from any to 0.0.0.0/0 23"

< permit | deny >: Specifies whether to forward or drop the identified IP traffic type from the authenticated client. (For information on explicitly permitting or denying all inbound IP traffic from an authenticated client, or for implicitly denying all such IP traffic not already permitted or denied, refer to “Configuration Notes” on page 6-22.)

in: Required keyword specifying that the ACL applies only to the traffic inbound from the authenticated client.

< ip | ip-protocol-value >: Options for specifying the type of traffic to filter.

ip: Applies the ACE to all IP traffic from the authenticated client.

ip-protocol-value: This option applies the ACE to the type of IP traffic specified by either a protocol number or by tcp, udp, icmp, or (for IPv4-only) igmp. The range of protocol numbers is 0-255. (Protocol numbers are defined in RFC 2780. For a complete listing, refer to “Protocol Registries” on the Web site of the Internet Assigned Numbers Authority at www.iana.com.) Some examples of protocol numbers include:

<table>
<thead>
<tr>
<th>Protocol Number</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ICMP</td>
</tr>
<tr>
<td>2</td>
<td>IGMP (IPv4 only)</td>
</tr>
<tr>
<td>6</td>
<td>TCP*IPv4 traffic only</td>
</tr>
<tr>
<td>17</td>
<td>UDP</td>
</tr>
</tbody>
</table>

from any: Required keywords specifying the (authenticated) client source. (Note that a RADIUS-assigned ACL assigned to a port filters only the inbound traffic having a source MAC address that matches the MAC address of the client whose authentication invoked the ACL assignment.)

to: Required destination keyword.
Any:
- Specifies any IPv4 destination address if one of the following is true:
  - The ACE uses the standard attribute (Nas-filter-Rule). For example:
    Nas-filter-Rule="permit in tcp from any to any 23"
    Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
    Nas-filter-Rule="deny in ip from any to any"
  - The HP-Nas-Filter-Rule VSA is used instead of the above option. For example, all of the following destinations are for IPv4 traffic:
    HP-Nas-filter-Rule="permit in tcp from any to any 23"
    HP-Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
    HP-Nas-filter-Rule="deny in ip from any to any"

<ipv4-addr> Specifies a single destination IPv4 address.
</ipv4-addr>/<mask>: Specifies a series of contiguous destination addresses or all destination addresses in a subnet. The <mask> is CIDR notation for the number of leftmost bits in a packet’s destination IPv4 address that must match the corresponding bits in the destination IPv4 address listed in the ACE. For example, a destination of 10.100.17.1/24 in the ACE means that a match occurs when an inbound packet (of the designated IPv4 type) from the authenticated client has a destination IPv4 address where the first three octets are 10.100.17. (The fourth octet is a wildcard, and can be any value up to 255.)

[tcp/udp-port|tcp/udp-port-range]: Optional TCP or UDP port specifier. Used when the ACE is intended to filter client TCP or UDP traffic with one or more specific TCP or UDP destination port numbers. You can specify port numbers as individual values and/or ranges. For example, the following ACE shows two ways to deny any UDP traffic from an authenticated client that has a DA of any address and a UDP destination port of 135, 137-139, or 445:

deny in udp from any to any 135, 137-139, 445
deny in 17 from any to any 135, 137-139, 445

[ icmp-type ]: Optional ICMP type specifier. This can be either a keyword or an ICMP type number. For a listing of numbers and types, refer to table 6-5, “ICMP Type Numbers and Keywords” on page 6-26.

[ cnt ]: Optional counter specifier for a RADIUS-assigned ACE. When used, the counter increments each time there is a “match” with the ACE. This option does not require that you configure the switch for RADIUS accounting.

Example Using the Standard Attribute (92) In an IPv4 ACL

The Standard attribute (92) filters IPv4 traffic inbound from the authenticated client. (Any IPv6 traffic inbound from the client is dropped.) This example illustrates configuring RADIUS-assigned IPv4 ACL support on FreeRADIUS using the standard attribute for two different client identification methods (username/password and MAC address).
Configuring RADIUS Server Support for Switch Services
Configuring and Using RADIUS-Assigned Access Control Lists

1. Enter the ACL standard attribute in the FreeRADIUS dictionary.rfc4849 file.

```
ATTRIBUTE       Nas-FILTER-Rule 92
```

2. Enter the switch IP address, NAS (Network Attached Server) type, and the key used in the FreeRADIUS clients.conf file. For example, if the switch IP address is 10.10.10.125 and the key ("secret") is “1234”, you would enter the following in the server’s clients.conf file:

```
client 10.10.10.125
nastype = other
secret = 1234
```

---

**Note:** The key configured in the switch and the secret configured in the RADIUS server supporting the switch must be identical. Refer to the chapter titled “RADIUS Authentication and Accounting” in the latest Access Security Guide for your switch.

---

Figure 6-3. Example of Switch Identity Information for a FreeRADIUS Application

3. For a given client username/password pair or MAC address, create an ACL by entering one or more ACEs in the FreeRADIUS “users” file. Remember that every ACL you create automatically includes an implicit deny in ip from any to any ACE. For example, suppose that you wanted to create identical ACL support for the following:

- a client having a username of “mobilE011” and a password of “run10kFast”
- a client having a MAC address of 08 E9 9C 4F 00 19

The ACL in this example must achieve the following:

- permit http (TCP port 80) traffic from the client to the device at 10.10.10.101
- deny http (TCP port 80) traffic from the client to all other devices
- permit all other traffic from the client to all other devices

To configure the above ACL, you would enter the username/password and ACE information shown in figure 6-4 into the FreeRADIUS “users” file.

Example of Configuring a RADIUS-assigned ACL Using the FreeRADIUS Application

This example illustrates one method for configuring RADIUS-assigned ACL support for two different client identification methods (username/password and MAC address). For information on how to configure this functionality on other RADIUS server types, refer to the documentation provided with the server.
1. Enter the HP vendor-specific ID and the ACL VSA in the FreeRADIUS dictionary file:

```
VENDOR          HP    11
BEGIN-VENDOR    HP
ATTRIBUTE       HP-IP-FILTER-RAW 61 STRING
END-VENDOR      HP
```

Note that if you were also using the RADIUS server to administer 802.1p (CoS) priority, you would also insert the ATTRIBUTE entries for these functions above the END-VENDOR entry.

Figure 6-4. Example of Configuring the VSA for RADIUS-assigned ACLs in a FreeRADIUS Server

2. Enter the switch IP address, NAS (Network Attached Server) type, and the key in the FreeRADIUS clients.conf file. For example, if the switch IP address is 10.10.10.125 and the key is “1234”, you would enter the following in the server’s clients.conf file:

```
client 10.10.18.12
nastype = other
secret = 1234
```

Note: The key configured in the switch and the secret configured in the RADIUS server supporting the switch must be identical. Refer to the chapter titled “RADIUS Authentication and Accounting” in the Access Security Guide for your switch.

Figure 6-5. Example of Configuring the Switch’s Identity Information in a FreeRADIUS Server

3. For a given client username/password pair or MAC address, create an ACL by entering one or more ACEs in the FreeRADIUS “users” file. Enter the ACEs in an order that promotes optimum traffic management and conservation of system resources, and remember that every ACL you create automatically includes an implicit deny in IP from any to any ACE. For example, suppose that you wanted to create identical ACL support for the following:
   - a client having a username of “mobile011” and a password of “run101112”
   - a client having a MAC address of 08 E9 9C 4F 00 19

The ACL in this example must achieve the following:
   - permit http (TCP port 80) traffic from the client to the device at 10.10.10.101
   - deny http (TCP port 80) traffic from the client to all other devices
   - permit all other traffic from the client to all other devices

To configure the above ACL, you would enter the username/password and ACE information shown in figure6-6 into the FreeRADIUS users file.
For syntax details on RADIUS-assigned ACLs, refer to the next section, “Format Details for ACEs Configured in a RADIUS-Assigned ACL”.

**Figure 6-6. Example of Configuring the FreeRADIUS Server To Support ACLs for the Indicated Clients**

**Format Details for ACEs Configured in a RADIUS-Assigned ACL**

Any instance of a RADIUS-assigned ACL is structured to filter authenticated client traffic as follows:

- Applies only to inbound client traffic on the switch port the authenticated client is using.
- Allows only the “any” source address (for any authenticated IP device connected to the port).
- Applies to all IP traffic from the authenticated client or to a specific type of IP traffic type from the client. Options include TCP, UDP, or any other type of IP traffic that is identified by an IP protocol number. (More information on protocol numbers is provided in the following ACL syntax description.) Has one of the following destination types:
  - A specific IP address
  - A contiguous series of IP address or an entire subnet
  - Any IP address
- Where the traffic type is either TCP or UDP, the ACE can optionally include one or more TCP or UDP port numbers.
Configuration Notes

Explicitly Permitting Any IP Traffic. Entering a `permit in ip from any to any` (permit any any) ACE in an ACL permits all IP traffic not previously permitted or denied by that ACL. Any ACEs listed after that point do not have any effect.

Explicitly Denying Any IP Traffic. Entering a `deny in ip from any to any` ACE in an ACL denies all IP traffic not previously permitted or denied by that ACL. Any ACEs listed after that point have no effect.

Implicitly Denying Any IP Traffic. For any packet being filtered by a static port ACL, there will always be a match. That is, any packet that does not have a match with an explicit permit or deny ACE in the list will match with the implicit `deny in ip from any to any` that is automatically implied at the end of the list. Thus, the ACL denies any IP packet it filters that does not match any explicitly configured ACE. If you want an ACL to permit any packets that are not explicitly denied, you must configure `permit in ip from any to any` as the last explicit ACE in the ACL. This `permit any any` only applies to an authenticated user. It pre-empts the implicit `deny in ip from any to any` ACE and permits packets not explicitly permitted or denied by earlier ACEs in the list.

Configuring the Switch To Support RADIUS-Assigned ACLs

An ACL configured in a RADIUS server is identified by the authentication credentials of the client or group of clients the ACL is designed to support. When a client authenticates with credentials associated with a particular ACL, the switch applies that ACL to the switch port the client is using. To enable the switch to forward a client’s credentials to the RADIUS server, you must first configure RADIUS operation and an authentication method on the switch.

1. Configure RADIUS operation on the switch:

   **Syntax:** `radius-server host <ip-address> key <key-string>`

   This command configures the IP address and encryption key of a RADIUS server. The server should be accessible to the switch and configured to support authentication requests from clients using the switch to access the network. For more on RADIUS configuration, refer to chapter 5, “RADIUS Authentication, Authorization, and Accounting”.

2. Configure RADIUS network accounting on the switch (optional). RADIUS network accounting is necessary to retrieve counter information if the `cnt` (counter) option is included in any of the ACEs configured on the RADIUS server.
Configuring RADIUS Server Support for Switch Services
Configuring and Using RADIUS-Assigned Access Control Lists

Syntax: aaa accounting network < start-stop | stop-only > radius

Note
Refer to the documentation provided with your RADIUS server for information on how the server receives and manages network accounting information, and how to perform any configuration steps necessary to enable the server to support network accounting data from the switch.

3. Configure an authentication method. Options include 802.1X, Web authentication, and MAC authentication. (You can configure 802.1X and either Web or MAC authentication to operate simultaneously on the same ports.)

802.1X Option:

Syntax: aaa port-access authenticator < port-list >
aaa authentication port-access chap-radius
aaa port-access authenticator active

These commands configure 802.1X port-based access control on the switch, and activates this feature on the specified ports. For more on 802.1X configuration and operation, refer to chapter 12, “Configuring Port-Based and User-Based Access Control (80.1X)” in this guide.

MAC Authentication Option:

Syntax: aaa port-access mac-based < port-list >

This command configures MAC authentication on the switch and activates this feature on the specified ports. For more on MAC authentication, refer to chapter 3, “Web and MAC Authentication”.

Web Authentication Option:

Syntax: aaa port-access web-based < port-list >

This command configures Web authentication on the switch and activates this feature on the specified ports. For more on Web authentication, refer to chapter 3, “Web and MAC Authentication”.
Configuring RADIUS Server Support for Switch Services
Configuring and Using RADIUS-Assigned Access Control Lists

Displaying the Current RADIUS-Assigned ACL Activity on the Switch

These commands output data indicating the current ACL activity imposed per-port by RADIUS server responses to client authentication.

**Syntax:** show access-list radius < port-list >

*For the specified ports, this command lists the explicit ACEs, switch port, and client MAC address for each ACL dynamically assigned by a RADIUS server as a response to client authentication. If cnt (counter) is included in an ACE, then the output includes the current number of inbound packet matches the switch has detected in the current session for that ACE.*

**Note:** If a client authenticates but the server does not return a RADIUS-assigned ACL to the client port, then the server does not have a valid ACL configured and assigned to that client’s authentication credentials.

For example, the following output shows that a RADIUS server has assigned an ACL to port B1 to filter inbound traffic from an authenticated client identified by a MAC address of 00-11-85-C6-54-7D.

```
HP Switch(config)# show access-list radius b1
Radius-configured Port-based ACL for Port B1, Client -- 001185C6547D
  deny in tcp from any to 10.30.248.184 23 cnt
    Packet Hit Counter : 1
  deny in tcp from any to 10.30.248.184 80 cnt
    Packet Hit Counter : 10
  permit in tcp from any to 10.30.248.184 7
  permit in udp from any to 10.30.248.184 7
  deny in tcp from any to 10.30.248.184 161 cnt
    Packet Hit Counter : 25
  deny in udp from any to 10.30.248.184 161 cnt
    Packet Hit Counter : 7
  permit in ip from any to any
```

Figure 6-7. Example Showing a RADIUS-assigned ACL Application to a Currently Active Client Session
Syntax: show port-access authenticator < port-list >

For ports, in <port-list> that are configured for authentication, this command indicates whether there are any RADIUS-assigned features active on the port(s). (Any ports in <port-list> that are not configured for authentication do not appear in this listing.)

Port: Port number of port configured for authentication.

Auth Clients: Number of authorized clients

Unauth Clients: Number of unauthorized clients

Untagged VLAN: VLAN IDs (VIDs) of the untagged VLANs currently supporting the authenticated connection.

Tagged VLANs: VLAN IDs (VIDs) of the tagged VLANs currently supporting the authenticated connection

Port CoS: Indicates the status of the current 802.1p priority setting for inbound traffic.

- No-override: Indicates that no RADIUS-assigned 802.1p priority is currently active on the indicated port. (For more on traffic prioritization for the switches covered in this guide, refer to the chapter titled “Quality of Service (QoS): Managing Bandwidth More Effectively”, in the Advanced Traffic Configuration Guide.)

- 0 - 7: Indicates that the displayed 802.1p priority has been assigned by a RADIUS server to inbound traffic on the indicated port for a currently active, authenticated client session. This assignment remains active until the session ends.

Kbps In Limit: Indicates the ingress rate-limit assigned by the RADIUS server to the port for traffic inbound from the authenticated client. If there is no ingress rate-limit assigned, then Not Set appears in this field.

RADIUS ACL: Indicates whether a RADIUS-assigned ACL is currently active on the port.

- Yes: An ACL has been assigned by a RADIUS server to inbound traffic on the indicated port for a currently active, authenticated client session. This assignment remains active until the session ends.

- No: There is no RADIUS-assigned ACL currently active on the indicated port.

Cntrl Dir: Directions in which flow of incoming and outgoing traffic is blocked on 802.1X-aware port that has not yet entered the authenticated state:

- Both: Incoming and outgoing traffic is blocked on port until authentication occurs.

- In: Only incoming traffic is blocked on port before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on the unauthenticated 802.1X-aware port.
Configuring RADIUS Server Support for Switch Services
Configuring and Using RADIUS-Assigned Access Control Lists

HP Switch(config)# show port-access authenticator 2-3

Port Access Authenticator Status

Port-access authenticator activated [No] : No
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

<table>
<thead>
<tr>
<th>Auth Port Clients</th>
<th>Unauth Clients</th>
<th>Untagged VLAN</th>
<th>Tagged VLANs</th>
<th>Port COS</th>
<th>Kbps In Limit</th>
<th>RADIUS Ctrl ACL</th>
<th>Dir</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>7</td>
<td>90</td>
<td>No</td>
<td>In</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>50</td>
<td>Yes</td>
<td>In</td>
</tr>
</tbody>
</table>

Figure 6-8. Example of Output Showing Current RADIUS-Assigned Features

ICMP Type Numbers and Keywords

Below are the possible optional ICMP type specifiers for the `icmp-type` parameter.

Table 6-5. ICMP Type Numbers and Keywords

<table>
<thead>
<tr>
<th>#</th>
<th>Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>echo reply</td>
</tr>
<tr>
<td>3</td>
<td>destination unreachable</td>
</tr>
<tr>
<td>4</td>
<td>source quench</td>
</tr>
<tr>
<td>5</td>
<td>redirect</td>
</tr>
<tr>
<td>8</td>
<td>echo request</td>
</tr>
<tr>
<td>9</td>
<td>router advertisement</td>
</tr>
<tr>
<td>10</td>
<td>router solicitation</td>
</tr>
<tr>
<td>11</td>
<td>time-to-live exceeded</td>
</tr>
<tr>
<td>12</td>
<td>IP header bad</td>
</tr>
<tr>
<td>13</td>
<td>timestamp request</td>
</tr>
<tr>
<td>14</td>
<td>timestamp reply</td>
</tr>
<tr>
<td>15</td>
<td>information request</td>
</tr>
<tr>
<td>16</td>
<td>information reply</td>
</tr>
<tr>
<td>17</td>
<td>address mask request</td>
</tr>
<tr>
<td>18</td>
<td>address mask reply</td>
</tr>
</tbody>
</table>
## Event Log Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE parsing error, permit/deny keyword <code>&lt;ace-#&gt;</code> client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies of a problem with the <code>permit/deny</code> keyword in the indicated ACE included in the access list for the indicated client on the indicated switch port.</td>
</tr>
<tr>
<td>Could not add ACL entry.</td>
<td></td>
</tr>
<tr>
<td>Could not create ACL entry.</td>
<td></td>
</tr>
<tr>
<td>Could not add ACL, client mac <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>, at max per-port ACL quantity.</td>
<td>Notifies that the ACL could not be added because the per-port ACL quantity would be exceeded.</td>
</tr>
<tr>
<td>ACE parsing error, IN keyword, <code>&lt;ace-#&gt;</code> client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies of a problem with the IN keyword in the indicated ACE of the access list for the indicated client on the indicated switch port.</td>
</tr>
<tr>
<td>ACE parsing error, protocol field, <code>&lt;ace-#&gt;</code> client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies of a problem with the protocol field in the indicated ACE of the access list for the indicated client on the indicated switch port.</td>
</tr>
<tr>
<td>ACE parsing error, FROM keyword, <code>&lt;ace-#&gt;</code> client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies of a problem with the FROM keyword in the indicated ACE of the access list for the indicated client on the indicated switch port.</td>
</tr>
<tr>
<td>ACE parsing error, ANY keyword, <code>&lt;ace-#&gt;</code> client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies of a problem with the ANY keyword in the indicated ACE of the access list for the indicated client on the indicated switch port.</td>
</tr>
<tr>
<td>ACE parsing error, TO keyword, <code>&lt;ace-#&gt;</code> client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies of a problem with the TO keyword in the indicated ACE of the access list for the indicated client on the indicated switch port.</td>
</tr>
<tr>
<td>ACE parsing error, destination IP, <code>&lt;ace-#&gt;</code> client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies of a problem with the destination IP field in the indicated ACE of the access list for the indicated client on the indicated switch port.</td>
</tr>
<tr>
<td>ACE parsing error, tcp/udp ports, <code>&lt;ace-#&gt;</code> client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies of a problem with the TCP/UDP port field in the indicated ACE of the access list for the indicated client on the indicated switch port.</td>
</tr>
<tr>
<td>Rule limit per ACL exceeded. <code>&lt;ace-#&gt;</code> client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies that an ACL has too many rules.</td>
</tr>
<tr>
<td>Duplicate mac. An ACL exists for client. Deauthenticating second. client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code>.</td>
<td>Notifies that an ACL for this mac on this port already exists.</td>
</tr>
</tbody>
</table>
Configuring RADIUS Server Support for Switch Services
Configuring and Using RADIUS-Assigned Access Control Lists

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Access-list entry length, client <code>&lt;mac-address&gt;</code> port <code>&lt;port-#&gt;</code></td>
<td>Notifies that the string configured for an ACE entry on the Radius server exceeds 80 characters.</td>
</tr>
<tr>
<td>Memory allocation failure for IDM ACL.</td>
<td>Notifies of a memory allocation failure for a RADIUS-assigned ACL assigned by a RADIUS server performing client authentication. (This message is used in IDM and non-IDM environments.)</td>
</tr>
</tbody>
</table>

Causes of Client Deauthentication Immediately After Authenticating

- ACE formatted incorrectly in the RADIUS server
  - “from”, “any”, or “to” keyword missing
  - An IP protocol number in the ACE exceeds 255.
  - An optional UDP or TCP port number is invalid, or a UDP/TCP port number is specified when the protocol is neither UDP or TCP.
- A RADIUS-assigned ACL limit has been exceeded.
  - An ACE in the ACL for a given authenticated client exceeds 80 characters.
  - The TCP/UDP port-range quantity of 14 per slot or port group has been exceeded.

Monitoring Shared Resources

Currently active, RADIUS-based authentication sessions (including HP IDM client sessions) using RADIUS-assigned ACLs share internal routing switch resources with several other features. The routing switch provides ample resources for all features. However, if the internal resources do become fully subscribed, new RADIUS-based sessions using RADIUS-assigned ACLs cannot be authenticated until the necessary resources are released from other applications.
Configuring Secure Shell (SSH)

Overview

The switches covered in this guide use Secure Shell version 2 (SSHv2) to provide remote access to management functions on the switches via encrypted paths between the switch and management station clients capable of SSH operation.

SSH provides Telnet-like functions but, unlike Telnet, SSH provides encrypted, authenticated transactions. The authentication types include:

- Client public-key authentication
- Switch SSH and user password authentication

Client Public Key Authentication (Login/Operator Level) with User Password Authentication (Enable/Manager Level). This option uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a stored public key can gain access to the switch. (The same private key can be stored on one or more clients.)
Configuring Secure Shell (SSH)

Overview

Figure 7-1. Client Public Key Authentication Model

Note

SSH in HP switches is based on the OpenSSH software toolkit. For more information on OpenSSH, visit www.openssh.com.

Switch SSH and User Password Authentication. This option is a subset of the client public-key authentication shown in figure 7-1. It occurs if the switch has SSH enabled but does not have login access (login public-key) configured to authenticate the client's key. As in figure 7-1, the switch authenticates itself to SSH clients. Users on SSH clients then authenticate themselves to the switch (login and/or enable levels) by providing passwords stored locally on the switch or on a TACACS+ or RADIUS server. However, the client does not use a key to authenticate itself to the switch.

Figure 7-2. Switch/User Authentication
Terminology

- **SSH Server**: An HP switch with SSH enabled.

- **Key Pair**: A pair of keys generated by the switch or an SSH client application. Each pair includes a public key, that can be read by anyone and a private key held internally in the switch or by a client.

- **PEM (Privacy Enhanced Mode)**: Refers to an ASCII-formatted client public-key that has been encoded for portability and efficiency. SSHv2 client public-keys are typically stored in the PEM format. See figure 7-3 for an example of PEM-encoded ASCII keys.

- **Private Key**: An internally generated key used in the authentication process. A private key generated by the switch is not accessible for viewing or copying. A private key generated by an SSH client application is typically stored in a file on the client device and, together with its public key counterpart, can be copied and stored on multiple devices.

- **Public Key**: An internally generated counterpart to a private key. A device's public key is used to authenticate the device to other devices.

- **Enable Level**: Manager privileges on the switch.

- **Login Level**: Operator privileges on the switch.

- **Local password or username**: A Manager-level or Operator-level password configured in the switch.

- **SSH Enabled**: (1) A public/private key pair has been generated on the switch (`generate ssh [dsa | rsa]`) and (2) SSH is enabled (`ip ssh`). (You can generate a key pair without enabling SSH, but you cannot enable SSH without first generating a key pair. See “2. Generating the Switch’s Public and Private Key Pair” on page 7-9 and “4. Enabling SSH on the Switch and Anticipating SSH Client Contact Behavior” on page 7-15.)
Prerequisite for Using SSH

Before using the switch as an SSH server, you must install a publicly or commercially available SSH client application on the computer(s) you use for management access to the switch. If you want client public-key authentication (page 7-1), then the client program must have the capability to generate or import keys.

Public Key Formats

Any client application you use for client public-key authentication with the switch must have the capability to export public keys. The switch can accept keys in the PEM-Encoded ASCII Format or in the Non-Encoded ASCII format.

![Figure 7-3. Example of Public Key in PEM-Encoded ASCII Format Common for SSHv2 Clients](image-url)
Steps for Configuring and Using SSH for Switch and Client Authentication

For two-way authentication between the switch and an SSH client, you must use the login (Operator) level.

Table 7-1. SSH Options

<table>
<thead>
<tr>
<th>Switch Access Level</th>
<th>Primary SSH Authentication</th>
<th>Authenticate Switch Public Key to SSH Clients?</th>
<th>Authenticate Client Public Key to the Switch?</th>
<th>Primary Switch Password Authentication</th>
<th>Secondary Switch Password Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator (Login) Level</td>
<td>ssh login rsa</td>
<td>Yes</td>
<td>Yes†</td>
<td>No†</td>
<td>local or none</td>
</tr>
<tr>
<td></td>
<td>ssh login Local</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ssh login TACACS</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>local or none</td>
</tr>
<tr>
<td></td>
<td>ssh login RADIUS</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>local or none</td>
</tr>
<tr>
<td>Manager (Enable) Level</td>
<td>ssh enable local</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ssh enable tacacs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>local or none</td>
</tr>
<tr>
<td></td>
<td>ssh enable radius</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>local or none</td>
</tr>
</tbody>
</table>

† For ssh login public-key, the switch uses client public-key authentication instead of the switch password options for primary authentication.

The general steps for configuring SSH include:

A. Client Preparation

1. Install an SSH client application on a management station you want to use for access to the switch. (Refer to the documentation provided with your SSH client application.)

2. Optional—If you want the switch to authenticate a client public-key on the client:
   a. Either generate a public/private key pair on the client computer (if your client application allows) or import a client key pair that you have generated using another SSH application.
   b. Copy the client public key into an ASCII file on a TFTP server accessible to the switch and download the client public key file to the switch. (The client public key file can hold up to 100 client keys.) This topic is covered under “To Create a Client-Public-Key Text File” on page 7-25.
B. Switch Preparation

1. Assign a login (Operator) and enable (Manager) password on the switch (page 7-9).

2. Generate a public/private key pair on the switch (page 7-9).
   You need to do this only once. The key remains in the switch even if you reset the switch to its factory-default configuration. (You can remove or replace this key pair, if necessary.)

3. Copy the switch’s public key to the SSH clients you want to access the switch (page 7-13).

4. Enable SSH on the switch (page 7-15).

5. Configure the primary and secondary authentication methods you want the switch to use. In all cases, the switch will use its host-public-key to authenticate itself when initiating an SSH session with a client.
   • SSH Login (Operator) options:
     – Option A:
       Primary: Local, TACACS+, or RADIUS password
       Secondary: Local password or none. If the primary option is local, the secondary option must be none.
     – Option B:
       Primary: Client public-key authentication (login public-key — page 7-24)
       Secondary: none
       Note that if you want the switch to perform client public-key authentication, you must configure the switch with Option B.
   • SSH Enable (Manager) options:
     Primary: Local, TACACS+, or RADIUS
     Secondary: Local password or none. If the primary option is local, the secondary option must be none.

6. Use your SSH client to access the switch using the switch’s IP address or DNS name (if allowed by your SSH client application). Refer to the documentation provided with the client application.
General Operating Rules and Notes

■ Public keys generated on an SSH client must be exportable to the switch. The switch can store 100 client key pairs.

■ The switch’s own public/private key pair and the (optional) client public key file are stored in the switch’s flash memory and are not affected by reboots or the `erase startup-config` command.

■ Once you generate a key pair on the switch you should avoid re-generating the key pair without a compelling reason. Otherwise, you will have to re-introduce the switch’s public key on all management stations (clients) you previously set up for SSH access to the switch. In some situations this can temporarily allow security breaches.

❖ With SSH running, the switch allows one console session and up to five other sessions (SSH and/or Telnet).
# Configuring Secure Shell (SSH)

## Configuring the Switch for SSH Operation

### SSH-Related Commands in This Section

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh</td>
</tr>
<tr>
<td>show crypto client-public-key [manager</td>
</tr>
<tr>
<td>show crypto host-public-key [babble</td>
</tr>
<tr>
<td>show authentication</td>
</tr>
<tr>
<td>crypto key &lt;generate</td>
</tr>
<tr>
<td>ip ssh</td>
</tr>
<tr>
<td>cipher &lt;cipher-type&gt;</td>
</tr>
<tr>
<td>filetransfer</td>
</tr>
<tr>
<td>ip-version</td>
</tr>
<tr>
<td>mac</td>
</tr>
<tr>
<td>port &lt;1 - 65535&gt;</td>
</tr>
<tr>
<td>timeout &lt;5 - 120&gt;</td>
</tr>
<tr>
<td>aaa authentication ssh</td>
</tr>
<tr>
<td>login &lt;local</td>
</tr>
<tr>
<td>enable &lt;tacacs</td>
</tr>
<tr>
<td>copy tftp pub-key-file &lt;tftp server IP&gt; &lt;public key file&gt; [append</td>
</tr>
<tr>
<td>clear crypto client-public-key [keylist-str]</td>
</tr>
<tr>
<td>ssh [user &lt;username</td>
</tr>
<tr>
<td>copy sftp ssh-client-key [user &lt;username</td>
</tr>
<tr>
<td>copy sftp ssh-client-known-hosts [user &lt;username</td>
</tr>
</tbody>
</table>
Configuring Secure Shell (SSH)
Configuring the Switch for SSH Operation

1. Assigning a Local Login (Operator) and Enable (Manager) Password

At a minimum, HP recommends that you always assign at least a Manager password to the switch. Otherwise, under some circumstances, anyone with Telnet, web, or serial port access could modify the switch’s configuration.

To Configure Local Passwords. You can configure both the Operator and Manager password with one command.

**Syntax:** password < manager | operator | all >

```
Switch(config)# password all
New password for Operator: ********
Please retype new password for Operator: ********
New password for Manager: *******
Please retype new password for Manager: *******
New password for Manager: *******
```

Figure 7-4. Example of Configuring Local Passwords

2. Generating the Switch’s Public and Private Key Pair

You must generate a public and private host key pair on the switch. The switch uses this key pair, along with a dynamically generated session key pair to negotiate an encryption method and session with an SSH client trying to connect to the switch.

The host key pair is stored in the switch’s flash memory, and only the public key in this pair is readable. The public key should be added to a "known hosts" file (for example, $HOME/.ssh/known_hosts on UNIX systems) on the SSH clients which should have access to the switch. Some SSH client applications automatically add the switch’s public key to a "known hosts" file. Other
SSH applications require you to manually create a known hosts file and place the switch’s public key in the file. (Refer to the documentation for your SSH client application.)

(The session key pair mentioned above is not visible on the switch. It is a temporary, internally generated pair used for a particular switch/client session, and then discarded.)

---

**Note**

When you generate a host key pair on the switch, the switch places the key pair in flash memory (and not in the running-config file). Also, the switch maintains the key pair across reboots, including power cycles. You should consider this key pair to be “permanent”; that is, avoid re-generating the key pair without a compelling reason. Otherwise, you will have to re-introduce the switch’s public key on all management stations you have set up for SSH access to the switch using the earlier pair.

Removing (zeroing) the switch’s public/private key pair renders the switch unable to engage in SSH operation and automatically disables IP SSH on the switch. (To verify whether SSH is enabled, execute `show ip ssh`.) However, any active SSH sessions will continue to run, unless explicitly terminated with the CLI 'kill' command.

---

**To Generate or Erase the Switch’s Public/Private Host Key Pair.**

Because the host key pair is stored in flash instead of the running-config file, it is not necessary to use `write memory` to save the key pair. Erasing the key pair automatically disables SSH.

**Syntax:**

```
crypto key generate <autourun-key [rsa] | cert [rsa] <keysizes> | ssh [dsa | rsa] bits <keysizes>>
```

Installs authentication files for ssh or https server, or for autorun.

- **autourun-key**

  Install RSA key for autorun. See “Configuring Autorun on the Switch” in Appendix A of the Management and Configuration Guide for more information.

- **cert**

  Install RSA key for https certificate. See “Configuring the Switch for SSL Operation” on page 8-6 in this guide for more information.
 ssh [dsa | rsa]  
  
  *Install host key for ssh server. Specify the key type as DSA or RSA.*  

bits <keysize>  
  
  *Specify the key size (in bits). See Table 7-2.*  

zeroize <ssh | cert | autorun [rsa]>  
  
  *Erases the switch's public/private key pair and disables SSH operation.*  

show crypto host-public-key  
  
  *Displays switch's public key. Displays the version 2 views of the key.*  

  See “SSH Client Public-Key Authentication” on page 2-19 in this guide for information about public keys saved in a configuration file.  

[ babble ]  
  
  *Displays hashes of the switch's public key in phonetic format.*  

(See “Displaying the Public Key” on page 7-14.)  

[ fingerprint ]  
  
  *Displays fingerprints of the switch's public key in hexadecimal format.*  

(See “Displaying the Public Key” on page 7-14.)  

For example, to generate and display a new key:
Conﬁguring Secure Shell (SSH)
Conﬁguring the Switch for SSH Operation

If you wish to compare the switch key to the key as stored in your client’s known-hosts ﬁle, the formatting and commands need not match.

Notes
“Zeroizing” the switch’s key automatically disables SSH (sets \texttt{ip ssh} to no). Thus, if you zeroize the key and then generate a new key, you must also re-enable SSH with the \texttt{ip ssh} command before the switch can resume SSH operation.

Conﬁguring Key Lengths
The \texttt{crypto key generate ssh} command allows you to specify the type and length of the generated host key. The size of the host key is platform-dependent as different switches have different amounts of processing power. The size is represented by the \texttt{<keysize>} parameter and has the values shown in Table \ref{table7-2}. The default value is used if \texttt{keysize} is not speciﬁed.

\begin{table}[h]
\centering
\caption{RSA/DSA Values for Various HP Networking Switches}
\begin{tabular}{|c|c|c|}
\hline
\textbf{Platform} & \textbf{Maximum RSA Key Size (in bits)} & \textbf{DSA Key Size (in bits)} \\
\hline
5400/3500/6200/8200/2910 & 1024, 2048, 3072 & 1024 \\
& Default: 2048 & \\
\hline
4200/2900/2810/2610/2510 & 1024, 2048 & 1024 \\
& Default: 2048 & \\
\hline
5300/2800/2400/2600 & 896 & 512 \\
\hline
\end{tabular}
\end{table}
3. Providing the Switch’s Public Key to Clients

When an SSH client contacts the switch for the first time, the client will challenge the connection unless you have already copied the key into the client’s "known host" file. Copying the switch’s key in this way reduces the chance that an unauthorized device can pose as the switch to learn your access passwords. The most secure way to acquire the switch’s public key for distribution to clients is to use a direct, serial connection between the switch and a management device (laptop, PC, or UNIX workstation), as described below.

The public key body follows the comments:

```
ssh-rsa AAAAB3NzaC1yc2EAAAAADAQABAAABAQCKzbhu89Lp5vmpuDwHMynUDNaBPPDltL9J8zcr4BLXi
k8G7VoMGqxJisLewYjFUVV8Oha8XCCGh4aVCur/H11PlenMGl1fu42oYDobmfgf/kJCK6U527rEUG
qc+1VjxebjRGA5j0Bs8R2xo2k5ty62ciMnDoEBcruoxd58dwzy7kU5hjQHSkubqgw88HYv7vmLtY0dPz
RHIRSoEezm5jFDhtF2EubuB9adA43bqgmKqci228EfioMKE9QwQCWLw2vUnXhفFhxYwo7CoTir4yJA
1lTSYFTdd0G/pD67VfToz9DeH0163Y19ukQQNXGE0LRK+8I1S2O33J7eb5
```

Figure 7-7. Example of a Correctly Formatted Public Key

With a direct serial connection from a management station to the switch:

1. Use a terminal application such as HyperTerminal to display the switch’s public key with the `show crypto host-public-key` command.

2. Bring up the SSH client’s "known host" file in a text editor such as Notepad as straight ASCII text, and copy the switch’s public key into the file.

3. Ensure that there are no changes or breaks in the text string. (A public key must be an unbroken ASCII string. Line breaks are not allowed Changes in the line breaks will corrupt the Key.) For example, if you are using Windows® Notepad, ensure that **Word Wrap** (in the **Edit** menu) is disabled, and that the key text appears on a single line.
4. Add any data required by your SSH client application. For example, before saving the key to an SSH client’s "known hosts" file you may have to insert the switch’s IP address:

![Figure 7-8. Example of a Switch Public Key Edited To Include the Switch’s IP Address](image)

For more on this topic, refer to the documentation provided with your SSH client application.

**Displaying the Public Key.** The switch provides three options for displaying its public key. This is helpful if you need to visually verify that the public key the switch is using for authenticating itself to a client matches the copy of this key in the client’s "known hosts" file:

- **Non-encoded ASCII numeric string:** Requires a client ability to display the keys in the "known hosts" file in the ASCII format. This method is tedious and error-prone due to the length of the keys. (See figure 7-7 on page 7-13.)

- **Phonetic hash:** Outputs the key as a relatively short series of alphabetic character groups. Requires a client ability to convert the key to this format.

- **Hexadecimal hash:** Outputs the key as a relatively short series of hexadecimal numbers. Requires a parallel client ability.

For example, on the switch, you would generate the phonetic and hexadecimal versions of the switch’s public key in figure 7-7 as follows:

```
Switch(config)# show crypto host-public-key babble
1024 xUEp=neyrTzyz=ecFe=heMNaVx=TVzhFpuoR=dumSc=jkyz=m8xk
host_ssh2.pub
```

```
Switch(config)# show crypto host-public-key fingerprint
```

![Figure 7-9. Examples of Visual Phonetic and Hexadecimal Conversions of the Switch’s Public Key](image)
The two commands shown in figure 7-9 convert the displayed format of the switch's (host) public key for easier visual comparison of the switch's public key to a copy of the key in a client's “known host” file. The switch has only one RSA host key. The 'babble' and 'fingerprint' options produce two hashes for the key—one that corresponds to the challenge hash you will see if connecting with a v1 client, and the other corresponding to the hash you will see if connecting with a v2 client. These hashes do not correspond to different keys, but differ only because of the way v1 and v2 clients compute the hash of the same RSA key. The switch always uses ASCII version (without babble or fingerprint conversion) of its public key for file storage and default display format.

4. Enabling SSH on the Switch and Anticipating SSH Client Contact Behavior

The `ip ssh` command enables or disables SSH on the switch and modifies parameters the switch uses for transactions with clients. After you enable SSH, the switch can authenticate itself to SSH clients.

Before enabling SSH on the switch you must generate the switch's public/private key pair. If you have not already done so, refer to “2. Generating the Switch's Public and Private Key Pair” on page 7-9.

When configured for SSH, the switch uses its host public-key to authenticate itself to SSH clients. If you also want SSH clients to authenticate themselves to the switch you must configure SSH on the switch for client public-key authentication at the login (Operator) level. To enhance security, you should also configure local, TACACS+, or RADIUS authentication at the enable (Manager) level.

Refer to “5. Configuring the Switch for SSH Authentication” on page 7-20.

**SSH Client Contact Behavior.** At the first contact between the switch and an SSH client, if the switch's public key has not been copied into the client, then the client's first connection to the switch will question the connection and, for security reasons, provide the option of accepting or refusing. If it is safe to assume that an unauthorized device is not using the switch's IP address in an attempt to gain access to the client's data or network, the connection can be accepted. (As a more secure alternative, the client can be directly connected to the switch's serial port to download the switch's public key into the client. See the following Note.)
Configuring Secure Shell (SSH)
Configuring the Switch for SSH Operation

Note
When an SSH client connects to the switch for the first time, it is possible for a “man-in-the-middle” attack; that is, for an unauthorized device to pose undetected as the switch, and learn the usernames and passwords controlling access to the switch. This possibility can be removed by directly connecting the management station to the switch’s serial port, using a `show` command to display the switch’s public key, and copying the key from the display into a file. This requires a knowledge of where the client stores public keys, plus the knowledge of what key editing and file format might be required by the client application. However, if the first contact attempt between a client and the switch does not pose a security problem, this is unnecessary.

To enable SSH on the switch.
1. Generate a public/private key pair if you have not already done so. (Refer to “2. Generating the Switch’s Public and Private Key Pair” on page 7-9.)
2. Execute the `ip ssh` command.

To disable SSH on the switch, do either of the following:
- Execute `no ip ssh`.
- Zeroize the switch’s existing key pair. (page 7-10).
Configuring Secure Shell (SSH)
Configuring the Switch for SSH Operation

**Syntax:**

```
[no] ip ssh
```

Enables or disables SSH on the switch.

```
[cipher <cipher-type>]
```

Specify a cipher type to use for connection.

Valid types are:

- `aes128-cbc`
- `3des-cbc`
- `aes192-cbc`
- `aes256-cbc`
- `rijndael-cbc@lysator.liu.se`
- `aes128-ctr`
- `aes192-ctr`
- `aes256-ctr`

Default: All cipher types are available.

Use the **no** form of the command to disable a cipher type.

```
[filetransfer]
```

Enable/disable secure file transfer capability. SCP and SFTP secure file transfer will not function unless SSH is also enabled.

```
[ip-version <4|6|4or6>]
```

Select the IP mode to run in. The mode “ip-version 4” only accepts connections from IPv4 clients. The mode “ip-version 6” only accepts connections from IPv6 clients. The mode “ip-version 4or6” accepts connections from both IPv4 and IPv6 clients.

Default: ip-version 4or6
Configuring Secure Shell (SSH)
Configuring the Switch for SSH Operation

[mac <mac-type>]

Allows configuration of the set of MACs that can be selected.
Valid types are:
- hmac-md5
- hmac-sha1
- hmac-sha1-96
- hmac-md5-96

Default: All MAC types are available.

Use the no form of the command to disable a MAC type.

[port <1-65535 | default >]

The TCP port number for SSH connections (default: 22).
Important: See “Note on Port Number” on page 7-18.

[timeout <5 - 120 >]

Sets the maximum length of time (in seconds) allowed for
initial protocol negotiation and authentication. Default: 120 seconds

Note on Port Number

HP Networking recommends using the default TCP port number (22). However, you can use ip ssh port to specify any TCP port for SSH connections except those reserved for other purposes. Examples of reserved IP ports are 23 (Telnet) and 80 (http). Some other reserved TCP ports on the switch are 49, 80, 1506, and 1513.
Configuring Secure Shell (SSH)
Configuring the Switch for SSH Operation

Figure 7-10. Example of Enabling IP SSH and Displaying the SSH Configuration

```
HP Switch(config) ip ssh
HP Switch(config)# show ip ssh
SSH Enabled : Yes
TCP Port Number : 22
IP Version : IPv4 or IPv6
Host Key Type : RSA
Host Key Size : 1024
Ciphers : aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc,
          rijndael-cbc@lysator.liu.se, aes128-ctr, aes192-ctr, aes256-ctr
MACs : hmac-md5, hmac-shal, hmac-shal-96, hmac-md5-96

<table>
<thead>
<tr>
<th>Ses Type</th>
<th>Source IP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 console</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 telnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 ssh</td>
<td>12.255.255.255</td>
<td></td>
</tr>
<tr>
<td>4 inactive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 inactive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 inactive</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

With SSH running, the switch allows one console session and up to five other sessions (SSH and/or Telnet). WebAgent sessions are also allowed, but do not appear in the `show ip ssh` listing.

Protect your private key file from access by anyone other than yourself. If someone can access your private key file, they can then penetrate SSH security on the switch by appearing to be you.

SSH does not protect the switch from unauthorized access via the WebAgent, Telnet, SNMP, or the serial port. While WebAgent and Telnet access can be restricted by the use of passwords local to the switch, if you are unsure of the security this provides, you may want to disable web-based and/or Telnet access (no web-management and no telnet). If you need to increase SNMP security, you should use SNMP version 3 only. If you need to increase the security of your web interface see the section on SSL. Another security measure is to use the Authorized IP Managers feature described in the switch’s Management and Configuration Guide. To protect against unauthorized access to the serial port (and the Clear button, which removes local password protection), keep physical access to the switch restricted to authorized personnel.
5. Configuring the Switch for SSH Authentication

Note that all methods in this section result in authentication of the switch's public key by an SSH client. However, only Option B, below results in the switch also authenticating the client's public key. Also, for a more detailed discussion of the topics in this section, refer to “Further Information on SSH Client Public-Key Authentication” on page 7-24.

**Note**

HP Networking recommends that you always assign a Manager-Level (enable) password to the switch. Without this level of protection, any user with Telnet, web, or serial port access to the switch can change the switch’s configuration. Also, if you configure only an Operator password, entering the Operator password through telnet, web, ssh or serial port access enables full manager privileges. See “1. Assigning a Local Login (Operator) and Enable (Manager) Password” on page 7-9.

**Option A: Configuring SSH Access for Password-Only SSH Authentication.** When configured with this option, the switch uses its public key to authenticate itself to a client, but uses only passwords for client authentication.

**Syntax:**

```
aaa authentication ssh login < local | tacacs | radius>[< local | none >]
```

Configures a password method for the primary and secondary login (Operator) access. If you do not specify an optional secondary method, it defaults to none. If the primary method is local, the secondary method must be none.

```
aaa authentication ssh enable < local | tacacs | radius>[< local | none >]
```

Configures a password method for the primary and secondary enable (Manager) access. If you do not specify an optional secondary method, it defaults to none. If the primary method is local, the secondary method must be none.

**Option B: Configuring the Switch for Client Public-Key SSH Authentication.** If configured with this option, the switch uses its public key to authenticate itself to a client, but the client must also provide a client public-key for the switch to authenticate. This option requires the additional step of copying a client public-key file from a TFTP or SFTP server into the switch. This means that before you can use this option, you must:

1. Create a key pair on an SSH client.

```
2. Copy the client’s public key into a public-key file (which can contain up to ten client public-keys).

3. Copy the public-key file into a TFTP or SFTP server accessible to the switch and download the file to the switch.

(For more on these topics, refer to “Further Information on SSH Client Public-Key Authentication” on page 7-24.)

With steps 1 - 3, above, completed and SSH properly configured on the switch, if an SSH client contacts the switch, login authentication automatically occurs first, using the switch and client public-keys. After the client gains login access, the switch controls client access to the manager level by requiring the passwords configured earlier by the \texttt{aaa authentication ssh enable} command.

\textbf{Syntax:} \texttt{copy tftp pub-key-file < ip-address > < filename >}

\textit{Copies a public key file into the switch.}

\texttt{aaa authentication ssh login public-key}

\textit{Configures the switch to authenticate a client public-key at the login level with an optional secondary password method (default: none).}

\textbf{Syntax:} \texttt{aaa authentication ssh enable < local | tacacs | radius > < local | none >}

\textit{Configures a password method for the primary and secondary enable (Manager) access. If you do not specify an optional secondary method, it defaults to none.}

\textit{If the primary access method is local, you can only specify none for a secondary access method.}

\textbf{Note:} The configuration of SSH clients’ public keys is stored in flash memory on the switch. You also can save SSH client public-key configurations to a configuration file by entering the following commands:

\texttt{include-credentials}

\texttt{write memory}

\textit{For more information about saving security credentials to a configuration file, see “Saving Security Credentials in a Config File” on page 2-10 in this guide.}
Configuring Secure Shell (SSH)
Configuring the Switch for SSH Operation

For example, assume that you have a client public-key file named Client-Keys.pub (on a TFTP server at 10.33.18.117) ready for downloading to the switch. For SSH access to the switch you want to allow only clients having a private key that matches a public key found in Client-Keys.pub. For Manager-level (enable) access for successful SSH clients you want to use TACACS+ for primary password authentication and **local** for secondary password authentication, with a Manager username of "leader" and a password of "m0ns00n". To set up this operation you would configure the switch in a manner similar to the following:

```
HP Switch(config)# password manager user-name leader
New password for Manager: ********
Please retype new password for Manager: ********
HP Switch(config)# aaa authentication ssh login public-key none
HP Switch(config)# aaa authentication ssh enable tacacs local
HP Switch(config)# coy tftp pub-key-file 10.33.18.117
HP Switch(config)# write memory
```

Figure 7-11. Configuring for SSH Access Requiring a Client Public-Key Match and Manager Passwords

Figure 7-12 shows how to check the results of the above commands.
6. Use an SSH Client To Access the Switch

Test the SSH configuration on the switch to ensure that you have achieved the level of SSH operation you want for the switch. If you have problems, refer to “RADIUS-Related Problems” in the Troubleshooting chapter of the Management and Configuration Guide for your switch.
Further Information on SSH Client Public-Key Authentication

The section titled “5. Configuring the Switch for SSH Authentication” on page 7-20 lists the steps for configuring SSH authentication on the switch. However, if you are new to SSH or need more details on client public-key authentication, this section may be helpful.

When configured for SSH operation, the switch automatically attempts to use its own host public-key to authenticate itself to SSH clients. To provide the optional, opposite service—client public-key authentication to the switch—you can configure the switch to store up to ten public keys for authenticating clients. This requires storing an ASCII version of each client’s public key (without babble conversion, or fingerprint conversion) in a client public-key file that you create and TFTP-copy to the switch. In this case, only clients that have a private key corresponding to one of the stored public keys can gain access to the switch using SSH. That is, if you use this feature, only the clients whose public keys are in the client public-key file you store on the switch will have SSH access to the switch over the network. If you do not allow secondary SSH login (Operator) access via local password, then the switch will refuse other SSH clients.

SSH clients that support client public-key authentication normally provide a utility to generate a key pair. The private key is usually stored in a password-protected file on the local host; the public key is stored in another file and is not protected.

(Note that even without using client public-key authentication, you can still require authentication from whoever attempts to access the switch from an SSH client—by employing the local username/password, TACACS+, or RADIUS features. Refer to “5. Configuring the Switch for SSH Authentication” on page 7-20.)

If you enable client public-key authentication, the following events occur when a client tries to access the switch using SSH:

1. The client sends its public key to the switch with a request for authentication.

2. The switch compares the client’s public key to those stored in the switch’s client-public-key file. (As a prerequisite, you must use the switch’s `copy tftp` command to download this file to flash.)
3. If there is not a match, and you have not configured the switch to accept a login password as a secondary authentication method, the switch denies SSH access to the client.

4. If there is a match, the switch:
   a. Generates a random sequence of bytes.
   b. Uses the client’s public key to encrypt this sequence.
   c. Sends these encrypted bytes to the client.

5. The client uses its private key to decrypt the byte sequence.

6. The client then:
   a. Combines the decrypted byte sequence with specific session data.
   b. Uses a secure hash algorithm to create a hash version of this information.
   c. Returns the hash version to the switch.

7. The switch computes its own hash version of the data from step 6 and compares it to the client’s hash version. If they match, then the client is authenticated. Otherwise, the client is denied access.

Using client public-key authentication requires these steps:

1. Generate a public/private key pair for each client you want to have SSH access to the switch. This can be a separate key for each client or the same key copied to several clients.

2. Copy the public key for each client into a client-public-key text file.

3. Use `copy tftp` to copy the client-public-key file into the switch. Note that the switch can hold 100 keys. The new key is appended to the client public-key file.

4. Use the `aaa authentication ssh` command to enable client public-key authentication.

To Create a Client-Public-Key Text File. These steps describe how to copy client-public-keys into the switch for challenge-response authentication, and require an understanding of how to use your SSH client application.
Configuring Secure Shell (SSH)
Further Information on SSH Client Public-Key Authentication

Figure 7-13. Example of a Client Public Key

Notes
Comments in public key files, such as smith@support/cairns.com in figure 7-13, may appear in a SSH client application’s generated public key. While such comments may help to distinguish one key from another, they do not pose any restriction on the use of a key by multiple clients and/or users.

Public key illustrations such as the key shown in figure 7-13 usually include line breaks as a method for showing the whole key. However, in practice, line breaks in a public key will cause errors resulting in authentication failure.

1. Use your SSH client application to create a public/private key pair. Refer to the documentation provided with your SSH client application for details. The switch supports the following client-public-key properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Supported Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Format</td>
<td>ASCII</td>
<td>See figure 7-7 on page 7-13. The key must be one unbroken ASCII string. If you add more than one client-public-key to a file, terminate each key (except the last one) with a &lt;CR&gt;&lt;LF&gt;. Spaces are allowed within the key to delimit the key’s components. Note that, unlike the use of the switch’s public key in an SSH client application, the format of a client-public-key used by the switch does not include the client’s IP address.</td>
</tr>
<tr>
<td>Key Type</td>
<td>RSA or DSA</td>
<td>You can choose either RSA or DSA key types when using the crypto key generate ssh command. The cert and autorun parameters only use RSA key types.</td>
</tr>
<tr>
<td>Maximum Supported Public Key Length</td>
<td>3072 bits</td>
<td>Shorter key lengths allow faster operation, but also mean diminished security.</td>
</tr>
<tr>
<td>Maximum Host Key Sizes In Bits</td>
<td>RSA: 1024, 2048, 3072 DSA: 1024</td>
<td>Includes the bit size, public index, modulus, any comments, &lt;CR&gt;, &lt;LF&gt;, and all blank spaces. If necessary, you can use an editor application to verify the size of a key. For example, placing a client-public-key into a Word for Windows text file and clicking on File I Properties I Statistics, lets you view the number of characters in the file, including spaces.</td>
</tr>
</tbody>
</table>
2. Copy the client’s public key into a text file (filename.txt). (For example, you can use the Notepad editor included with the Microsoft® Windows® software. If you want several clients to use client public-key authentication, copy a public key for each of these clients (up to ten) into the file. Each key should be separated from the preceding key by a <CR><LF>.

3. Copy the client-public-key file into a TFTP server accessible to the switch.

Copying a client-public-key into the switch requires the following:

- One or more client-generated public keys. Refer to the documentation provided with your SSH client application.
- A copy of each client public key (up to ten) stored in a single text file or individually on a TFTP server to which the switch has access. Terminate all client public-keys in the file except the last one with a <CR><LF>.

**Note on Public Keys**

The actual content of a public key entry in a public key file is determined by the SSH client application generating the key. (Although you can manually add or edit any comments the client application adds to the end of the key, such as the smith@support.cairns.com at the end of the key in figure 7-13.)

**Syntax:**

```
copy <tftp | sftp> pub-key-file <ip-address> <filename> [<append | manager | operator>]
```

Copies a public key file from a TFTP server into flash memory in the switch.

- The append option adds the key(s) for operator access.
- The manager option replaces the key(s) for manager access; follow with the ‘append’ option to add the key(s).
- The operator option replaces the key(s) for operator access (default); follow with the ‘append’ option to add the key(s).

```
show crypto client-public-key [manager | operator] [keylist-str] [babble | fingerprint]
```

Displays the client public key(s) in the switch’s current client-public-key file.

See “SSH Client Public-Key Authentication” on page 2-19 in this guide for information about public keys saved in a configuration file.
Configuring Secure Shell (SSH)
Further Information on SSH Client Public-Key Authentication

The **babble** option converts the key data to phonetic hashes that are easier for visual comparisons.

The **fingerprint** option converts the key data to hexadecimal hashes that are for the same purpose.

The **keylist-str** selects keys to display (comma-delimited list).

The **manager** option allows you to select manager public keys.

The **operator** option allows you to select operator public keys.

---

**Note**

The `copy usb pub-key file` command can also be used as a method for copying a public key file to the switch. SFTP can also be used as a method for copying a public key file to the switch.

For example, if you wanted to copy a client public-key file named `clientkeys.txt` from a TFTP server at 10.38.252.195 and then display the file contents:

```
HP Switch(config)# copy tftp pub-key-file 10.38.252.195 Clientkeys.txt
HP Switch(config)# show crypto client-public-key
```

```
Key Index Number
0: "Maden name [1024-bit rsa, Jamie_wilson@Jamiewilson, Thu Nov 07 2002 21:25:41 21] ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAAAg0C9cOvfqx11UFEc6SuLa4U1EFzn1h0qmP291Dwx61\1R/100UmActrFUOD11E14HQIN/XVZH/kItRdD6o5exFX/S10toRaFYzi9UjK80dBl1gVBCBZ1YVXJCVwlqAdqbaEX3d/Na?S2zArLCHFs1ZhnCVQTZDOC-AB1fr1ou== l,"[768-bit rsa, Jamie_wilson@Jamiewilson, Mon Dec 16 2002 23:01:51]" ssh-rsa AAAAB3NzaC1yo2EAAADAQABAAAYQD0tmza3ZJBgeuFJNOiXI3bfooPKZ09KBPQoCENvK7NKf9HOX vmmfr3EpufgIvlsE66n8FDu7U/B2tXI13OLFOtXCIvNCLN0/Do5AuEvmEnclCu/LgAH9daM=
```

**Figure 7-14. Example of Copying and Displaying a Client Public-Key File Containing Two Different Client Public Keys for the Same Client**

**Replacing or Clearing the Public Key File.** The client public-key file remains in the switch’s flash memory even if you erase the startup-config file, reset the switch, or reboot the switch.
You can remove the existing client public-key file or specific keys by executing the `clear crypto client-public-key` command. This clears the public keys from both management modules. The module that is not active must be in standby mode.

**Syntax:** clear crypto client-public-key  
*Deletes the client-public-key file from the switch.*

**Syntax:** clear crypto client-public-key 3  
*Deletes the entry with an index of 3 from the client-public-key file on the switch.*

**Enabling Client Public-Key Authentication.** After you TFTP a client-public-key file into the switch (described above), you can configure the switch to allow the following:

- If an SSH client’s public key matches the switch’s client-public-key file, allow that client access to the switch. If there is not a public-key match, then deny access to that client.

**Syntax:** aaa authentication ssh login public-key none  
*Allows SSH client access only if the switch detects a match between the client’s public key and an entry in the client-public-key file most recently copied into the switch.*

---

**Caution**

To enable client public-key authentication to block SSH clients whose public keys are not in the client-public-key file copied into the switch, you must configure the Login Secondary as `none`. Otherwise, the switch allows such clients to attempt access using the switch’s Operator password.

---

**SSH Client and Secure Sessions**

SSH Client provides a method for establishing a secure session from one HP switch to another. In addition to providing secure sessions, SFTP is enhanced to allow bidirectional secure copying of files between a switch and an SFTP
server, initiated from the switch with the copy command. The SFTP server
can be another switch or a workstation/server with a running SSH server that
supports SFTP.

Each switch with the SSH Client feature will have a known hosts file that can
contain the public key from switches and servers that have been determined
to be genuine. New public keys can be added to the known hosts file when
new SSH servers are contacted, up to a maximum of 100 entries (if memory
allows). The known hosts file can also be copied to another switch or to a
server where it can be edited.

Note
You must be in manager context to use this SSH and SFTP feature.

Opening a Secure Session to an HP Switch
To initiate an SSH client session to another network device, use the following
command, executed in the manager context.

Syntax:  

\[ssh \{user \langle\text{username} | \text{username}@\rangle\} <\text{hostname} | \text{IPv4} | \text{IPv6}> [port \langle1-65535\rangle]\]

Enables an SSH client to open a secure session to an HP switch. Opening secure sessions to devices other than HP
switches is not supported.

\[\{user \langle\text{username} | \text{username}@\rangle\}\]: Optional; the username on
the destination (remote) system. Usernames for Operator
and Manager must be configured.

If \langle\text{username}@\rangle \text{is specified, enter the remote system information of either hostname, IPv4 address, or IPv6 address.}

If no \text{username} is configured, the \text{username} of the current
login is used. There will be a prompt for a password if
needed.

\text{hostname}: Hostname of the remote system.

\text{IPv4}: IPv4 address of the remote system.

\text{IPv6}: IPv6 address of the remote system.

\[\text{port} \langle1-65535\rangle\]: The TCP port running the SSH server on
the remote system. If no port number is specified, the
default port 22 is used.

Default: Port 22
Operating Notes

- The SSH server may challenge the client to authenticate itself depending on the authentication methods configured on the destination SSH server. The client first tries the “none” method of authentication; if that is unsuccessful, it examines the list of supported authentication methods from the server, if provided. If the server does not provide such a list, all methods of authentication will be tried in the following order until the session is successfully opened or rejected by the server:
  - Authentication Method “publickey”, if a private key has been loaded onto the switch.
  - Authentication method “password”.
- During “public-key” authentication, the client must use its private key to authenticate itself to the server. There can be only one key pair on the switch for the manager.
- The private key should be passphrase protected for highest security; the user is prompted to enter the passphrase.
- The private key can be configured by copying it to the SSH client switch (using the `copy` command).
- If the public-key authentication fails or the client has not been configured with a key pair, the “password” method of authentication is used and the user is prompted for a password.
- Successful TACACS or RADIUS logins will give the user either operator or manager privileges. This is important if there are chained SSH sessions.

Copying Client Key Files

Only one ssh client key for authenticating the manager is allowed on a switch. The `copy` command allows you to copy the client key files using `sftp`, `tftp`, and `usb` or `xmodem`, allowing encryption and authentication through SSH. There is no way to generate the private key on the switch; it must be copied onto the switch.
To load the client’s private key onto the switch, use one of these commands.

**Syntax:**
```plaintext
copy sftp ssh-client-key [user <username> | <username@>] <hostname | IPv4 | IPv6> <private-key-filename> [port <tcp-port-num>]
copy tftp ssh-client-key <hostname | IPv4 | IPv6> <private-key-filename>
copy usb ssh-client-key <private-key-filename>
copy xmodem ssh-client-key
```

Copies the client key file `<private-key-filename>` onto the switch.

- **ssh-client-key:** The client key file being copied to the switch. The file must contain an RSA or DSA key.
- **[user <username | username@>]:** Optional; there must be configured usernames for Operator and Manager.
  - If no username is specified, the client’s current username is used. There will be a prompt for a password if needed.
- **hostname:** Specifies the hostname of the SFTP or TFTP server.
- **IPv4:** Specifies the SFTP or TFTP server’s IPv4 address.
- **IPv6:** Specifies the SFTP or TFTP server’s IPv6 address.
- **<private-key-filename>:** The remote filename containing the key.
- **[port <tcp-port-num>]:** TCP port of the SSH server on the remote system.

The copied private key is stored in the ssh directory of the switch’s file system and is persistent across switch reboots. After the initial copying is complete, the client key can be overwritten by repeating the `copy` command. No verification of the validity of the key is done when executing the copy command.
Configuring Secure Shell (SSH)

SSH Client and Secure Sessions

Copying the SSH-Client-Known-Hosts File

Replacing or Appending the SSH-Client-Known-Hosts File

There is one SSH client known hosts file per switch, stored in the ssh directory of the switch’s file system. The SSH client known hosts file can be overwritten or appended using the commands below. If the file already exists at that location, you will be prompted for confirmation before overwriting the existing file:

Warning: The existing known hosts file will be overwritten, continue [y/n] ?

Syntax:

copy sftp ssh-client-known-hosts [user <username> | <username@>] <hostname | IPv4 | IPv6> <filename> [append]
copy tftp ssh-client-known-hosts <hostname | IPv4 | IPv6> <filename> [append]
copy usb ssh-client-known-hosts <filename> [append]
copy xmodem ssh-client-known-hosts [append]

Copies the SSH client known hosts file to the switch.

ssh-client-known-hosts: The known hosts file.

[user <username | username@>]: Optional; there must be configured usernames for Operator and Manager.

If no username is specified, the client’s current username is used. There will be a prompt for a password if needed.

hostname: Specifies the hostname of the TFTP server.

IPv4: Specifies the TFTP server’s IPv4 address.

IPv6: Specifies the TFTP server’s IPv6 address.

<filename>: The remote filename containing the key.

[append]: Append hosts to the existing ssh-client-known-hosts file.
Default: Replace the existing known hosts file.
Copying the SSH Client Known Hosts File to Another Location

The SSH client known hosts file can be copied to a location on a remote device using the commands below. If the file already exists on the remote device, you are prompted for confirmation before overwriting the file:

Warning: The remote file will be overwritten, continue [y/n] ?

Syntax:

```
copy ssh-client-known-hosts sftp [user <username> | <username@>] <hostname | IPv4 | IPv6> <filename>
copy ssh-client-known-hosts tftp <hostname | IPv4 | IPv6> <filename>
copy ssh-client-known-hosts <filename> usb

copy ssh-client-known-hosts xmodem
```

Copies the SSH client known hosts file to another location.

- **ssh-client-known-hosts**: The known hosts file.
- **[user <username | username@>]**: Optional; there must be configured usernames for Operator and Manager.
  
  If no **username** is specified, the client's current **username** is used. There will be a prompt for a password if needed.

- **hostname**: Specifies the hostname of the TFTP server.
- **IPv4**: Specifies the TFTP server's IPv4 address.
- **IPv6**: Specifies the TFTP server's IPv6 address.
- **<filename>**: The remote filename containing the key.
Copying the Host Public Key

The following `copy` commands can be used to manage public keys in a known hosts file. The public key can only be copied from the switch to a server or other media, not to another switch.

**Syntax:**

- `copy ssh-server-pub-key sftp [user <username> | <username@>] <hostname | IPv4 | IPv6> <filename>`
- `copy ssh-server-pub-key tftp <hostname | IPv4 | IPv6> <filename>`
- `copy ssh-server-pub-key usb`
- `copy ssh-server-pub-key xmodem`

Copies the switch’s SSH server public key to a server or other media.

- `[user <username | username@>]`: Optional; there must be configured usernames for Operator and Manager.
- If no `username` is specified, the client’s current `username` is used. There will be a prompt for a password if needed.
- `hostname`: Specifies the hostname of the TFTP server.
- `IPv4`: Specifies the TFTP server’s IPv4 address.
- `IPv6`: Specifies the TFTP server’s IPv6 address.
- `<filename>`: The name of the file to be copied.

Removing the SSH Client Key Pair

To remove the SSH client key pair file, use this command.

**Syntax:**

- `crypto key zeroize ssh-client-key`

Deletes the SSH client key pair.

You will be prompted for confirmation with the message:

```
Warning: The manager key pair will be deleted, continue [y/n] ?
```
Removing the SSH Client Known Hosts File

To remove the SSH client known hosts file, use this command.

**Syntax:** crypto key zeroize ssh-client-known-hosts

*Deletes the SSH client known hosts file.*

You will be prompted with a message:

```
Warning: The SSH client known hosts file will be deleted, continue
[y/n] ?
```

Displaying Open Sessions

To view all open sessions, including console, telnet and ssh, enter the command `show session-list`.

**Syntax:** show session-list

*Displays the active incoming and outgoing sessions.*
```
HP Switch(config)# show session-list

Session Information
Source IP Selection: Outgoing Interface

Session  :     1
Privilege: Superuser
From     : Console
To       :

Session  :     2
Privilege: Manager
From     : 172.22.16.3
To       : 10.1.248.198

Session  : **  3
Privilege: Manager
From     : 10.1.248.179
To       :
```

Figure 7-15. Example of Open Sessions Listing
### Messages Related to SSH Operation

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| 00000K Peer unreachable. | File transfer did not occur. Indicates an error in communicating with the tftp server or not finding the file to download. Causes include such factors as:  
- Incorrect IP configuration on the switch  
- Incorrect IP address in the command  
- Case (upper/lower) error in the filename used in the command  
- Incorrect configuration on the TFTP server  
- The file is not in the expected location.  
- Network misconfiguration  
- No cable connection to the network |
| 00000K Transport error. | File transfer did not occur. Indicates the switch experienced a problem when trying to copy tftp the requested file. The file may not be in the expected directory, the filename may be misspelled in the command, or the file permissions may be wrong. |
| Cannot bind reserved TCP port <port-number>. | The ip ssh port command has attempted to configure a reserved TCP port. Use the default or select another port number. See “Note on Port Number” on page 7-18. |
| Client public key file corrupt or not found. Use 'copy tftp pub-key-file <ip-addr> <filename>' to download new file. | The client key does not exist in the switch. Use copy tftp to download the key from a TFTP server. |
| Download failed: overlength key in key file. | The public key file you are trying to download has one of the following problems:  
- A key in the file is too long. The maximum key length is 1024 characters, including spaces. This could also mean that two or more keys are merged together instead of being separated by a <CR><LF>.  
- There are more than ten public keys in the key file and switch total. Delete some keys from the switch or file. The switch does not detect duplicate keys.  
- One or more keys in the file is corrupted or is not a valid public key.  
Refer to “To Create a Client-Public-Key Text File” on page 25 for information on client-public-key properties. |
| Download failed: too many keys in key file. |  |
| Download failed: one or more keys is not a valid public key. |  |
| Error: Requested keyfile does not exist. | The client key does not exist in the switch. Use copy tftp to download the key from a TFTP server. |
Configuring Secure Shell (SSH)

Messages Related to SSH Operation

Logging Messages

There are event log messages when a new key is generated and zeroized for the server:

```
ssh: New <num-bits>-bit [rsa | dsa] SSH host key installed
ssh: SSH host key zeroized
```

There are also messages that indicates when a client public key is installed or removed:

```
```

**Note:** Only up to 39 characters of the key comment are included in the event log message.

Debug Logging

To add ssh messages to the debug log output, enter this command:

```
HP Switch# debug ssh LOGLEVEL
```

where LOGLEVEL is one of the following (in order of increasing verbosity):

- fatal
- error
- info
- verbose
- debug
- debug2
- debug3

---

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating new RSA host key. If the cache is depleted, this could take up to two minutes.</td>
<td>After you execute the `generate ssh [dsa</td>
</tr>
<tr>
<td>Host RSA key file corrupt or not found. Use 'generate ssh [dsa</td>
<td>rsa]' to create new host key.</td>
</tr>
</tbody>
</table>
Configuring Secure Shell (SSH)
Messages Related to SSH Operation
Configuring Secure Socket Layer (SSL)

Overview

The switches covered in this guide use Secure Socket Layer Version 3 (SSLv3) and support for Transport Layer Security (TLSv1) to provide remote web access to the switches via encrypted paths between the switch and management station clients capable of SSL/TLS operation.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>WebAgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating a Self Signed Certificate on the switch</td>
<td>No</td>
<td>n/a</td>
<td>page 8-6</td>
<td>page 8-12</td>
</tr>
<tr>
<td>Generating a Certificate Request on the switch</td>
<td>No</td>
<td>n/a</td>
<td>n/a</td>
<td>page 8-13</td>
</tr>
<tr>
<td>Enabling SSL</td>
<td>Disabled</td>
<td>n/a</td>
<td>page 8-15</td>
<td>page 8-16</td>
</tr>
</tbody>
</table>

Note

HP Switches use SSL and TLS for all secure web transactions, and all references to SSL mean using one of these algorithms unless otherwise noted.

SSL provides all the web functions but, unlike standard web access, SSL provides encrypted, authenticated transactions. The authentication type includes server certificate authentication with user password authentication.

Note

SSL in the switches covered in this guide is based on the OpenSSL software toolkit. For more information on OpenSSL, visit [www.openssl.com](http://www.openssl.com).

Server Certificate authentication with User Password Authentication. This option is a subset of full certificate authentication of the user and host. It occurs only if the switch has SSL enabled. As in figure 8-1, the switch authenticates itself to SSL-enabled web browser. Users on SSL browser then authenticate themselves to the switch (operator and/or manager levels) by providing passwords stored locally on the switch or on a TACACS+ or RADIUS server. However, the client does not use a certificate to authenticate itself to the switch.
Configuring Secure Socket Layer (SSL)

Overview

Figure 8-1. Switch/User Authentication

SSL on the switches covered in this guide supports these data encryption methods:

- 3DES (168-bit, 112 Effective)
- DES (56-bit)
- RC4 (40-bit, 128-bit)

Note

HP Switches use RSA public key algorithms and Diffie-Hellman, and all references to a key mean keys generated using these algorithms unless otherwise noted.
Terminology

- **SSL Server**: An HP switch with SSL enabled.

- **Key Pair**: Public/private pair of RSA keys generated by switch, of which public portion makes up part of server host certificate and private portion is stored in switch flash (not user accessible).

- **Digital Certificate**: A certificate is an electronic “passport” that is used to establish the credentials of the subject to which the certificate was issued. Information contained within the certificate includes: name of the subject, serial number, date of validity, subject’s public key, and the digital signature of the authority who issued the certificate. Certificates on HP switches conform to the X.509v3 standard, which defines the format of the certificate.

- **Self-Signed Certificate**: A certificate not verified by a third-party certificate authority (CA). Self-signed certificates provide a reduced level of security compared to a CA-signed certificate.

- **CA-Signed Certificate**: A certificate verified by a third party certificate authority (CA). Authenticity of CA-Signed certificates can be verified by an audit trail leading to a trusted root certificate.

- **Root Certificate**: A trusted certificate used by certificate authorities to sign certificates (CA-Signed Certificates) and used later on to verify that authenticity of those signed certificates. Trusted certificates are distributed as an integral part of most popular web clients. (see browser documentation for which root certificates are pre-installed).

- **Manager Level**: Manager privileges on the switch.

- **Operator Level**: Operator privileges on the switch.

- **Local password or username**: A Manager-level or Operator-level password configured in the switch.

- **SSL Enabled**: (1) A certificate key pair has been generated on the switch (WebAgent or CLI command: `crypto key generate cert [key size]`) (2) A certificate been generated on the switch (WebAgent or CLI command: `crypto host-cert generate self-signed [arg-list]`) and (3) SSL is enabled (WebAgent or CLI command: `web-management ssl`). (You can generate a certificate without enabling SSL, but you cannot enable SSL without first generating a Certificate.)
Prerequisite for Using SSL

Before using the switch as an SSL server, you must install a publicly or commercially available SSL-enabled web browser application on the computer(s) you use for management access to the switch.

Steps for Configuring and Using SSL for Switch and Client Authentication

The general steps for configuring SSL include:

A. Client Preparation
   1. Install an SSL capable browser application on a management station you want to use for access to the switch. (Refer to the documentation provided with your browser.)

B. Switch Preparation
   1. Assign a login (Operator) and enable (Manager) password on the switch. (page 8-6)
   2. Generate a host certificate on the switch. (page 8-6)
      i. Generate certificate key pair
      ii. Generate host certificate

You need to do this only once. The switch's own public/private certificate key pair and certificate are stored in the switch's flash memory and are not affected by reboots or the erase startup-config command. (You can remove or replace this certificate, if necessary.) The certificate key pair and the SSH key pair are independent of each other, which means a switch can have two keys pairs stored in flash.

Note

The latest versions of Microsoft Internet Explorer and Netscape web browser support SSL and TLS functionality. See browser documentation for additional details.
3. Enable SSL on the switch. (page 8-15)

4. Use your SSL enabled browser to access the switch using the switch’s IP address or DNS name (if allowed by your browser). Refer to the documentation provided with the browser application.

General Operating Rules and Notes

■ Once you generate a certificate on the switch you should avoid re-generating the certificate without a compelling reason. Otherwise, you will have to re-introduce the switch’s certificate on all management stations (clients) you previously set up for SSL access to the switch. In some situations this can temporarily allow security breaches.

■ The switch's own public/private certificate key pair and certificate are stored in the switch's flash memory and are not affected by reboots or the erase startup-config command

■ The public/private certificate key pair is not be confused with the SSH public/private key pair. The certificate key pair and the SSH key pair are independent of each other, which means a switch can have two keys pairs stored in flash
Configuring the Switch for SSL Operation

<table>
<thead>
<tr>
<th>SSL-Related CLI Commands in This Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>web-management ssl</td>
<td>8-16</td>
</tr>
<tr>
<td>show config</td>
<td>8-16</td>
</tr>
<tr>
<td>show crypto host-cert</td>
<td>8-10</td>
</tr>
<tr>
<td>crypto key</td>
<td></td>
</tr>
<tr>
<td>generate cert rsa bits &lt;1024</td>
<td>2048&gt;</td>
</tr>
<tr>
<td>zeroize cert</td>
<td>8-8</td>
</tr>
<tr>
<td>crypto host-cert</td>
<td></td>
</tr>
<tr>
<td>generate self-signed [arg-list]</td>
<td>8-8</td>
</tr>
<tr>
<td>zeroize</td>
<td>8-8</td>
</tr>
</tbody>
</table>

1. Assigning a Local Login (Operator) and Enabling (Manager) Password

At a minimum, HP recommends that you always assign at least a Manager password to the switch. Otherwise, under some circumstances, anyone with Telnet, web, or serial port access could modify the switch’s configuration.

Using the WebAgent To Configure Local Passwords. You can configure both the Operator and Manager password in the WebAgent. To access the WebAgent, refer to the chapter titled “Using the HP WebAgent” in the Basic Operation Guide for your switch.

2. Generating the Switch’s Server Host Certificate

You must generate a server certificate on the switch before enabling SSL. The switch uses this server certificate, along with a dynamically generated session key pair to negotiate an encryption method and session with a browser trying to connect via SSL to the switch. (The session key pair mentioned above is not visible on the switch. It is a temporary, internally generated pair used for a particular switch/client session, and then discarded.)
The server certificate is stored in the switch’s flash memory. The server certificate should be added to your certificate folder on the SSL clients who you want to have access to the switch. Most browser applications automatically add the switch’s host certificate to there certificate folder on the first use. This method does allow for a security breach on the first access to the switch. (Refer to the documentation for your browser application.)

There are two types of certified that can be used for the switch’s host certificate. The first type is a self-signed certificate, which is generated and digitally signed by the switch. Since self-signed certificates are not signed by a third-party certificate authority, there is no audit trail to a root CA certificate and no fool-proof means of verifying authenticity of certificate. The second type is a certificate authority-signed certificate, which is digitally signed by a certificate authority, has an audit trail to a root CA certificate, and can be verified unequivocally.

**Note**

There is usually a fee associated with receiving a verified certificate and the valid dates are limited by the root certificate authority issuing the certificate.

When you generate a certificate key pair and/or certificate on the switch, the switch places the key pair and/or certificate in flash memory (and not in running config). Also, the switch maintains the certificate across reboots, including power cycles. You should consider this certificate to be “permanent”; that is, avoid re-generating the certificate without a compelling reason. Otherwise, you will have to re-introduce the switch’s host certificate on all management stations you have set up for SSL access to the switch using the earlier certificate.

Removing (zeroizing) the switch’s certificate key pair or certificate render the switch unable to engage in SSL operation and automatically disables SSL on the switch. (To verify whether SSL is enabled, execute `show config`.)

**To Generate or Erase the Switch’s Server Certificate with the CLI**

Because the host certificate is stored in flash instead of the running-config file, it is not necessary to use `write memory` to save the certificate. Erasing the host certificate automatically disables SSL.
Configuring Secure Socket Layer (SSL)
Configuring the Switch for SSL Operation

CLI commands used to generate a Server Host Certificate.

**Syntax:**
- `crypto key generate cert rsa bits < 1024 | 2048>`
  - Generates a key pair for use in the certificate.
- `crypto key zeroize cert`
  - Erases the switch's certificate key and disables SSL operation.
- `crypto host-cert generate self-signed [arg-list]`
  - Generates a self-signed host certificate for the switch. If a switch certificate already exists, replaces it with a new certificate. (See the Note, above.)
- `crypto host-cert zeroize`
  - Erases the switch's host certificate and disables SSL operation.

To generate a host certificate from the CLI:

i. Generate a certificate key pair. This is done with the `crypto key generate cert` command. The default key size is 512.

ii. Generate a new self-signed host certificate. This is done with the `crypto host-cert generate self-signed [arg-list]` command.

**Note**
If a certificate key pair is already present in the switch, it is not necessary to generate a new key pair when generating a new certificate. The existing key pair may be re-used and the `crypto key generate cert` command does not have to be executed.

**Note**
When generating a self-signed host certificate on the CLI if there is not certificate key generated this command will fail.

Comments on Certificate Fields.

There are a number arguments used in the generation of a server certificate. Table 8-1, “Certificate Field Descriptions” describes these arguments.
Configuring Secure Socket Layer (SSL)
Configuring the Switch for SSL Operation

Table 8-1. Certificate Field Descriptions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Start Date</td>
<td>This should be the date you desire to begin using the SSL functionality.</td>
</tr>
<tr>
<td>Valid End Date</td>
<td>This can be any future date, however good security practices would</td>
</tr>
<tr>
<td></td>
<td>suggest a valid duration of about one year between updates of passwords and</td>
</tr>
<tr>
<td></td>
<td>keys.</td>
</tr>
<tr>
<td>Common name</td>
<td>This should be the IP address or domain name associated with the switch.</td>
</tr>
<tr>
<td></td>
<td>Your web browser may warn you if this field does not match the URL entered</td>
</tr>
<tr>
<td></td>
<td>into the web browser when accessing the switch.</td>
</tr>
<tr>
<td>Organization</td>
<td>This is the name of the entity (e.g. company) where the switch is in service.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>This is the name of the sub-entity (e.g. department) where the switch is in</td>
</tr>
<tr>
<td>City or location</td>
<td>This is the name of the city where switch is in service.</td>
</tr>
<tr>
<td>State name</td>
<td>This is the name of the state or province where switch is in service.</td>
</tr>
<tr>
<td>Country code</td>
<td>This is the ISO two-letter country-code where switch is in service.</td>
</tr>
</tbody>
</table>

For example, to generate a new host certificate:

```
HP Switch(config)# crypto host-cert generate self-signed
Validity start date [05/17/2011]: 05/31/2011
Validity end date [05/31/2012]: 06/15/2011
Common name [10.115.134.111]: 10.255.255.255
Organizational unit [Dept Name]: Hewlett-Packard
Organization [Company Name]: HP Networking
City or location [City]: Roseville
State name [State]: CA
Country code [US]: US
```

Figure 8-2. Example of Generating a Self-Signed Server Host certificate on the CLI for the Switch

**Note**

“Zeroizing” the switch’s server host certificate or key automatically disables SSL (sets web-management ssl to No). Thus, if you zeroize the server host certificate or key and then generate a new key and server certificate, you must also re-enable SSL with the web-management ssl command before the switch can resume SSL operation.
CLI Command to view host certificates.

**Syntax:**  
```plaintext
show crypto host-cert
```

*Displays switch’s host certificate*

To view the current host certificate from the CLI you use the `show crypto host-cert` command.

For example, to display the new server host certificate:
HP Switch(config)# show crypto host-cert
Version: 3 (0x2)
Signature Algorithm: sha1withRSAEncryption
Issuer: CN=10.255.255.255, C=US, L=Roseville, O=HP Networking, OU=Hewlett-Packard, ST=CA
Validity
   Not Before: May 31 18:54:41 2011 GMT
   Not After : Jun 15 23:59:59 2011 GMT
Subject: CN=10.255.255.255, C=US, L=Roseville, O=HP Networking, OU=Hewlett-Packard, ST=CA
Subject Public Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
      Modulus (1024 bit):
         9c:26:6c:2e:8f:bf:1e:3b:cd:0d:ee:10:c4:53:36:
         29:7a:8f:68:00:0f:54:86:34:99:77:ff:bc:09:ea:
         60:74:2f:36:2a:ce:a6:b0:bc:4f:2f:01:02:dc:4a:
         f5:44:39:4:59:65:3e:1f
      Exponent: 65537 (0x10001)
Signature Algorithm: sha1withRSAEncryption
   bb:ff:89:34:89:90:1b:79:45:59:ad:8a:25:ff:ca:
   25:fd
MD5 Fingerprint: 7de9 74a5 b91b a71f 05da 8af8 c0d0 0dc0
SHA1 Fingerprint: 09dc ea88 5b7f 73b9 7524 9245 18d2 a410 1ebe 690d

Figure 8-3. Example of show crypto host-cert Command
Generate a Self-Signed Host Certificate with the WebAgent

You can configure SSL from the WebAgent. For more information on how to access the WebAgent refer to the chapter titled “Using the HP WebAgent” in the Basic Operation Guide for your switch.

To generate a self signed host certificate from the WebAgent:
   i. In the WebAgent navigation pane, click on Security.
   ii. Click on SSL.
   iii. In the Web Management box, enable SSL if it is not already checked.
   iv. Complete the fields in the SSL Certificate box and click on Create request.

**Note**

When generating a self-signed host certificate, if no key is present and the current option is selected in the RSA key size box and error will be generated. New key generation can take up to two minutes if the key queue is empty.
Generating a CA-Signed server host certificate with the WebAgent

The installation of a CA-signed certificate involves interaction with other entities and consists of three phases. The first phase is the creation of the CA certificate request, which is then copied off from the switch for submission to the certificate authority. The second phase is the actual submission process that involves having the certificate authority verify the certificate request and then digitally signing the request to generate a certificate response (the usable server host certificate). The third phase is the download phase consisting of pasting to the switch web server the certificate response, which is then validated by the switch and put into use by enabling SSL.

To generate a certificate request from the WebAgent:

i. In the navigation pane, click on Security.
ii. Click on SSL.
iii. In the Web Management box, enable SSL if it is not already checked.
iv. In the SSL Certificate box, fill out the fields and select **Create request**.

*Figure 8-5. Example of CA Certificate Generation via SSL WebAgent Screen*

To access the online help for SSL certificate generation, click on “?” in the upper right corner of the screen.
3. Enabling SSL on the Switch and Anticipating SSL Browser Contact Behavior

The `web-management ssl` command enables SSL on the switch and modifies parameters the switch uses for transactions with clients. After you enable SSL, the switch can authenticate itself to SSL enabled browsers. If you want to disable SSL on the switch, use the `no web-management ssl` command.

**Note**

Before enabling SSL on the switch you must generate the switch’s host certificate and key. If you have not already done so, refer to “2. Generating the Switch’s Server Host Certificate” on page 8-6.

When configured for SSL, the switch uses its host certificate to authenticate itself to SSL clients, however unless you disable the standard HP WebAgent with the `no web-management` command it will be still available for unsecured transactions.

**SSL Client Contact Behavior.** At the first contact between the switch and an SSL client, if you have not copied the switch’s host certificate into the browser’s certificate folder, your browser’s first connection to the switch will question the connection and, for security reasons, give you the option of accepting or refusing. If a CA-signed certificate is used on the switch, for which a root certificate exists on the client browser side, then the browser will NOT prompt the user to ensure the validity of the certificate. The browser will be able to verify the certificate chain of the switch server certificate up to the root certificate installed in the browser, thus authenticating the switch unequivocally. As long as you are confident that an unauthorized device is not using the switch’s IP address in an attempt to gain access to your data or network, you can accept the connection.

**Note**

When an SSL client connects to the switch for the first time, it is possible for a “man-in-the-middle” attack; that is, for an unauthorized device to pose undetected as the switch, and learn the usernames and passwords controlling access to the switch. When using self-signed certificates with the switch, there is a possibility for a “man-in-the-middle” attack when connecting for the first time; that is, an unauthorized device could pose undetected as a switch, and learn the usernames and passwords controlling access to the switch. Use caution when connecting for the first time to a switch using self-signed certificates. Before accepting the certificate, closely verify the contents of the certificate (see browser documentation for additional information on viewing contents of certificate).
The security concern described above does not exist when using CA-signed certificates that have been generated by certificate authorities that the web browser already trusts.

Using the CLI Interface to Enable SSL

**Syntax:**  
[no] web-management ssl

*Enables or disables SSL on the switch.*

[port < 1-65535 | default:443 >]

*The TCP port number for SSL connections (default: 443). Important: See "Note on Port Number" on page 8-17.*

`show config`

*Shows status of the SSL server. When enabled `web-management ssl` will be present in the config list.*

To enable SSL on the switch:

1. Generate a Host certificate if you have not already done so. (Refer to “2. Generating the Switch’s Server Host Certificate” on page 8-6.)
2. Execute the `web-management ssl` command.

To disable SSL on the switch, do either of the following:

- Execute `no web-management ssl`.
- Zeroize the switch’s host certificate or certificate key. (page 8-7).

Using the WebAgent to Enable SSL

To enable SSL on the switch:

1. In the navigation pane, click on **Security**.
2. Click on **SSL**.
3. Click on the **Change** button.
4. Check the SSL **Enable** box to enable SSL.
5. Enter the TCP port you desire to connect on. It is recommended you use the default IP port number of 443.
6. Click on **Save**.

To disable SSL on the switch:

1. In the navigation pane, click on **Security**.
2. Click on **SSL**.
iii. Click on the **Change** button.

iv. Uncheck the SSL **Enable** box to disable SSL.

v. Click on **Save**.

---

**Note on Port Number**

HP recommends using the default IP port number (443). However, you can use `web-management ssl tcp-port` to specify any TCP port for SSL connections except those reserved for other purposes. Examples of reserved IP ports are 23 (Telnet) and 80 (http). Some other reserved TCP ports on the switches are 49, 80, 1506, and 1513.

---

**Caution**

SSL does not protect the switch from unauthorized access via the Telnet, SNMP, or the serial port. While Telnet access can be restricted by the use of passwords local to the switch, if you are unsure of the security this provides, you may want to disable Telnet access (**no telnet**). If you need to increase SNMP security, use SNMP version 3 only for SNMP access. Another security measure is to use the Authorized IP Managers feature described in the switch’s *Security Guide*. To protect against unauthorized access to the serial port (and the Clear button, which removes local password protection), keep physical access to the switch restricted to authorized personnel.
## Common Errors in SSL Setup

<table>
<thead>
<tr>
<th>Error During</th>
<th>Possible Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating host certificate on CLI</td>
<td>You have not generated a certificate key. (Refer to “CLI commands used to generate a Server Host Certificate” on page 8-8.)</td>
</tr>
<tr>
<td>Enabling SSL on the CLI or WebAgent</td>
<td>You have not generated a host certificate. (Refer to “Generate a Self-Signed Host Certificate with the WebAgent” on page 8-12.) You may be using a reserved TCP port. (Refer to “Note on Port Number” on page 8-17.)</td>
</tr>
<tr>
<td>Unable to Connect with SSL</td>
<td>You may not have SSL enabled (Refer to “3. Enabling SSL on the Switch and Anticipating SSL Browser Contact Behavior” on page 8-15.) Your browser may not support SSLv3 or TLSv1 or it may be disabled. (Refer to the documentation provided for your browser.)</td>
</tr>
</tbody>
</table>
IPv4 Access Control Lists (ACLs)

Introduction
An Access Control List (ACL) is a list of one or more Access Control Entries (ACEs) specifying the criteria the switch uses to either permit (forward) or deny (drop) IP packets traversing the switch’s interfaces. This chapter describes how to configure, apply, and edit IPv4 ACLs in a network populated with the switches covered by this guide, and how to monitor IPv4 ACL actions.

Note
This chapter describes ACLs for IPv4 configuration and operation. In this chapter, unless otherwise noted:
- The term “ACL” refers to IPv4 ACLs.
- Descriptions of ACL operation apply only to IPv4 ACLs.
For information on dynamic (RADIUS-assigned) ACLs, refer to “Dynamic Port ACLs” on page 9-3.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard ACLs</td>
<td>None</td>
<td>9-41</td>
</tr>
<tr>
<td>Extended ACLs</td>
<td>None</td>
<td>9-50</td>
</tr>
<tr>
<td>Enable or Disable an ACL</td>
<td>n/a</td>
<td>9-70</td>
</tr>
<tr>
<td>Display ACL Data</td>
<td>n/a</td>
<td>9-82</td>
</tr>
<tr>
<td>Delete an ACL</td>
<td>n/a</td>
<td>9-71</td>
</tr>
<tr>
<td>Configure an ACL from a TFTP Server</td>
<td>n/a</td>
<td>9-91</td>
</tr>
<tr>
<td>Enable ACL Logging</td>
<td>n/a</td>
<td>9-95</td>
</tr>
</tbody>
</table>

IPv4 filtering with ACLs can help improve network performance and restrict network use by creating policies for:
- **Switch Management Access**: Permits or denies in-band management access. This includes limiting and/or preventing the use of designated protocols that run on top of IPv4, such as TCP, UDP, IGMP, ICMP, and others. Also included are the use of precedence and ToS criteria, and control for application transactions based on source and destination IPv4 addresses and transport layer port numbers.
IPv4 Access Control Lists (ACLs)

Introduction

- **Application Access Security:** Eliminates unwanted traffic in a path by filtering IPv4 packets where they enter or leave the switch on specific interfaces.

IPv4 ACLs can filter traffic to or from a host, a group of hosts, or entire subnets.

---

**Notes**

IPv4 ACLs can enhance network security by blocking selected traffic, and can serve as part of your network security program. *However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IPv4 packet transmissions, they should not be relied upon for a complete security solution.*

IPv4 ACLs on the switches covered by this manual do not filter non-IPv4 traffic such as IPv6, AppleTalk, and IPX packets.
Overview of Options for Applying IPv4 ACLs on the Switch

To apply IPv4 ACL filtering, assign a configured IPv4 ACL to the interface on which you want traffic filtering to occur. Port traffic ACLs can be applied either statically or dynamically (using a RADIUS server).

Static ACLs

Static ACLs are configured on the switch. To apply a static ACL, you must assign it to an interface. A static port ACL is an ACL configured on a port to filter traffic entering the switch on that port, regardless of whether the traffic is routed, switched, or addressed to a destination on the switch itself.

Dynamic Port ACLs

A dynamic port ACL is configured on a RADIUS server for assignment to a given port when the server authenticates a specific client on that port. When the server authenticates a client associated with that ACL, the ACL is assigned to the port the client is using. The ACL then filters the IP traffic received inbound on that port from the authenticated client. When the client session ends, the ACL is removed from the port. The switch allows as many dynamic port ACLs on a port as it allows authenticated clients.

Note

This chapter describes the IPv4 ACL applications you can statically configure on the switch. For information on dynamic port ACLs assigned by a RADIUS server, refer to chapter 6, “Configuring RADIUS Server Support for Switch Services”.

9-3
**IPv4 Access Control Lists (ACLs)**

Overview of Options for Applying IPv4 ACLs on the Switch

<table>
<thead>
<tr>
<th>Action</th>
<th>Command(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create a Standard, Named ACL</strong>&lt;br&gt;or Add an ACE to the End of an Existing Standard, Named ACL</td>
<td>HP Switch(config)# ip access-list standard &lt; name-str &gt;&lt;br&gt;HP Switch(config-std-nacl)# &lt; deny</td>
<td>permit &gt;&lt;br&gt;&lt; any</td>
</tr>
<tr>
<td><strong>Create a Standard, Numbered ACL</strong>&lt;br&gt;or Add an ACE to the End of an Existing Standard, Numbered ACL</td>
<td>HP Switch(config)# access-list &lt; 1-99 &gt; &lt; deny</td>
<td>permit &gt;&lt;br&gt;&lt; any</td>
</tr>
<tr>
<td><strong>Use a Sequence Number To Insert an ACE in a Standard ACL</strong></td>
<td>HP Switch(config)# ip access-list standard &lt; name-str &gt;</td>
<td>1-99 &gt; &lt; deny</td>
</tr>
<tr>
<td><strong>Use an ACE’s Sequence Number To Delete the ACE from a Standard ACL</strong></td>
<td>HP Switch(config)# ip access-list standard &lt; name-str &gt;</td>
<td>1-99 &gt; &lt; 1-2147483647 &gt;&lt;br&gt;HP Switch(config-std-nacl)# no &lt; 1-2147483647 &gt;</td>
</tr>
<tr>
<td><strong>Resequence the ACEs in a Standard ACL</strong></td>
<td>HP Switch(config)# ip access-list resequence &lt; name-str &gt;</td>
<td>1-99 &gt;</td>
</tr>
<tr>
<td><strong>Enter or Remove a Remark from a Standard ACL</strong></td>
<td>HP Switch(config)# ip access-list standard &lt; name-str &gt;</td>
<td>1-99 &gt;&lt;br&gt;HP Switch(config-ext-nacl)# [ remark &lt; remark-str &gt;</td>
</tr>
<tr>
<td><strong>Delete a Standard ACL</strong></td>
<td>HP Switch(config)# no ip access-list standard &lt; name-str &gt;</td>
<td>1-99 &gt;</td>
</tr>
</tbody>
</table>

*For numbered, standard ACLs only, the following remark commands can be substituted for the above:*<br>HP Switch(config)# access-list < 1 - 99 > remark < remark-str ><br>HP Switch(config)# [ no ] access-list < 1 - 99 > remark

*The mask can be in either dotted-decimal notation (such as 0.0.15.255) or CIDR notation (such as /20).*

*The [ log ] function applies only to “deny” ACLs, and generates a message only when there is a “deny” match.*
Overview of Options for Applying IPv4 ACLs on the Switch

Table 9-2. Command Summary for IPv4 Extended ACLs

<table>
<thead>
<tr>
<th>Action</th>
<th>Command(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an Extended, Named ACL or Add an ACE to the End of an Existing, Extended ACL</td>
<td>HP Switch(config)# ip access-list extended &lt; name-str</td>
<td>100-199 &gt; &lt; deny</td>
</tr>
</tbody>
</table>

Note: Uses the same IP, TCP/UDP, IGMP, and ICMP options as shown above for “Create an Extended, Named ACL”.

Insert an ACE by Assigning a Sequence Number | HP Switch(config)# ip access-list extended < name-str | 100-199 > HP Switch(config-ext-nacl)# 1-2147483647 < deny | permit > |

Uses the options shown above for “Create an Extended, Named ACL”.

Delete an ACE by Specifying Its Sequence Number | HP Switch(config)# ip access-list extended < name-str | 100-199 > HP Switch(config-std-nacl)# no 1-2147483647 > |

Resequence the ACEs in an ACL | HP Switch(config)# ip access-list resequence < name-str | 100-199 > < 1-2147483647 > < 1-2147483646 > |

The mask can be in either dotted-decimal notation (such as 0.0.15.255) or CIDR notation (such as /20).
The [log] function applies only to “deny” ACLs, and generates a message only when there is a “deny” match.
**IPv4 Access Control Lists (ACLs)**

Overview of Options for Applying IPv4 ACLs on the Switch

<table>
<thead>
<tr>
<th>Action</th>
<th>Command(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter or Remove a</td>
<td>HP Switch(config)# ip access-list extended &lt;name-str</td>
<td>100-199&gt;</td>
</tr>
<tr>
<td>Remark</td>
<td>HP Switch(config-ext-nacl)# [remark &lt;remark-str&gt;</td>
<td>no remark]</td>
</tr>
<tr>
<td></td>
<td>For numbered, extended ACLs only, the following remark commands can be</td>
<td></td>
</tr>
<tr>
<td></td>
<td>substituted for the above:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP Switch(config)# access-list &lt;100-199&gt; remark &lt;remark-str&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP Switch(config)# [no] access-list &lt;100-199&gt; remark</td>
<td></td>
</tr>
<tr>
<td>Delete an Extended</td>
<td>HP Switch(config)# no ip access-list extended &lt;name-str</td>
<td>100-199&gt;</td>
</tr>
<tr>
<td>ACL</td>
<td>For numbered, extended ACLs only, the following command can also be used:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP Switch(config)# no access-list &lt;100-199&gt;</td>
<td></td>
</tr>
</tbody>
</table>

**Table 9-3. Command Summary for Enabling, Disabling, and Displaying ACLs**

| Enable or Disable a     | HP Switch(config)# [no] interface <port-list | Trk> access-group <identifier> in |      |
| Static Port ACL         | HP Switch(eth-<port-list | Trk>)# [no] ip access-group <identifier> in |      |
| Displaying ACL Data     | HP Switch(config)# show access-list | acl-identifier>                  | 9-82 |
|                         | HP Switch(config)# show access-list <acl-identifier>                      |      |
|                         | HP Switch(config)# show access-list config                                |      |
|                         | HP Switch(config)# show access-list ports <port-list | trk> |      |
|                         | HP Switch(config)# show access-list radius                                |      |
IPv4 Access Control Lists (ACLs)

Terminology

**Access Control Entry (ACE):** A policy consisting of criteria and an action (permit or deny) to execute on a packet if it meets the criteria. The elements composing the criteria include:
- source IPv4 address and mask (standard and extended ACLs)
- destination IPv4 address and mask (extended ACLs only)
- either of the following:
  - all IPv4 traffic
  - IPv4 traffic of a specific IP protocol (extended ACLs only) (In the cases of TCP, UDP, ICMP, and IGMP, the criteria can include either all IP traffic of the protocol type or only the traffic of a specific sub-type within the protocol.)
- option to log packet matches with **deny** ACEs
- optional use of IP precedence and ToS settings (extended ACLs only)

**Access Control List (ACL):** A list (or set) consisting of one or more explicitly configured Access Control Entries (ACEs) and terminating with an implicit “deny” ACE. ACL types include “standard” and “extended”. See also “Standard ACL” and “Extended ACL”. To filter IPv4 traffic, apply either type:
- Static Port ACL: an ACL assigned to filter inbound traffic on a specific switch port
- Dynamic Port ACL: dynamic ACL assigned to a port by a RADIUS server to filter inbound traffic from an authenticated client on that port

An ACL can be configured on a port (or static trunk) as a static port ACL. (Dynamic port ACLs are configured on a RADIUS server.)

**ACE:** See “Access Control Entry”.

**ACL:** See “Access Control List”.

**ACL ID:** A number or alphanumeric string used to identify an ACL. A standard IPv4 ACL ID can have either an alphanumeric string or a number in the range of 1 to 99. An extended IPv4 ACL ID can have either an alphanumeric string or a number in the range of 100 to 199. See also “Identifier”.

**Note:** RADIUS-assigned ACLs are identified by client authentication data and do not use the ACL ID strings described here.
IPv4 Access Control Lists (ACLs)

Terminology

**ACL Mask**: Follows any IPv4 address (source or destination) listed in an ACE. Defines which bits in a packet’s corresponding IPv4 addressing must exactly match the addressing in the ACE, and which bits need not match (wildcards). See also “How an ACE Uses a Mask To Screen Packets for Matches” on page 9-25.

**CIDR**: This is the acronym for Classless Inter-Domain Routing.

**DA**: The acronym used in text to represent *Destination Address*. In an IPv4 packet, this is the destination address carried in the header, and identifies the destination intended by the packet’s originator. In an extended ACE, this is the second of two addresses required by the ACE to determine whether there is a match between a packet and the ACE. See also “SA”.

**Deny**: An ACE configured with this action causes the switch to drop a packet for which there is a match within an applicable ACL.

**Dynamic Port ACL**: An ACL assigned by a RADIUS server to a port to filter inbound IP traffic from a client authenticated by the server for that port. A dynamic port ACL can be configured (on a RADIUS) server to filter inbound IPv4 traffic. When the client session ends, the dynamic port ACL for that client is removed from the port. See also “Implicit Deny”.

**Extended ACL**: This type of IPv4 Access Control List uses layer-3 IP criteria composed of source and destination addresses and (optionally) TCP/UDP port, ICMP, IGMP, precedence, or ToS criteria to determine whether there is a match with an IP packet. Except for RADIUS-assigned ACLs, which use client credentials for identifiers, extended ACLs require an alphanumeric name or an identification number (ID) in the range of 100 - 199.

**Identifier**: A term used in ACL syntax statements to represent either the name or number by which the ACL can be accessed. See also NAME-STR. Note that RADIUS-assigned ACLs are identified by client authentication data and do not use the identifiers described in this chapter.

**Implicit Deny**: If the switch finds no matches between an IPv4 packet and the configured criteria in an applicable static or dynamic ACL, then the switch denies (drops) the packet with an implicit deny any function (for standard ACLs) or an implicit deny ip any any function (for extended ACLs). You can preempt the Implicit Deny in a given ACL by configuring a permit any (standard) or permit ip any any (extended) as the last explicit ACE in the ACL. Doing so permits any IPv4 packet that is not explicitly permitted or denied by other ACEs configured sequentially earlier in the ACL. Unless otherwise noted, Implicit Deny refers to the “deny” function enforced by both standard and extended ACLs.
IPv4 Access Control Lists (ACLs)

Terminology

Inbound Traffic: For the purpose of defining where the switch applies IPv4 ACLs to filter traffic, inbound traffic is a packet that meets one of the following criteria:

- Static Port ACL: Inbound traffic is a packet entering the switch on the port.
- Dynamic Port ACL: Where a RADIUS server has authenticated a client and assigned an ACL to the port to filter the client’s IPv4 traffic, inbound traffic is a packet entering the switch from that client.

NAME-STR: A term used in extended ACL syntax statements to represent the “name string”; the alphanumeric string used to identify the ACL. See also identifier and ACL-ID.

Named ACL: An ACL created with the `ip access-list < extended | standard > < name-str >` command and then populated using the `< deny | permit >` command in the Named ACL (`nacl`) CLI context. (Refer to “Entering the IPv4 “Named ACL” (`nacl`) Context” on page 9-43.)

Numbered ACL: An ACL created and initially populated by using the `access-list < extended < 100 - 199 > | standard < 1-99 >>` command. (Refer to “Creating or Adding to an Standard, Numbered ACL” on page 9-47.) After a numbered ACL has been created, the switch manages it in the same way as a named ACL, meaning that it can be applied and edited in the same way as a named ACL.

Permit: An ACE configured with this action allows the switch to forward a packet for which there is a match within an applicable ACL.

Permit Any Forwarding: An ACE configured with this action causes the switch to forward IP packets that have not been permitted or denied by earlier ACEs in the list. In a standard ACL, this is `permit any`. In an extended ACL, it is `permit ip any any`.

RADIUS-Assigned ACL: See “Dynamic Port ACL”.

remark-str: The term used in ACL syntax statements to represent the variable “remark string”; a set of alphanumeric characters you can include in a remark in an ACL. A remark string can include up to 100 characters and must be delimited by single or double quotes if any spaces are included in the string.

SA: The acronym for Source Address. In an IPv4 packet, this is the source IPv4 address carried in the IP header, and identifies the packet’s sender. In a standard ACE, this is the IPv4 address used by the ACE to determine
whether there is a match between a packet and the ACE. In an extended ACE, this is the first of two IPv4 addresses used by the ACE to determine whether there is a match between a packet and the ACE. See also “DA”.

**seq-#**: The term used in ACL syntax statements to represent the sequence number variable used to insert an ACE within an existing list. The range allowed for sequence numbers is 1 - 2147483647.

**Standard ACL**: This type of access control list uses the layer-3 IP criteria of source IPv4 address to determine whether there is a match with an IPv4 packet. Except for RADIUS-assigned ACLs, standard ACLs require an alphanumeric name or an identification number (ID) in the range of 1-99. See also **identifier** on page 9-8.

**Static Port ACL**: An ACL statically configured on a specific port, group of ports, or trunk. A static port ACL filters all incoming IPv4 traffic on the port, regardless of whether it is switched or routed.

**Wildcard**: The part of a mask that indicates the bits in a packet's IPv4 addressing that do not need to match the corresponding bits specified in an ACL. See also **ACL Mask** on page 9-8.
Overview

Types of IPv4 ACLs

A permit or deny policy for IPv4 traffic you want to filter can be based on source address alone, or on source address plus other factors.

**Standard ACL:** Use a standard ACL when you need to permit or deny IPv4 traffic based on source address only. Standard ACLs are also useful when you need to quickly control a performance problem by limiting IPv4 traffic from a subnet, group of devices, or a single device. (This can block all IPv4 traffic from the configured source, but does not hamper IPv4 traffic from other sources within the network.) A standard ACL uses an alphanumeric ID string or a numeric ID of 1 through 99. You can specify a single host, a finite group of hosts, or any host.

**Extended ACL:** Use an extended ACL when simple IPv4 source address restrictions do not provide the sufficient traffic selection criteria needed on an interface. Extended ACLs allow use of the following criteria:

- source and destination IPv4 address combinations
- IP protocol options

Extended, named ACLs also offer an option to permit or deny IPv4 connections using TCP for applications such as Telnet, http, ftp, and others.

**ACL Applications**

ACL filtering is applied to IPv4 traffic as follows:

- Static port ACL: any inbound IPv4 traffic on that port.
- Dynamic port ACL: on a port having an ACL assigned by a RADIUS server to filter an authenticated client’s traffic, filters inbound IPv4 traffic from that client

(For information on RADIUS-assigned ACLs, refer to chapter 6 “Configuring RADIUS Server Support for Switch Services”.)
Static Port ACL and Dynamic Port ACL Applications

An IPv4 static port ACL filters any IPv4 traffic inbound on the designated port, regardless of whether the traffic is switched or routed.

Dynamic (RADIUS-assigned) Port ACL Applications

Dynamic (RADIUS-assigned) port ACLs are configured on RADIUS servers and, where such servers support configuration for IPv4 traffic filtering, can be assigned to filter IPv4 traffic inbound from clients authenticated by such servers. For example, client “A” connects to a given port and is authenticated by a RADIUS server. Because the server is configured to assign a dynamic ACL to the port, the IPv4 traffic inbound on the port from client “A” is filtered.

Effect of Dynamic Port ACLs When Multiple Clients Are Using the Same Port. Some network configurations may allow multiple clients to authenticate through a single port where a RADIUS server assigns a separate, dynamic port ACL in response to each client’s authentication on that port. In such cases, a given client’s inbound traffic will be allowed only if the RADIUS authentication response for that client includes a dynamic port ACL. For example, in figure 9-1 (below), clients A through D authenticate through the same port (B1) on the HP-A switch.

![Figure 9-1. Example of Multiple Clients Authenticating Through a Single Port](image)

In this case, the RADIUS server must be configured to assign a dynamic port ACL to port B1 each time any of the clients authenticates on the port.
802.1X User-Based and Port-Based Applications. User-Based 802.1X access control allows up to 8 individually authenticated clients on a given port. However, port-based access control does not set a client limit, and requires only one authenticated client to open a given port (and is recommended for applications where only one client at a time can connect to the port).

- If you configure 802.1X user-based security on a port and the RADIUS response includes a dynamic port ACL for at least one authenticated client, then the RADIUS response for all other clients authenticated on the port must also include a dynamic port ACL. Traffic on the port from any client that authenticates without the RADIUS server including a dynamic port ACL in its response will be dropped and the client will be de-authenticated.

- Using 802.1X port-based security on a port where the RADIUS response includes a dynamic port ACL, only the first client to authenticate can use the port. Traffic from other clients will be dropped.

Multiple ACLs on an Interface

Multiple ACL Assignments Allowed. The switch allows multiple ACL applications on an interface (subject to internal resource availability). This means that a port can simultaneously be subject to the following:

- One static port ACL for any IPv4 traffic entering the switch on the port.

- One dynamic (RADIUS-assigned) port ACL applied to inbound IPv4 traffic for each authenticated client on the port

Features Common to All ACL Applications

- Any ACL can have multiple entries (ACEs).

- You can apply any one ACL to multiple interfaces.

- All ACEs in an ACL configured on the switch are automatically sequenced (numbered). For an existing ACL, entering an ACE without specifying a sequence number automatically places the ACE at the end of the list. Specifying a sequence number inserts the ACE into the list at the correct sequential location.

  - Automatic sequence numbering begins with “10” and increases in increments of 10. You can renumber the ACEs in an ACL and also change the sequence increment between ACEs.
IPv4 Access Control Lists (ACLs)

Overview

- The CLI `remark` command option allows you to enter a separate comment for each ACE.

- A source or destination IPv4 address and a mask, together, can define a single host, a range of hosts, or all hosts.

- Every ACL populated with one or more explicit ACEs includes an Implicit Deny as the last entry in the list. The switch applies this action to any packets that do not match other criteria in the ACL. (For standard ACLs, the Implicit Deny is `deny any`. For extended ACLs, it is `deny ip any any`.)

- In any ACL, you can apply an ACL log function to ACEs that have an explicit “deny” action. The logging occurs when there is a match on a “deny” ACE (except when the ACL is used for mirroring). The switch sends ACL logging output to Syslog, if configured, and, optionally, to a console session.

You can create ACLs for the switch configuration using either the CLI or a text editor. The text-editor method is recommended when you plan to create or modify an ACL that has more entries than you can easily enter or edit using the CLI alone. Refer to “Creating or Editing ACLs Offline” on page 9-91.
General Steps for Planning and Configuring ACLs

1. Identify the ACL application to apply. As part of this step, determine the best points at which to apply specific ACL controls. For example, you can improve network performance by filtering unwanted IPv4 traffic at the edge of the network instead of in the core. Also, on the switch itself, you can improve performance by filtering unwanted IPv4 traffic where it is inbound to the switch instead of outbound.

<table>
<thead>
<tr>
<th>Traffic Source</th>
<th>ACL Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 traffic from a specific, authenticated client</td>
<td>dynamic port ACL (RADIUS-assigned ACL) for inbound IP traffic from an authenticated client on a port*</td>
</tr>
<tr>
<td>IPv4 traffic entering the switch on a specific port</td>
<td>static port ACL (static-port assigned) for any inbound IPv4 traffic on a port from any source</td>
</tr>
</tbody>
</table>

*For more on this option, refer to chapter 6, “Configuring RADIUS Server Support for Switch Services”, and also to the documentation for your RADIUS server.

2. Identify the traffic types to filter.
   - The SA and/or the DA of traffic you want to permit or deny. This can be a single host, a group of hosts, a subnet, or all hosts.
   - Traffic of a specific IPv4 protocol type (0-255)
   - Any TCP traffic (only) for a specific TCP port or range of ports, including optional control of connection traffic based on whether the initial request should be allowed
   - All UDP traffic or UDP traffic for a specific UDP port
   - All ICMP traffic or ICMP traffic of a specific type and code
   - All IGMP traffic or IGMP traffic of a specific type
   - Any of the above with specific precedence and/or ToS settings

3. Design the ACLs for the control points (interfaces) you have selected. Where you are using explicit “deny” ACEs, you can optionally use the ACL logging feature for notification that the switch is denying unwanted packets.

4. Configure the ACLs on the selected switches.

5. Assign the ACLs to the interfaces you want to filter, using the ACL application appropriate for each assignment. (For RADIUS-assigned ACLs, refer to the Note in the table in step 1 on page 9-15.)

6. Test for desired results.
IPv4 Access Control Lists (ACLs)

Overview

For more details on ACL planning considerations, refer to “Planning an ACL Application” on page 9-21.

---

**Caution Regarding the Use of Source Routing**

Source routing is enabled by default on the switch and can be used to override ACLs. For this reason, if you are using ACLs to enhance network security, the recommended action is to use the `no ip source-route` command to disable source routing on the switch. (If source routing is disabled in the running-config file, the `show running` command includes “no ip source-route” in the running-config file listing.)
IPv4 Static ACL Operation

Introduction

An ACL is a list of one or more Access Control Entries (ACEs), where each ACE consists of a matching criteria and an action (permit or deny). A static ACL applies only to the switch in which it is configured. ACLs operate on assigned interfaces, and offer these traffic filtering options:

- IPv4 traffic inbound on a port.

The following table lists the range of interface options:

<table>
<thead>
<tr>
<th>Interface</th>
<th>ACL Application</th>
<th>Application Point</th>
<th>Filter Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Static Port ACL (switch configured)</td>
<td>inbound on the switch port</td>
<td>inbound IPv4 traffic</td>
</tr>
<tr>
<td></td>
<td>Dynamic Port ACL(^1) (RADIUS assigned)</td>
<td>inbound on the switch port used by authenticated client</td>
<td>inbound IPv4 traffic from the authenticated client</td>
</tr>
</tbody>
</table>

\(^1\)This chapter describes ACLs statically configured on the switch. For information on dynamic port ACLs assigned by a RADIUS server, refer to chapter 6, “Configuring RADIUS Server Support for Switch Services”.

Note

After you assign an IPv4 ACL to an interface, the default action on the interface is to implicitly deny IPv4 traffic that is not specifically permitted by the ACL. (This applies only in the direction of traffic flow filtered by the ACL.)

The Packet-filtering Process

**Sequential Comparison and Action.** When an ACL filters a packet, it sequentially compares each ACE’s filtering criteria to the corresponding data in the packet until it finds a match. The action indicated by the matching ACE (deny or permit) is then performed on the packet.

**Implicit Deny.** If a packet does not have a match with the criteria in any of the ACEs in the ACL, the ACL denies (drops) the packet. If you need to override the implicit deny so that a packet that does not have a match will be permitted, then you can use the “permit any” option as the last ACE in the
IPv4 Access Control Lists (ACLs)
IPv4 Static ACL Operation

ACL. This directs the ACL to permit (forward) packets that do not have a match with any earlier ACE listed in the ACL, and prevents these packets from being filtered by the implicit “deny any”.

Example. Suppose the ACL in figure 9-2 is assigned to filter the IPv4 traffic from an authenticated client on a given port in the switch:

For an inbound packet with a destination IP address of 18.28.156.3, the ACL:

1. Compares the packet to this ACE first:
   Permit in ip from any to 18.28.136.24
   Permit in ip from any to 18.28.156.7
   Deny in ip from any to 18.28.156.3
   Deny in tcp from any to any 23
   Permit in ip from any to any
   (Deny in ip from any to any)

   This line demonstrates the “deny any any” ACE implicit in every RADIUS-assigned ACL. Any inbound IPv4 traffic from the authenticated client that does not have a match with any of the five explicit ACEs in this ACL will be denied by the implicit “deny any any”.

2. Since there is not a match with the first ACE, the ACL compares the packet to the second ACE, where there is also not a match.

3. The ACL compares the packet to the third ACE. There is a exact match, so the ACL denies (drops) the packet.

4. The packet is not compared to the fourth ACE.

As shown above, the ACL tries to apply the first ACE in the list. If there is not a match, it tries the second ACE, and so on. When a match is found, the ACL invokes the configured action for that entry (permit or drop the packet) and no further comparisons of the packet are made with the remaining ACEs in the list. This means that when an ACE whose criteria matches a packet is found, the action configured for that ACE is invoked, and any remaining ACEs in the ACL are ignored. Because of this sequential processing, successfully implementing an ACL depends in part on configuring ACEs in the correct order for the overall policy you want the ACL to enforce.
IPv4 Access Control Lists (ACLs)

IPv4 Static ACL Operation

Figure 9-3. The Packet-Filtering Process in an ACL with N Entries (ACEs)

Note

The order in which an ACE occurs in an ACL is significant. For example, if an ACL contains six ACEs, but the first ACE allows Permit Any forwarding, then the ACL permits all IPv4 traffic, and the remaining ACEs in the list do not apply, even if they specify criteria that would make a match with any of the traffic permitted by the first ACE.

End

For example, suppose you want to configure an ACL on the switch (with an ID of “Test-02”) to invoke these policies for routed traffic entering the switch:
IPv4 Access Control Lists (ACLs)
IPv4 Static ACL Operation

1. Permit inbound IPv4 traffic from IP address 10.11.11.42.
2. Deny only the inbound Telnet traffic from address 10.11.11.101.
3. Permit only inbound Telnet traffic from IP address 10.11.11.33.
4. Deny all other inbound IPv4 traffic.

The following ACL model, when assigned to inbound filtering on an interface, supports the above case:

```
ip access-list extended "Test-02"
  10 permit ip 10.11.11.42 0.0.0.0 0.0.0.0 255.255.255.255
  20 deny tcp 10.11.11.101 0.0.0.0 0.0.0.0 255.255.255.255 eq 23
  30 permit ip 10.11.11.101 0.0.0.0 0.0.0.0 255.255.255.255
  40 permit tcp 10.11.11.33 0.0.0.0 0.0.0.0 255.255.255.255 eq 23
< Implicit Deny> 
exit
```

1. **Permits** IPv4 traffic from source address 10.11.11.42. Packets matching this criterion are permitted and will not be compared to any later ACE in the list. IPv4 packets not matching this criterion will be compared to the next entry in the list.
2. **Denies** Telnet traffic from source address 10.11.11.101. Packets matching this criterion are dropped and are not compared to later criteria in the list. Packets not matching this criterion are compared to the next entry in the list.
3. **Permits** IPv4 traffic from source address 10.11.11.101. Any packets matching this criterion will be permitted and will not be compared to any later criteria in the list. Because this entry comes after the entry blocking Telnet traffic from this same address, there will not be any Telnet packets to compare with this entry; they have already been dropped as a result of matching the preceding entry.
4. **Permits** Telnet traffic from source address 10.11.11.33. Packets matching this criterion are permitted and are not compared to any later criteria in the list. Packets not matching this criterion are compared to the next entry in the list.
5. This entry does not appear in an actual ACL, but is implicit as the last entry in every ACL. Any IPv4 packets that do not match any of the criteria in the ACL's preceding entries will be denied (dropped).

Figure 9-4. Example of How an ACL Filters Packets

It is important to remember that all IPv4 ACLs configurable on the switch include an implicit **deny ip any**. That is, IPv4 packets that the ACL does not **explicitly** permit or deny will be **implicitly** denied, and therefore dropped instead of forwarded on the interface. If you want to preempt the implicit deny so that IPv4 packets not explicitly denied by other ACEs in the ACL will be permitted, insert an explicit “permit any” as the last ACE in the ACL. Doing so permits any packet not explicitly denied by earlier entries.
Planning an ACL Application

Before creating and implementing ACLs, you need to define the policies you want your ACLs to enforce, and understand how the ACL assignments will impact your network users.

**Note**

All IPv4 traffic entering the switch on a given interface is filtered by all ACLs configured for inbound traffic on that interface. For this reason, an inbound IPv4 packet will be denied (dropped) if it has a match with either an implicit or explicit **deny** in any of the inbound ACLs applied to the interface.

(Refer to “Multiple ACLs on an Interface” on page 9-13.)

**IPv4 Traffic Management and Improved Network Performance**

You can use ACLs to block traffic from individual hosts, workgroups, or subnets, and to block access to VLANs, subnets, devices, and services. Traffic criteria for ACLs include:

- Switched and/or routed traffic
- Any traffic of a specific IPv4 protocol type (0-255)
- Any TCP traffic (only) for a specific TCP port or range of ports, including optional control of connection traffic based on whether the initial request should be allowed
- Any UDP traffic or UDP traffic for a specific UDP port
- Any ICMP traffic or ICMP traffic of a specific type and code
- Any IGMP traffic or IGMP traffic of a specific type
- Any of the above with specific precedence and/or ToS settings

Answering the following questions can help you to design and properly position IPv4 ACLs for optimum network usage.
IPv4 Access Control Lists (ACLs)
Planning an ACL Application

■ What are the logical points for minimizing unwanted traffic, and what
ACL application(s) should be used? In many cases it makes sense to
prevent unwanted traffic from reaching the core of your network by
configuring ACLs to drop the unwanted traffic at or close to the edge
of the network. (The earlier in the network path you can block
unwanted traffic, the greater the benefit for network performance.)

■ From where is the traffic coming? The source and destination of
traffic you want to filter determines the ACL application to use (static
port ACL, and dynamic port ACL).

■ What traffic should you explicitly block? Depending on your network
size and the access requirements of individual hosts, this can involve
creating a large number of ACEs in a given ACL (or a large number of
ACLs), which increases the complexity of your solution.

■ What traffic can you implicitly block by taking advantage of the
implicit deny ip any to deny traffic that you have not explicitly
permitted? This can reduce the number of entries needed in an ACL.

■ What traffic should you permit? In some cases you will need to
explicitly identify permitted traffic. In other cases, depending on your
policies, you can insert an ACE with “permit any” forwarding at the
end of an ACL. This means that all IPv4 traffic not specifically
matched by earlier entries in the list will be permitted.

Security
ACLs can enhance security by blocking traffic carrying an unauthorized
source IPv4 address (SA). This can include:

■ blocking access from specific devices or interfaces
■ blocking access to or from subnets in your network
■ blocking access to or from the internet
■ blocking access to sensitive data storage or restricted equipment
■ preventing specific IP, TCP, UDP, IGMP, and ICMP traffic types,
  including unauthorized access using functions such as Telnet, SSH,
  and web browser

You can also enhance switch management security by using ACLs to block
IPv4 traffic that has the switch itself as the destination address (DA).
IPv4 Access Control Lists (ACLs)
Planning an ACL Application

**Caution**
IPv4 ACLs can enhance network security by blocking selected traffic, and can serve as one aspect of maintaining network security. *However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete security solution.*

**Note**
Static ACLs for the switches covered by this guide do not filter non-IPv4 traffic such as IPv6, AppleTalk, and IPX. Dynamic port ACLs assigned by a RADIUS server can be configured on the server to filter IPv4 traffic, but do not filter non-IP traffic.

**Guidelines for Planning the Structure of a Static ACL**

After determining the filtering type (standard or extended) to use at a particular point in your network, determine the order in which to apply individual ACEs to filter IPv4 traffic (For information on ACL applications, refer to “ACL Applications” on page 9-11.).

- The sequence of ACEs is significant. When the switch uses an ACL to determine whether to permit or deny an ip packet, it compares the packet to the criteria specified in the individual Access Control Entries (ACEs) in the ACL, beginning with the first ACE in the list and proceeding sequentially until a match is found. When a match is found, the switch applies the indicated action (permit or deny) to the packet.

- The first match in an ACL dictates the action on a packet. Subsequent matches in the same ACL are ignored. However, if a packet is permitted by one ACL assigned to an interface, but denied by another ACL assigned to the same interface, the packet will be denied on the interface.

- On any ACL, the switch implicitly denies IPv4 packets that are not explicitly permitted or denied by the ACEs configured in the ACL. If you want the switch to forward a packet for which there is not a match in an ACL, append an ACE that enables Permit Any forwarding as the last ACE in the ACL. This ensures that no packets reach the Implicit Deny case for that ACL.
IPv4 Access Control Lists (ACLs)
Planning an ACL Application

- Generally, you should list ACEs from the most specific (individual hosts) to the most general (subnets or groups of subnets) unless doing so permits traffic that you want dropped. For example, an ACE allowing a small group of workstations to use a specialized printer should occur earlier in an ACL than an entry used to block widespread access to the same printer.

IPv4 ACL Configuration and Operating Rules

- **Static Port ACLs**: A static port ACL filters traffic entering the switch on the port(s) or trunk(s) to which it is assigned.

- **Per Switch ACL Limits for All ACL Types**: At a minimum an ACL must have one, explicit “permit” or “deny” Access Control Entry. You can configure up to 512 ACLs. For IPv4 ACLs, the maximums are as follows:
  - Named (Extended or Standard) ACLs: Up to 512 (minus any numeric standard or extended ACL assignments)
  - Numeric Standard ACLs: Up to 99; numeric range: 1 - 99
  - Numeric Extended ACLs: Up to 100; numeric range: 100 - 199
  - The maximum number of ACEs supported by the switch is up to 1024 for IPv4 ACEs. The maximum number of ACEs allowed on a port depends on the concurrent resource usage by multiple configured features. For more information, use the **show < qos | access-list > resources** command and/or refer to “Monitoring Shared Resources” on page 9-97.

- **Implicit Deny**: In any static IPv4 ACL, the switch automatically applies an implicit **deny ip any** that does not appear in **show** listings. This means that the ACL denies any IPv4 packet it encounters that does not have a match with an entry in the ACL. Thus, if you want an ACL to permit any packets that you have not expressly denied, you must enter a **permit any** or **permit ip any any** as the last ACE in an ACL. Because, for a given packet the switch sequentially applies the ACEs in an ACL until it finds a match, any packet that reaches the **permit any** or **permit ip any any** entry will be permitted, and will not encounter the **deny ip any** ACE the switch automatically includes at the end of the ACL. For an example, refer to figure 9-4 on page 9-20. For Implicit Deny operation in dynamic ACLs, refer to chapter 6, “Configuring RADIUS Server Support for Switch Services”
Explicitly Permitting Any IPv4 Traffic: Entering a `permit any` or a `permit ip any any` ACE in an ACL permits all IPv4 traffic not previously permitted or denied by that ACL. Any ACEs listed after that point do not have any effect.

Explicitly Denying Any IPv4 Traffic: Entering a `deny any` or a `deny ip any any` ACE in an ACL denies all IPv4 traffic not previously permitted or denied by that ACL. Any ACEs after that point have no effect.

Replacing One ACL with Another Using the Same Application: For a specific interface, the most recent ACL assignment using a given application replaces any previous ACL assignment using the same application on the same interface.

Static Port ACLs: These are applied per-port, per port-list, or per static trunk. Adding a port to a trunk applies the trunk's ACL configuration to the new member. If a port is configured with an ACL, the ACL must be removed before the port is added to the trunk. Also, removing a port from an ACL-configured trunk removes the ACL configuration from that port.

How an ACE Uses a Mask To Screen Packets for Matches

When the switch applies an ACL to IPv4 traffic, each ACE in the ACL uses an IPv4 address and *ACL mask* to enforce a selection policy on the packets being screened. That is, the mask determines the range of IPv4 addresses (SA only or SA/DA) that constitute a match between the policy and a packet being screened.

What Is the Difference Between Network (or Subnet) Masks and the Masks Used with ACLs?

In common IPv4 addressing, a network (or subnet) mask defines which part of the address to use for the network number and which part to use for the hosts on the network. For example:

<table>
<thead>
<tr>
<th>Address</th>
<th>Mask</th>
<th>Network Address</th>
<th>Host Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.38.252.195</td>
<td>255.255.255.0</td>
<td>first three octets</td>
<td>The fourth octet.</td>
</tr>
<tr>
<td>10.38.252.195</td>
<td>255.255.248.0</td>
<td>first two octets and the left-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>most five bits of the third octet</td>
<td>The right most three bits of the third octet and all bits in the fourth octet.</td>
</tr>
</tbody>
</table>
IPv4 Access Control Lists (ACLs)
Planning an ACL Application

Thus, the bits set to 1 in a network mask define the part of an IPv4 address to use for the network number, and the bits set to 0 in the mask define the part of the address to use for the host number.

In an ACL, IPv4 addresses and masks provide criteria for determining whether to deny or permit a packet, or to pass it to the next ACE in the list. If there is a match, the configured deny or permit action occurs. If there is not a match, the packet is compared with the next ACE in the ACL. Thus, where a standard network mask defines how to identify the network and host numbers in an IPv4 address, the mask used with ACEs defines which bits in a packet’s SA or DA must match the corresponding bits in the SA or DA listed in an ACE, and which bits can be wildcards.

Rules for Defining a Match Between a Packet and an Access Control Entry (ACE)

- For a given ACE, when the switch compares an IPv4 address and corresponding mask in the ACE to an IPv4 address carried in a packet:
  - A **mask-bit setting of 0** (“off”) requires that the corresponding bits in the packet’s address and in the ACE’s address must be the same. Thus, if a bit in the ACE’s address is set to 1 (“on”), the same bit in the packet’s address must also be 1.
  - A **mask-bit setting of 1** (“on”) means the corresponding bits in the packet’s address and in the ACE’s address do not have to be the same. Thus, if a bit in the ACE’s address is set to 1, the same bit in the packet’s address can be either 1 or 0 (“on” or “off”).

For an example, refer to “Example of How the Mask Bit Settings Define a Match” on page 9-28.

- In any ACE, a mask of all ones means *any* IPv4 address is a match. Conversely, a mask of all zeros means the *only* match is an IPv4 address identical to the host address specified in the ACE.

- Depending on your network, a single ACE that allows a match with more than one source or destination IPv4 address may allow a match with multiple subnets. For example, in a network with a prefix of 31.30.240 and a subnet mask of 255.255.240.0 (the leftmost 20 bits), applying an ACL mask of 0.0.31.255 causes the subnet mask and the
ACL mask to overlap one bit, which allows matches with hosts in two subnets: 31.30.224.0 and 31.30.240.0.

<table>
<thead>
<tr>
<th>Bit Position in the Third Octet of Subnet Mask 255.255.240.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit Values</td>
</tr>
<tr>
<td>Subnet Mask Bits</td>
</tr>
<tr>
<td>Mask Bit Settings Affecting Subnet Addresses</td>
</tr>
</tbody>
</table>

This ACL supernetting technique can help to reduce the number of ACLs you need. You can apply it to a multinetted VLAN and to multiple VLANs. However, ensure that you exclude subnets that do not belong in the policy. If this creates a problem for your network, you can eliminate the unwanted match by making the ACEs in your ACL as specific as possible, and using multiple ACEs carefully ordered to eliminate unwanted matches.

Every IPv4 address and mask pair (source or destination) used in an ACE creates one of the following policies:

- **Any IPv4 address fits the matching criteria.** In this case, the switch automatically enters the address and mask in the ACE. For example:

  access-list 1 deny any

  produces this policy in an ACL listing:

<table>
<thead>
<tr>
<th>Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

  This policy states that every bit in every octet of a packet’s SA is a wildcard, which covers any IPv4 address.

- **One IPv4 address fits the matching criteria.** In this case, you provide the address and the switch provides the mask. For example:

  access-list 1 permit host 10.28.100.15

  produces this policy in an ACL listing:

<table>
<thead>
<tr>
<th>Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.28.100.15</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

  This policy states that every bit in every octet of a packet’s SA must be the same as the corresponding bit in the SA defined in the ACE.
IPv4 Access Control Lists (ACLs)
Planning an ACL Application

- A group of IPv4 addresses fits the matching criteria. In this case you provide both the address and the mask. For example:

  access-list 1 permit 10.28.32.1 0.0.0.31

<table>
<thead>
<tr>
<th>Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.28.32.1</td>
<td>0.0.0.31</td>
</tr>
</tbody>
</table>

  This policy states that:
  - In the first three octets of a packet’s SA, every bit must be set the same as the corresponding bit in the SA defined in the ACE.
  - In the last octet of a packet’s SA, the first three bits must be the same as in the ACE, but the last five bits are wildcards and can be any value.

  Unlike subnet masks, the wildcard bits in an ACL mask need not be contiguous. For example, 0.0.7.31 is a valid ACL mask. However, a subnet mask of 255.255.248.224 is not a valid subnet mask.

**Example of How the Mask Bit Settings Define a Match.** Assume an ACE where the second octet of the mask for an SA is 7 (the rightmost three bits are “on”, or “1”) and the second octet of the corresponding SA in the ACE is 31 (the rightmost five bits). In this case, a match occurs when the second octet of the SA in a packet being filtered has a value in the range of 24 to 31. Refer to table 9-1, below.

**Table 9-1. Example of How the Mask Defines a Match**

<table>
<thead>
<tr>
<th>Location of Òctet</th>
<th>Bit Position in the Octet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>128</td>
</tr>
<tr>
<td>SA in ACE</td>
<td>0</td>
</tr>
<tr>
<td>Mask for SA</td>
<td>0</td>
</tr>
<tr>
<td>Corresponding Octet of a Packet’s SA</td>
<td>0</td>
</tr>
</tbody>
</table>

The shaded area indicates bits in the packet that must exactly match the bits in the source address in the ACE. Wherever the mask bits are ones (wildcards), the corresponding address bits in the packet can be any value, and where the mask bits are zeros, the corresponding address bits in the packet must be the same as those in the ACE. **Note:** This example covers only one octet of an IPv4 address. An actual ACE applies this method to all four octets of the address.

**Example of Allowing Only One IPv4 Address (“Host” Option).** Suppose, for example, that you have configured the ACL in figure 9-5 to filter inbound packets on VLAN 20. Because the mask is all zeros, the ACE policy
dictates that a match occurs only when the source address on such packets is identical to the address configured in the ACE.

Inbound Packet “A” On VLAN 20
- Destination Address: 10.35.248.184
- Source Address: 10.28.252.117

Inbound Packet “B” On VLAN 20
- Destination Address: 10.35.248.184
- Source Address: 10.28.252.120

Examples Allowing Multiple IPv4 Addresses. Table 9-2 provides examples of how to apply masks to meet various filtering requirements.

<table>
<thead>
<tr>
<th>Address in the ACE</th>
<th>Mask</th>
<th>Policy for a Match Between a Packet and the ACE</th>
<th>Allowed Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: 10.38.252.195</td>
<td>0.0.0.255</td>
<td>Exact match in first three octets only.</td>
<td>10.38.252.&lt; 0-255 &gt;</td>
</tr>
<tr>
<td>B: 10.38.252.195</td>
<td>0.0.7.255</td>
<td>Exact match in the first two octets and the leftmost five bits (248) of the third octet.</td>
<td>10.38.&lt; 248-255 &gt;.&lt; 0-255 &gt;</td>
</tr>
<tr>
<td>C: 10.38.252.195</td>
<td>0.0.0.0</td>
<td>Exact match in all octets.</td>
<td>10.38.252.195</td>
</tr>
<tr>
<td>D: 10.38.252.195</td>
<td>0.15.255.255</td>
<td>Exact match in the first octet and the leftmost four bits of the second octet.</td>
<td>10.&lt; 32-47 &gt;.&lt; 0-255 &gt;.&lt;0-255&gt;</td>
</tr>
</tbody>
</table>
IPv4 Access Control Lists (ACLs)
Planning an ACL Application

Table 9-3. Mask Effect on Selected Octets of the IPv4 Addresses in Table 9-2

<table>
<thead>
<tr>
<th>Addr</th>
<th>Octet</th>
<th>Mask</th>
<th>Octet Range</th>
<th>128</th>
<th>64</th>
<th>32</th>
<th>16</th>
<th>8</th>
<th>4</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>3</td>
<td>0</td>
<td>all bits</td>
<td>252</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>3</td>
<td>7</td>
<td>last 3 bits</td>
<td>248-255</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>C</td>
<td>4</td>
<td>0</td>
<td>all bits</td>
<td>195</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>D</td>
<td>2</td>
<td>15</td>
<td>last 4 bits</td>
<td>32-47</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

*Shaded areas indicate bit settings that must be an exact match.*

If there is a match between the policy in the ACE and the IPv4 address in a packet, then the packet is either permitted or denied, according to how the ACE is configured. If there is not a match, the next ACE in the ACL is then applied to the packet. The same operation applies to a destination IPv4 address (DA) used in an extended ACE. (Where an ACE includes both source and destination addresses, there is one address/ACL-mask pair for the source address, and another address/ACL-mask pair for the destination address. See “Configuring and Assigning an IPv4 ACL” on page 9-31.)

**CIDR Notation.** For information on using CIDR notation to specify ACL masks, refer to “Using CIDR Notation To Enter the IPv4 ACL Mask” on page 9-40.
Configuring and Assigning an IPv4 ACL

### Overview

#### General Steps for Implementing ACLs

1. Configure one or more ACLs. This creates and stores the ACL(s) in the switch configuration.
2. Assign an ACL.

---

**Caution Regarding the Use of IPv4 Source Routing**

IPv4 source routing is enabled by default on the switch and can be used to override ACLs. For this reason, if you are using ACLs to enhance network security, the recommended action is to disable source routing on the switch. To do so, execute `no ip source-route`.
Options for Permit/Deny Policies

The permit or deny policy for IPv4 traffic you want to filter can be based on source address alone, or on source address plus other IPv4 factors.

- **Standard ACL**: Uses only a packet's source IPv4 address as a criterion for permitting or denying the packet. For a standard ACL ID, use either a unique numeric string in the range of 1-99 or a unique name string of up to 64 alphanumeric characters.

- **Extended ACL**: Offers the following criteria as options for permitting or denying a packet:
  - source IPv4 address
  - destination IPv4 address
  - IPv4 protocol options:
    - Any IPv4 traffic
    - Any traffic of a specific IPv4 protocol type (0-255)
    - Any TCP traffic (only) for a specific TCP port or range of ports, including optional control of connection traffic based on whether the initial request should be allowed
    - Any UDP traffic (only) or UDP traffic for a specific UDP port
    - Any ICMP traffic (only) or ICMP traffic of a specific type and code
    - Any IGMP traffic (only) or IGMP traffic of a specific type
    - Any of the above with specific precedence and/or ToS settings

For an extended ACL ID, use either a unique number in the range of 100-199 or a unique name string of up to 64 alphanumeric characters.

Carefully plan ACL applications before configuring specific ACLs. For more on this topic, refer to “Planning an ACL Application” on page 9-21.

ACL Configuration Structure

After you enter an ACL command, you may want to inspect the resulting configuration. This is especially true where you are entering multiple ACEs into an ACL. Also, it is helpful to understand the configuration structure when using later sections in this chapter.

The basic ACL structure includes four elements:

1. **ACL identity and type**: This identifies the ACL as **standard** or **extended** and shows the ACL name or number.
2. Optional **remark** entries.
3. One or more deny/permit list entries (ACEs): One entry per line.

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Standard or Extended</td>
</tr>
<tr>
<td>Identifier</td>
<td>• Alphanumeric; Up to 64 Characters, Including Spaces</td>
</tr>
<tr>
<td></td>
<td>• Numeric: 1 - 99 (Standard) or 100 - 199 (Extended)</td>
</tr>
<tr>
<td>Remark</td>
<td>Allows up to 100 alphanumeric characters, including blank spaces. (If</td>
</tr>
<tr>
<td></td>
<td>any spaces are used, the remark must be enclosed in a pair of single</td>
</tr>
<tr>
<td></td>
<td>or double quotes.) A remark is associated with a particular ACE</td>
</tr>
<tr>
<td></td>
<td>and will have the same sequence number as the ACE. (One remark is</td>
</tr>
<tr>
<td></td>
<td>allowed per ACE.) Refer to “Attaching a Remark to an ACE” on page</td>
</tr>
<tr>
<td></td>
<td>9-78.</td>
</tr>
<tr>
<td>Maximum ACEs Per per</td>
<td>The upper limit on ACEs supported by the switch depends on the</td>
</tr>
<tr>
<td>Switch</td>
<td>concurrent resource usage by configured ACL, QoS, IDM, Mirroring, and</td>
</tr>
<tr>
<td></td>
<td>other features. Refer to “Monitoring Shared Resources” on page 9-97.</td>
</tr>
</tbody>
</table>

4. Implicit Deny: Where an ACL is in use, it denies any packets that do not have a match with the ACEs explicitly configured in the list. The Implicit Deny does not appear in ACL configuration listings, but always functions when the switch uses an ACL to filter packets. (You cannot delete the Implicit Deny, but you can supersede it with a permit any or permit ip any any statement.)

Standard ACL Structure

Individual ACEs in a standard ACL include only a permit/deny statement, the source addressing, and an optional log command (available with “deny” statements).

```
ip access-list standard < identifier >
[ [ seq-# ] remark < remark-str > ]
< permit | deny > < SA > [ log ]
  
  
  < Implicit Deny >
exit
```

Figure 9-6. Example of the General Structure for a Standard ACL
For example, figure 9-7 shows how to interpret the entries in a standard ACL.

```plaintext
HP Switch(Config)# show running
.
.
.
ip access-list standard "Sample-List"
 10 deny 10.28.150.77 0.0.0.0 log
 20 permit 10.28.150.1 0.0.0.255
exit
```

Figure 9-7. Example of a Displayed Standard ACL Configuration with Two ACEs

Extended ACL Configuration Structure

Individual ACEs in an extended ACL include:

- A permit/deny statement
- Source and destination IPv4 addressing
- Choice of IPv4 criteria, including optional precedence and ToS
- Optional ACL `log` command (for `deny` entries)
- Optional remark statements
IPv4 Access Control Lists (ACLs)
Configuring and Assigning an IPv4 ACL

```
ip access-list extended <identifier>
[ [ seq-#] remark <remark-str>]
< permit | deny > <ipv4-protocol-type> <SA> <src-acl-mask> <DA> <dest-acl-mask> [log]

   < permit | deny > tcp
       < SA > < src-acl-mask > [ < operator > < port-id > ]
       < DA > < desti-acl-mask > [ < operator > < port-id > ] [log]
       [ established ]

< permit | deny > udp
   < SA > < src-acl-mask > [ < operator > < port-id > ]
   < DA > < dest-acl-mask > [ < operator > < port-id > ] [log]

< permit | deny > icmp
   < SA > < src-acl-mask > < DA > < dest-acl-mask > [ icmp-type ] [log]

< permit | deny > igmp
   < SA > < SA-mask > < DA > < dest-acl-mask > [ igmp-type ] [log]

[ precedence <priority>]
[ tos <tos-setting>]

...< Implicit Deny>
exit
```

Figure 9-8. Example of General Structure Options for an Extended ACL

Note: The optional log function is available only for “deny” ACEs.
IPv4 Access Control Lists (ACLs)
Configuring and Assigning an IPv4 ACL

For example, figure 9-9 shows how to interpret the entries in an extended ACL.

```
HP Switch(config)# show running

Running configuration:

; J9146A Configuration Editor; Created on release #W.14.XX
hostname "HP Switch"
ip access-list extended "Sample-List-1"
  10 permit ip 10.38.130.55 0.0.0.0 10.38.130.240 0.0.0.0
  20 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 23
  30 remark "ALLOWS HTTP FROM SINGLE HOST."
  30 permit tcp 10.38.131.14 0.0.0.0 eq 80 0.0.0.0 255.255.255.255 eq 3871
  40 remark "DENIES HTTP FROM ANY TO ANY."
  40 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80 log
  50 deny udp 10.42.120.19 0.0.0.0 eq 69 10.38.140.44 0.0.0.0 range 3680 3690 log
  60 deny udp 0.0.0.0 255.255.255.255 10.38.99.121 0.0.0.0 log
exit
```

ACL Configuration Factors

The Sequence of Entries in an ACL Is Significant

When the switch uses an ACL to determine whether to permit or deny a packet, it compares the packet to the criteria specified in the individual Access Control Entries (ACEs) in the ACL, beginning with the first ACE in the list and proceeding sequentially until a match is found. When a match is found, the switch applies the indicated action (permit or deny) to the packet. This is significant because, once a match is found for a packet, subsequent ACEs in the same ACL will not be applied to that packet, regardless of whether they match the packet.
IPv4 Access Control Lists (ACLs)
Configuring and Assigning an IPv4 ACL

For example, suppose that you have applied the ACL shown in figure 9-10 to inbound IPv4 traffic on VLAN 1 (the default VLAN):

```
ip access-list extended "Sample-List-2"
10 deny ip 10.28.235.10 0.0.0.0 0.0.0.0 255.255.255.255
20 deny ip 10.28.245.89 0.0.0.0 0.0.0.0 255.255.255.255
30 permit tcp 10.28.18.100 0.0.0.0 10.28.237.1 0.0.0.0
40 deny tcp 10.28.18.100 0.0.0.0 0.0.0.0 255.255.255.255
50 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Table 9-4. Effect of the Above ACL on Inbound IPv4 Traffic in the Assigned VLAN

<table>
<thead>
<tr>
<th>Line #</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>Shows type (extended) and ID (Sample-List-2).</td>
</tr>
<tr>
<td>10</td>
<td>A packet from SA 10.28.235.10 will be denied (dropped). This ACE filters out all packets received from 10.28.235.10. As a result, IPv4 traffic from that device will not be allowed and packets from that device will not be compared against any later entries in the list.</td>
</tr>
<tr>
<td>20</td>
<td>A packet from SA 10.28.245.89 will be denied (dropped). This ACE filters out all packets received from 10.28.245.89. As the result, IPv4 traffic from that device will not be allowed and packets from that device will not be compared against any later entries in the list.</td>
</tr>
<tr>
<td>30</td>
<td>A TCP packet from SA 10.28.18.100 with a DA of 10.28.237.1 will be permitted (forwarded). Since no earlier ACEs in the list have filtered TCP packets from 10.28.18.100 and destined for 10.28.237.1, the switch will use this ACE to evaluate such packets. Any packets that meet this criteria will be forwarded. (Any packets that do not meet this TCP source-destination criteria are not affected by this ACE.)</td>
</tr>
<tr>
<td>40</td>
<td>A TCP packet from source address 10.28.18.100 to any destination address will be denied (dropped). Since, in this example, the intent is to block TCP traffic from 10.28.18.100 to any destination except the destination stated in the ACE at line 30, this ACE must follow the ACE at line 30. (If their relative positions were exchanged, all TCP traffic from 10.28.18.100 would be dropped, including the traffic for the 10.28.18.1 destination.)</td>
</tr>
</tbody>
</table>
IPv4 Access Control Lists (ACLs)
Configuring and Assigning an IPv4 ACL

Allowing for the Implied Deny Function

In any ACL having one or more ACEs there will always be a packet match. This is because the switch automatically applies an Implicit Deny as the last ACE in any ACL. This function is not visible in ACL listings, but is always present. (Refer to figure 9-10.) This means that if you configure the switch to use an ACL for filtering either inbound or outbound IPv4 traffic, any packets not specifically permitted or denied by the explicit entries you create will be denied by the Implicit Deny action. If you want to preempt the Implicit Deny (so that IPv4 traffic not specifically addressed by earlier ACEs in a given ACL will be permitted), insert an explicit permit any (for standard ACLs) or permit ip any any (for extended ACLs) as the last explicit ACE in the ACL.

A Configured ACL Has No Effect Until You Apply It to an Interface

The switch stores ACLs in the configuration file. Thus, until you actually assign an ACL to an interface, it is present in the configuration, but not used (and does not use any of the monitored resources described in the appendix titled “Monitored Resources” in the Management and Configuration Guide for your switch.)

You Can Assign an ACL Name or Number to an Interface Even if the ACL Does Not Exist in the Switch’s Configuration

In this case, if you subsequently create an ACL with that name or number, the switch automatically applies each ACE as soon as you enter it in the running-config file. Similarly, if you modify an existing ACE in an ACL you already applied to an interface, the switch automatically implements the new ACE as soon as you enter it. (See “General ACL Operating Notes” on page 9-96.) The switch allows a maximum of 512 ACLs (IPv4), and determines the total from the number of unique ACL names in the configuration. (For more on this topic, refer to “Monitoring Shared Resources” on page 9-97.)
Using the CLI To Create an ACL

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (standard ACLs)</td>
<td>9-41</td>
</tr>
<tr>
<td>access-list (extended ACLs)</td>
<td>9-50</td>
</tr>
</tbody>
</table>

You can use either the switch CLI or an offline text editor to create an ACL. This section describes the CLI method, which is recommended for creating short ACLs. (To use the offline method, refer to “Creating or Editing ACLs Offline” on page 9-91.)

General ACE Rules

These rules apply to all IPv4 ACEs you create or edit using the CLI:

- Inserting or adding an ACE to an ACL:
  - **Named IPv4 ACLs**: Add an ACE to the end of a named ACE by using the `ip access-list` command to enter the Named ACL (nacl) context and entering the ACE without the sequence number. For example, if you wanted to add a “permit” ACL at the end of a list named “List-1” to allow traffic from the device at 10.10.10.100:

    ```
    HP Switch(config)# ip access-list standard List-1
    HP Switch(config-std-nacl)# permit host 10.10.10.100
    ```

  Insert an ACE anywhere in a named ACL by specifying a sequence number. For example, if you wanted to insert a new ACE as line 15 between lines 10 and 20 in an existing ACL named “List-2” to deny IPv4 traffic from the device at 10.10.10.77:

    ```
    HP Switch(config)# ip access-list standard List-2
    HP Switch(config-std-nacl)# 15 deny host 10.10.10.77
    ```

  - **Numbered IPv4 ACLs**: Add an ACE to the end of a numbered ACL by using the `access-list < 1 - 99 | 100 - 199 >` command. For example, if you wanted to add a “permit” ACE at the end of a list identified with the number “11” to allow IPv4 traffic from the device at 10.10.10.100:

    ```
    HP Switch(config)# access-list 11 permit host 10.10.10.100
    ```
IPv4 Access Control Lists (ACLs)
Configuring and Assigning an IPv4 ACL

To insert an ACE anywhere in a numbered ACL, use the same process as described above for inserting an ACE anywhere in a named ACL. For example, to insert an ACE denying IPv4 traffic from the host at 10.10.10.77 as line 52 in an existing ACL identified (named) with the number 11:

```
HP Switch(config)# ip access-list standard 99
HP Switch(config-std-nacl)# 52 deny host 10.10.10.77
```

Note
After a numbered ACL has been created (using `access-list < 1 - 99 | 100 - 199>`), it can be managed as either a named or numbered ACL, as shown above.

- Deleting an ACE: Enter the ACL context and delete the sequence number for the unwanted ACE. (To view the sequence numbers of the ACEs in a list, use `show access-list < acl-name-str>`.)
- Duplicate ACEs are not allowed in the same ACL. Attempting to enter a duplicate ACE displays the **Duplicate access control entry** message.

Using CIDR Notation To Enter the IPv4 ACL Mask

You can use CIDR (Classless Inter-Domain Routing) notation to enter ACL masks. The switch interprets the bits specified with CIDR notation as the address bits in an ACL and the corresponding address bits in a packet that must match. The switch then converts the mask to inverse notation for ACL use.

### Table 9-5. Examples of CIDR Notation for Masks

<table>
<thead>
<tr>
<th>Address Used In an ACL with CIDR Notation</th>
<th>Resulting ACL Mask</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.38.240.125/15</td>
<td>0.1.255.255</td>
<td>The leftmost 15 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>10.38.240.125/20</td>
<td>0.0.15.255</td>
<td>The leftmost 20 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>10.38.240.125/21</td>
<td>0.0.7.255</td>
<td>The leftmost 21 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>10.38.240.125/24</td>
<td>0.0.0.255</td>
<td>The leftmost 24 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>18.38.240.125/32</td>
<td>0.0.0.0</td>
<td>All bits must match.</td>
</tr>
</tbody>
</table>
# Configuring Standard ACLs

## Table 9-6. Command Summary for Standard ACLs

<table>
<thead>
<tr>
<th>Action</th>
<th>Command(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Standard, <strong>Named</strong> ACL or Add an ACE to the End of an Existing Standard, <strong>Named</strong> ACL</td>
<td>HP Switch(config)# ip access-list standard <code>&lt;name-str&gt;</code></td>
<td>9-43</td>
</tr>
<tr>
<td></td>
<td>HP Switch(config-std-nacl)# `&lt;deny</td>
<td>permit&gt;<code> </code>&lt; any</td>
</tr>
<tr>
<td>Create a Standard, <strong>Numbered</strong> ACL or Add an ACE to the End of an Existing Standard, <strong>Numbered</strong> ACL</td>
<td>HP Switch(config)# access-list <code>&lt;1-99&gt;</code> `&lt;deny</td>
<td>permit&gt;<code> </code>&lt; any</td>
</tr>
<tr>
<td>Use a Sequence Number To Insert an ACE in an ACL</td>
<td>HP Switch(config)# ip access-list standard `&lt;name-str</td>
<td>1-99&gt;`</td>
</tr>
<tr>
<td></td>
<td>HP Switch(config-std-nacl)# `&lt;deny</td>
<td>permit&gt;<code> </code>&lt; any</td>
</tr>
<tr>
<td>Use an ACE's Sequence Number To Delete the ACE from an ACL</td>
<td>HP Switch(config)# ip access-list standard `&lt;name-str</td>
<td>1-99&gt;<code>no</code>&lt;1-2147483647&gt;`</td>
</tr>
<tr>
<td></td>
<td>HP Switch(config-std-nacl)# [remark <code>&lt;remark-str&gt;</code></td>
<td>no <code>&lt;1-2147483647&gt;</code> remark ]</td>
</tr>
<tr>
<td>Resequence the ACEs in an ACL</td>
<td>HP Switch(config)# ip access-list resequence `&lt;name-str</td>
<td>1-99&gt;<code> </code>&lt;1-2147483647&gt;`</td>
</tr>
<tr>
<td>Enter or Remove a Remark from an ACL</td>
<td>HP Switch(config)# ip access-list standard `&lt;name-str</td>
<td>1-99&gt;<code>[remark</code>&lt;remark-str&gt;`</td>
</tr>
<tr>
<td></td>
<td>HP Switch(config-std-nacl)# [no] access-list <code>&lt;1-99&gt;</code> remark ]</td>
<td>9-78</td>
</tr>
<tr>
<td>Delete an ACL</td>
<td>HP Switch(config)# no ip access-list standard `&lt;name-str</td>
<td>1-99&gt;`</td>
</tr>
<tr>
<td></td>
<td>For numbered, standard ACLs only, the following remark commands can be substituted for the above:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP Switch(config)# access-list <code>&lt;1-99&gt;</code> remark <code>&lt;remark-str&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP Switch(config)# [no] access-list <code>&lt;1-99&gt;</code> remark ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For numbered, standard ACLs only, the following command can be substituted for the above:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP Switch(config)# access-list <code>&lt;1-99&gt;</code> remark <code>&lt;remark-str&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

<sup>1</sup>The mask can be in either dotted-decimal notation (such as 0.0.15.255) or CIDR notation (such as /20).
<sup>2</sup>The [ log ] function applies only to “deny” ACLs, and generates a message only when there is a “deny” match.
A standard ACL uses only source IPv4 addresses in its ACEs. This type of ACE is useful when you need to:

- Permit or deny any IPv4 traffic based on source address only.
- Quickly control the IPv4 traffic from a specific address. This allows you to isolate IPv4 traffic problems generated by a specific device, group of devices, or a subnet threatening to degrade network performance. This gives you an opportunity to troubleshoot without sacrificing performance for users outside of the problem area.

A named, standard ACL is identified by an alphanumeric string of up to 64 characters and is created by entering the Named ACL (nacl) context. A numbered, standard ACL is identified by a number in the range of 1 - 99 and is created without having to leave the global config context. Note that the CLI command syntax for creating a named ACL differs from the command syntax for creating a numbered ACL. For example, the first pair of entries below illustrate how to create (or enter) a named, standard ACL and enter an ACE. The next entry illustrates creating a numbered, standard ACL with the same ACE.

```
HP Switch(config)# ip access-list standard Test-List
HP Switch(config-std-nacl)# permit host 10.10.10.147
```

```
HP Switch(config)# access-list 1 permit host 10.10.10.147
```

Note that once a numbered ACL has been created, it can be accessed using the named ACL method. This is useful if it becomes necessary to edit a numbered ACL by inserting or removing individual ACEs. (Inserting or deleting an ACE is done by sequence number, and requires the Named ACL (nacl) context.) The switch allows a maximum of 512 unique ACL identities. (For more on this topic, refer to “Monitoring Shared Resources” on page 9-97.)

**Note**

For a summary of standard ACL commands, refer to table 9-6 on page 9-41. For a summary of all IPv4 ACL commands, refer to tables 9-1 and 9-2 on pages 9-4 and 9-5.
Configuring Named, Standard ACLs

This section describes the commands for performing the following:

- creating and/or entering the context of a named, standard ACL
- appending an ACE to the end of an existing list or entering the first ACE in a new list

For other IPv4 ACL topics, refer to the following:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuring numbered, standard ACLs</td>
<td>9-46</td>
</tr>
<tr>
<td>configuring named, extended ACLs</td>
<td>9-52</td>
</tr>
<tr>
<td>configuring numbered, extended ACLs</td>
<td>9-62</td>
</tr>
<tr>
<td>applying or removing an ACL on an interface</td>
<td>9-70</td>
</tr>
<tr>
<td>deleting an ACL</td>
<td>9-71</td>
</tr>
<tr>
<td>editing an ACL</td>
<td>9-72</td>
</tr>
<tr>
<td>sequence numbering in ACLs</td>
<td>9-73</td>
</tr>
<tr>
<td>including remarks in an ACL</td>
<td>9-78</td>
</tr>
<tr>
<td>displaying ACL configuration data</td>
<td>9-82</td>
</tr>
<tr>
<td>creating or editing ACLs offline</td>
<td>9-91</td>
</tr>
<tr>
<td>enabling ACL “Deny” logging</td>
<td>9-93</td>
</tr>
</tbody>
</table>

**Entering the IPv4 “Named ACL” (nacl) Context.** This command is a prerequisite to entering or editing ACEs in a named ACL.

**Syntax:**

```
ip access-list standard < name-str >
```

Places the CLI in the “Named ACL” (nacl) context specified by the `< name-str >` alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.

* `< name-str >`: Specifies an identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: “*Accounting ACL*”.

Refer also to table 9-6 on page 9-41.
IPv4 Access Control Lists (ACLs)
Configuring Standard ACLs

Configuring ACEs in an Named, Standard ACL. Configuring ACEs is done after using the `ip access-list standard < name-str >` command described above to enter the “Named ACL” (nacl) context of an access list. For a standard ACL syntax summary, refer to table 9-6 on page 9-41.

Syntax: `< deny | permit >
       < any | host < SA > | SA <mask | SA/ mask-length >> [log]

Executing this command appends the ACE to the end of the list of ACEs in the current ACL. In the default ACL configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using `resequence` (page 9-77).

Note: To insert a new ACE between two existing ACEs, precede `deny` or `permit` with an appropriate sequence number. (Refer to “Inserting an ACE in an Existing ACL” on page 9-74.)

< deny | permit >

For named ACLs, used in the “Named ACL” (nacl) context to configure an ACE. Specifies whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.

< any | host < SA > | SA < mask > | SA/ mask-length >

Defines the source IPv4 address (SA) a packet must carry for a match with the ACE.

- **any** — Allows IPv4 packets from any SA.
- **host < SA >** — Specifies only packets having `< SA >` as the source. Use this criterion when you want to match the IPv4 packets from a single source address.
- **SA < mask >** or **SA/ mask-length** — Specifies packets received from either a subnet or a group of IPv4 addresses. The mask format can be in either dotted-decimal format or CIDR format (number of significant bits). (Refer to “Using CIDR Notation To Enter the IPv4 ACL Mask” on page 9-40).

**Mask Application:** The mask is applied to the IPv4 address in the ACE to define which bits in a packet’s SA must exactly match the SA configured in the ACE and which bits need not match. For example: 10.10.10.1/24 and 10.10.10.0 0.0.0.255 both define any address in the range of 10.10.10.(1 - 255).

Note: Specifying a group of contiguous addresses may require more than one ACE. For more on how masks operate, refer to “How an ACE Uses a Mask To Screen Packets for Matches” on page 9-25.
IPv4 Access Control Lists (ACLs)
Configuring Standard ACLs

Example of Creating and Listing a Standard, Named ACL. This example illustrates how to create a standard, named ACL with several ACEs. This example creates an ACL that:

1. permits IPv4 traffic from a host with the address of 10.10.10.104
2. creates another ACE that blocks all other IPv4 traffic from the same subnet
3. allows all other IPv4 traffic

```
HP Switch(config)# ip access-list standard Sample-List
HP Switch(config-std-nacl)# permit host 10.10.10.104
HP Switch(config-std-nacl)# deny 10.10.10.1/24 log
HP Switch(config-std-nacl)# permit any
HP Switch(config-std-nacl)# exit
HP Switch(config)# _
```

Figure 9-11. Example of Commands Used To Create an Standard, Named ACL
Creating Numbered, Standard ACLs

Use the following general steps to create or add to a numbered, standard ACL:

1. Create a numbered, standard ACL by entering the first ACE in the list.
2. Append a new ACE to the end of an existing, standard ACL.

This section describes the commands for performing these steps. For other IPv4 ACL topics, refer to the following:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuring named, standard ACLs</td>
<td>9-43</td>
</tr>
<tr>
<td>configuring named, extended ACLs</td>
<td>9-52</td>
</tr>
<tr>
<td>configuring numbered, extended ACLs</td>
<td>9-62</td>
</tr>
<tr>
<td>applying or removing an ACL on an interface</td>
<td>9-70</td>
</tr>
<tr>
<td>deleting an ACL</td>
<td>9-71</td>
</tr>
<tr>
<td>editing an ACL</td>
<td>9-72</td>
</tr>
<tr>
<td>sequence numbering in ACLs</td>
<td>9-73</td>
</tr>
<tr>
<td>including remarks in an ACL</td>
<td>9-78</td>
</tr>
<tr>
<td>displaying ACL configuration data</td>
<td>9-82</td>
</tr>
<tr>
<td>creating or editing ACLs offline</td>
<td>9-91</td>
</tr>
<tr>
<td>enabling ACL “Deny” logging</td>
<td>9-93</td>
</tr>
</tbody>
</table>

---

Note that each ACE is automatically assigned a sequence number.
Creating or Adding to an Standard, Numbered ACL. This command is an alternative to using `ip access-list standard < name-str >` and does not use the “Named ACL” (nacl) context. For a standard ACL syntax summary, refer to table 9-6 on page 9-41.

**Syntax:**

```
access-list < 1-99 > < deny | permit > < any | host < SA > | SA < mask | SA/mask-length >> [log]
```

Appends an ACE to the end of the list of ACEs in the current IPv4 standard, numbered ACL. If the ACL does not already exist, creates both the ACL and its first ACE. In the default configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using `resequence` (page 9-77).

**Note:** To insert a new ACE between two existing ACEs in a standard, numbered ACL:

a. Use `ip access list extended < 1 - 99 >` to open the ACL as a named ACL.

b. Enter the desired sequence number along with the ACE keywords and variables you want.

(After a numbered ACL has been created, it can be managed as either a named or numbered ACL. Refer to the “Numbered ACLs” list item on page 9-39.)

< 1-99 >

Specifies the ACL identifier as a number. The switch interprets an ACL with a value in this range as a standard ACL (which filters all IPv4 traffic on the basis of SA). (To create a standard access list with an alphanumeric name (`name-str`) instead of a number, refer to “Configuring Named, Standard ACLs” on page 9-43.)

< deny | permit >

Specifies whether the ACE denies or permits a packet matching the criteria in the ACE, as described next.
Configuring Standard ACLs

< any | host < SA > | SA < mask | SA/mask-length >>

Defines the source IPv4 address (SA) a packet must carry for a match with the ACE.

- **any** — Allows IPv4 packets from any SA.
- **host < SA >** — Specifies only packets having < SA > as the source. Use this criterion when you want to match only the IPv4 packets from a single SA.
- **SA < mask > or SA/mask-length** — Specifies packets received from an SA, where the SA is either a subnet or a group of IPv4 addresses. The mask format can be in either dotted-decimal format or CIDR format (number of significant bits). (Refer to “Using CIDR Notation To Enter the IPv4 ACL Mask” on page 9-40).

**SA Mask Application:** The mask is applied to the SA in the ACE to define which bits in a packet’s SA must exactly match the SA configured in the ACL and which bits need not match.

**Example:** `10.10.10.1/24` and `10.10.10.1 0.0.0.255` both define any address in the range of 10.10.10.(1 - 255).

**Note:** Specifying a group of contiguous addresses may require more than one ACE. For more on how masks operate in ACLs, refer to “How an ACE Uses a Mask To Screen Packets for Matches” on page 9-25.
Example of Creating and Viewing a Standard ACL. This example creates a standard, numbered ACL with the same ACE content as shown in Figure 9-11 on page 9-45.

```
HP Switch(config)# access-list 17 permit host 10.10.10.104
HP Switch(config)# access-list 17 deny 10.10.10.1/24 log
HP Switch(config)# access-list 17 permit any
HP Switch(config)# show access-list 17

Access Control Lists

   Name: 17
   Type: Standard
   Applied: No

SEQ   Entry
----------------------------------------------------------
   10   Action: permit
         IP : 10.10.10.104   Mask: 0.0.0.0
   20   Action: deny (log)
         IP : 10.10.10.1     Mask: 0.0.0.255
   30   Action: permit
         IP : 0.0.0.0        Mask: 255.255.255.255

Note that each ACE is automatically assigned a sequence number.
```

Figure 9-13. Standard, Numbered ACL with the Same ACEs as the Standard, Named ACL in Figure 9-11
IPv4 Access Control Lists (ACLs)
Configuring Extended ACLs

Configuring Extended ACLs

Table 9-7. Command Summary for Extended ACLs

<table>
<thead>
<tr>
<th>Action</th>
<th>Command(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an Extended, Named ACL or Add an ACE to the End of an Existing, Extended ACL</td>
<td>HP Switch(config)# ip access-list extended &lt; name-str</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100-199 &gt;</td>
</tr>
<tr>
<td></td>
<td>HP Switch(config-std-nacl)# &lt; deny</td>
<td>permit &gt;</td>
</tr>
<tr>
<td></td>
<td>&lt; ip</td>
<td>ip-protocol</td>
</tr>
<tr>
<td></td>
<td>&lt; any</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>&lt; any</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>[ tcp</td>
<td>udp ]</td>
</tr>
<tr>
<td></td>
<td>&lt; any</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>[ comparison-operator &lt; value &gt; ]</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td>&lt; any</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>[ comparison-operator &lt; value &gt; ]</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td>[established]</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td>&lt; igmp &gt;</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td>&lt; any</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>&lt; any</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>[ igmp-packet-type ]</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td>&lt; icmp &gt;</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td>&lt; any</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>&lt; any</td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>[ [0 - 255]</td>
<td>[0 - 255] ]</td>
</tr>
<tr>
<td></td>
<td>[precedence &lt; priority &gt;]</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td>[tos &lt; tos- setting &gt;]</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td>[log] 2</td>
<td>9-52</td>
</tr>
<tr>
<td></td>
<td>Create an Extended, Numbered ACL or Add an ACE to the End of an Existing, Numbered ACL</td>
<td>HP Switch(config)# ip access-list extended &lt; 100-199 &gt;</td>
</tr>
<tr>
<td></td>
<td>HP Switch(config-ext-nacl)# &lt; deny</td>
<td>permit &gt;</td>
</tr>
<tr>
<td></td>
<td>&lt; ip-options tcp/udp-options igmp-options icmp-options &gt;</td>
<td>9-62</td>
</tr>
<tr>
<td></td>
<td>[log] 2</td>
<td>9-62</td>
</tr>
<tr>
<td></td>
<td>[precedence &lt; priority &gt;]</td>
<td>9-62</td>
</tr>
<tr>
<td></td>
<td>[tos &lt; tos- setting &gt;]</td>
<td>9-62</td>
</tr>
<tr>
<td><strong>Note:</strong> Uses the same IP, TCP/UDP, IGMP, and ICMP options as shown above for “Create an Extended, Named ACL”.</td>
<td>9-62</td>
<td></td>
</tr>
<tr>
<td>Insert an ACE by Assigning a Sequence Number</td>
<td>HP Switch(config)# ip access-list extended &lt; name-str</td>
<td>9-74</td>
</tr>
<tr>
<td></td>
<td>HP Switch(config-ext-nacl)# 1-2147483647 &lt; deny</td>
<td>permit &gt;</td>
</tr>
<tr>
<td></td>
<td>Uses the options shown above for “Create an Extended, Named ACL”.</td>
<td>9-74</td>
</tr>
<tr>
<td>Use Sequence Number To Delete an ACE</td>
<td>HP Switch(config)# ip access-list extended &lt; name-str</td>
<td>9-76</td>
</tr>
<tr>
<td></td>
<td>HP Switch(config-std-nacl)# no &lt; 1-2147483647 &gt;</td>
<td>9-76</td>
</tr>
<tr>
<td>Resequence the ACEs in an ACL</td>
<td>HP Switch(config)# ip access-list resequence &lt; name-str</td>
<td>9-77</td>
</tr>
<tr>
<td></td>
<td>HP Switch(config-ext-nacl)# 1-2147483647 &lt; 1-2147483646 &gt;</td>
<td>9-77</td>
</tr>
</tbody>
</table>

1The mask can be in either dotted-decimal notation (such as 0.0.15.255) or CIDR notation (such as /20).
2The [ log ] function applies only to “deny” ACLs, and generates a message only when there is a “deny” match.

Table continues on the next page.
IPv4 Access Control Lists (ACLs)
Configuring Extended ACLs

Standard ACLs use only source IPv4 addresses for filtering criteria, extended ACLs use multiple filtering criteria. This enables you to more closely define your IPv4 packet-filtering. Extended ACLs enable filtering on the following:

- Source and destination IPv4 addresses (required), in one of the following options:
  - specific host
  - subnet or group of addresses
  - any address
- choice of any IPv4 protocol
- optional packet-type criteria for IGMP and ICMP traffic
- optional source and/or destination TCP or UDP port, with a further option for comparison operators and (for TCP) an option for establishing connections
- filtering for TCP traffic based on whether the subject traffic is initiating a connection ("established" option)
- optional IP precedence and ToS criteria

The switch allows up to 512 ACLs, and determines the total from the number of unique identifiers in the configuration. For example, configuring two ACLs results in an ACL total of two, even if neither is assigned to an interface. If you then assign a nonexistent ACL to an interface, the new ACL total is three, because the switch now has three unique ACL names in its configuration. (For more on ACL limits, refer to “Monitoring Shared Resources” on page 9-97.)
Configuring Named, Extended ACLs

For a match to occur with an ACE in an extended ACL, a packet must have the source and destination address criteria specified by the ACE, as well as any IPv4 protocol-specific criteria included in the command.

Use the following general steps to create or add to a named, extended ACL:

1. Create and/or enter the context of a named, extended ACL.
2. Enter the first ACE in a new, extended ACL or append an ACE to the end of an existing, extended ACL.

This section describes the commands for performing these steps. For other ACL topics, refer to the following:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuring named, standard ACLs</td>
<td>9-43</td>
</tr>
<tr>
<td>configuring numbered, standard ACLs</td>
<td>9-46</td>
</tr>
<tr>
<td>configuring numbered, extended ACLs</td>
<td>9-62</td>
</tr>
<tr>
<td>applying or removing an ACL on an interface</td>
<td>9-70</td>
</tr>
<tr>
<td>deleting an ACL</td>
<td>9-71</td>
</tr>
<tr>
<td>editing an ACL</td>
<td>9-72</td>
</tr>
<tr>
<td>sequence numbering in ACLs</td>
<td>9-73</td>
</tr>
<tr>
<td>including remarks in ACL</td>
<td>9-78</td>
</tr>
<tr>
<td>displaying ACL configuration data</td>
<td>9-82</td>
</tr>
<tr>
<td>creating or editing ACLs offline</td>
<td>9-91</td>
</tr>
<tr>
<td>enabling ACL “Deny” logging</td>
<td>9-93</td>
</tr>
</tbody>
</table>
Creating a Named, Extended ACL and/or Entering the “Named ACL” (nacl) Context. This command is a prerequisite to entering or editing ACEs in a named, extended ACL. (For a summary of the extended ACL syntax options, refer to table 9-7 on page 9-50.)

Syntax:  ip access-list extended < name-str >

Places the CLI in the “Named ACL” (nacl) context specified by the < name-str > alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.

< name-str >: Specifies an alphanumeric identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: “Accounting ACL”. You can also use this command to access an existing, numbered ACL. Refer to “Using the CLI To Edit ACLs” on page 9-72

| HP Switch(config)# ip access-list extended Sample-List  
| HP Switch(config-ext-nacl)# |

Figure 9-14. Example of Entering the Named ACL Context
Configure ACEs in a Named, Extended ACL and/or Enter the “Named ACL” (nacl) Context. Configuring ACEs is done after using the `ip access-list standard < name-str >` command described on page 9-53 to enter the “Named ACL” (nacl) context of an ACL. For an extended ACL syntax summary, refer to table 9-7 on page 9-50.

**Syntax:**
```
< deny | permit > < ip | ip-protocol | ip-protocol-nbr >
  
  < any | host < SA > | SA/ mask-length | SA < mask >>
  < any | host < DA > | DA/ mask-length | DA < mask >>
  [ precedence | [ tos ] | [ log ]
```

Appends an ACE to the end of the list of ACEs in the current ACL. In the default configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using `resequence` (page 9-77).

**Note:** To insert a new ACE between two existing ACEs in an extended, named ACL, precede `deny` or `permit` with an appropriate sequence number along with the ACE keywords and variables you want. (Refer to “Inserting an ACE in an Existing ACL” on page 9-74.)

For a match to occur, a packet must have the source and destination addressing criteria specified in the ACE, as well as:

- the protocol-specific criteria configured in the ACE, including any included, optional elements (described later in this section)
- any (optional) precedence and/or ToS settings configured in the ACE

For named ACLs, these keywords are used in the “Named ACL” (nacl) context to specify whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.
Configuring Extended ACLs

### IPv4 Access Control Lists (ACLs)

- **< ip | ip-protocol | ip-protocol-nbr >**
  
  **Used after** deny **or** permit **to specify the packet protocol type required for a match.** An extended ACL must include one of the following:

  - **ip** — any IPv4 packet.
  - **ip-protocol** — any one of the following IPv4 protocol names:
    - ip-in-ip
    - ipv6-in-ip
    - gre
    - esp
    - ah
    - ospf
    - pim
    - vrrp
    - sctp
    - tcp*
    - udp*
    - icmp*
    - igmp*
  - **ip-protocol-nbr** — the protocol number of an IPv4 packet type, such as “8” for Exterior Gateway Protocol or 121 for Simple Message Protocol. (For a listing of IPv4 protocol numbers and their corresponding protocol names, refer to the IANA “Protocol Number Assignment Services” at www.iana.com.) (Range: 0 - 255)

  * For TCP, UDP, ICMP, and IGMP, additional criteria can be specified, as described on pages 9-58 through 9-62.

- **< any | host < SA > | SA < mask > | SA/ mask-length >**
  
  **This is the first instance of IPv4 addressing in an extended ACE.** It follows the protocol specifier and defines the source address (SA) a packet must carry for a match with the ACE.

  - **any** — Allows IPv4 packets from any SA.
  - **host < SA >** — Specifies only packets having a single address as the SA. Use this criterion when you want to match only the IPv4 packets from a single SA.
  - **SA < mask >** or **SA/ mask-length** — Specifies packets received from an SA, where the SA is either a subnet or a group of addresses. The mask can be in either dotted-decimal format or CIDR format (number of significant bits). Refer to “Using CIDR Notation To Enter the IPv4 ACL Mask” on page 9-40.

  **SA Mask Application:** The mask is applied to the SA in the ACL to define which bits in a packet’s SA must exactly match the SA configured in the ACL and which bits need not match.

  **Example:** 10.10.10.1/24 and 10.10.10.1 0.0.0.255 both define any address in the range of 10.10.10.(1 - 255).

  **Note:** Specifying a group of contiguous addresses may require more than one ACE. For more on how masks operate in ACLs, refer to “How an ACE Uses a Mask To Screen Packets for Matches” on page 9-25.
IPv4 Access Control Lists (ACLs)
Configuring Extended ACLs

< any | host < DA > | DA/mask-length | DA/ < mask >>

This is the second instance of IPv4 addressing in an extended ACE. It follows the first (SA) instance, described earlier, and defines the destination address (DA) that a packet must carry in order to have a match with the ACE.

- **any** — Allows routed IPv4 packets to any DA.
- **host < DA >** — Specifies only packets having DA as the destination address. Use this criterion when you want to match only the IPv4 packets for a single DA.
- **DA/mask-length or DA < mask >** — Specifies packets intended for a destination address, where the address is either a subnet or a group of addresses. The mask format can be in either dotted-decimal format or CIDR format (number of significant bits). Refer to “Using CIDR Notation To Enter the IPv4 ACL Mask” on page 9-40.

**DA Mask Application:** The mask is applied to the DA in the ACL to define which bits in a packet’s DA must exactly match the DA configured in the ACL and which bits need not match. See also the above example and note.

[ precedence < 0 - 7 | precedence-name > ]

This option can be used after the DA to cause the ACE to match packets with the specified IP precedence value. Values can be entered as the following IP precedence numbers or alphanumeric names:

- 0 or routine
- 1 “ priority
- 2 “ immediate
- 3 “ flash
- 4 “ flash-override
- 5 “ critical
- 6 “ internet (for internetwork control)
- 7 “ network (for network control)

**Note:** The precedence criteria described in this section are applied in addition to any other selection criteria configured in the same ACE.
[tos < tos-setting>]

This option can be used after the DA to cause the ACE to match packets with the specified Type-of-Service (ToS) setting. ToS values can be entered as the following numeric settings or, in the case of 0, 2, 4, and 8, as alphanumeric names:

0 or normal
2 " max-reliability
4 " max-throughput
6
8 " minimize-delay
10
12
14

Note: The ToS criteria in this section are applied in addition to any other criteria configured in the same ACE.

[log]

This option can be used after the DA to generate an Event Log message if:

- The action is deny. (Not applicable to permit.)
- There is a match.
- ACL logging is enabled. (Refer to “Enabling ACL Logging on the Switch” on page 9-95.)
Options for TCP and UDP Traffic in Extended ACLs. An ACE designed to permit or deny TCP or UDP traffic can optionally include port number criteria for either the source or destination, or both. Use of TCP criteria also allows the established option for controlling TCP connection traffic. (For a summary of the extended ACL syntax options, refer to table 9-7 on page 9-50.)

**Syntax:**

\[
\text{\textless\; deny | permit \; \textgreater\; <\; tcp | udp \; \textgreater}
\]\n
\[
\text{\textless\; SA \; \textgreater\; [\text{\textit{comparison-operator\; <\; tcp/udp-src-port\; >}}]}
\]\n
\[
\text{\textless\; DA \; \textgreater\; [\text{\textit{comparison-operator\; <\; tcp/udp-src-port\; >\; [\textit{established}\;]}}]
\text{\textit{comparison-operator\; <\; tcp/udp-dest-port\; >\;]}}
\]

In an extended ACL using either tcp or udp as the packet protocol type, you can optionally use TCP or UDP source and/or destination port numbers or ranges of numbers to further define the criteria for a match. For example:

\[
\#\text{deny tcp host 10.20.10.17 eq 23 host 10.20.10.155 established}
\]

\[
\#\text{permit tcp host 10.10.10.100 host 10.20.10.17 eq telnet}
\]

\[
\#\text{deny udp 10.30.10.1/24 host 10.20.10.17 range 161 162 [\text{\textit{comparison-operator\; <\; tcp/udp-src-port\; >}}]}
\]

To specify a TCP or UDP source port number in an ACE, (1) select a comparison operator from the following list and (2) enter the port number or a well-known port name.

**Comparison Operators:**

- `eq < tcp/udp-port-nbr>` — “Equal To”; to have a match with the ACE entry, the TCP or UDP source port number in a packet must be equal to `< tcp/udp-port-nbr >`.
- `gt < tcp/udp-port-nbr>` — “Greater Than”; to have a match with the ACE entry, the TCP or UDP source port number in a packet must be greater than `< tcp/udp-port-nbr >`.
- `lt < tcp/udp-port-nbr>` — “Less Than”; to have a match with the ACE entry, the TCP or UDP source port number in a packet must be less than `< tcp/udp-port-nbr >`.
- `neq < tcp/udp-port-nbr>` — “Not Equal”; to have a match with the ACE entry, the TCP or UDP source port number in a packet must not be equal to `< tcp/udp-port-nbr >`.
- `range < start-port-nbr > < end-port-nbr >` — For a match with the ACE entry, the TCP or UDP source port number in a packet must be in the range `< start-port-nbr > < end-port-nbr >`.
IPv4 Access Control Lists (ACLs)
Configuring Extended ACLs

Port Number or Well-Known Port Name:
Use the TCP or UDP port number required by your application. The switch also accepts these well-known TCP or UDP port names as an alternative to their port numbers:
- **TCP**: bgp, dns, ftp, http, imap4, ldap, nntp, pop2, pop3, smtp, ssl, telnet
- **UDP**: bootpc, bootps, dns, ntp, radius, radius-old, rip, snmp, snmp-trap, tftp

To list the above names, press the [Shift] [?] key combination after entering an operator. For a comprehensive listing of port numbers, visit www.iana.org/assignments/port-numbers.

```
[comparison-operator < tcp-dest-port>] [established]
[comparison-operator < udp-dest-port>]
```

This option, if used, is entered immediately after the `< DA >` entry. To specify a TCP or UDP port number, (1) select a comparison operator and (2) enter the port number or a well-known port name.

Comparison Operators and Well-Known Port Names — These are the same as are used with the TCP/UDP source-port options, and are listed earlier in this command description.

**[established]** — This option applies only where TCP is the configured protocol type. It blocks the synchronizing packet associated with establishing a TCP connection in one direction on a VLAN while allowing all other IPv4 traffic for the same type of connection in the opposite direction. For example, a Telnet connect requires TCP traffic to move both ways between a host and the target device. Simply applying a Deny to inbound Telnet traffic on a VLAN would prevent Telnet sessions in either direction because responses to outbound requests would be blocked. However, by using the **established** option, inbound Telnet traffic arriving in response to outbound Telnet requests would be permitted, but inbound Telnet traffic trying to establish a connection would be denied.
Options for ICMP Traffic in Extended ACLs. This option is useful where it is necessary to permit some types of ICMP traffic and deny other types, instead of simply permitting or denying all types of ICMP traffic. That is, an ACE designed to permit or deny ICMP traffic can optionally include an ICMP type and code value to permit or deny an individual type of ICMP packet while not addressing other ICMP traffic types in the same ACE. As an optional alternative, the ACE can include the name of an ICMP packet type. (For a summary of the extended ACL syntax options, refer to table 9-7 on page 9-50.)

**Syntax:**

```
< deny | permit > icmp < SA > < DA > [ icmp-type [ icmp-code ] ]
< deny | permit > icmp < SA > < DA > [ icmp-type-name ]
```

In an extended ACL using `icmp` as the packet protocol type (see above), you can optionally specify an individual ICMP packet type or packet type/code pair to further define the criteria for a match. This option, if used, is entered immediately after the destination address (DA) entry. The following example shows two ACEs entered in a Named ACL context:

```
#permit icmp any any host-unknown
#permit icmp any any 3 7
```

This option identifies an individual ICMP packet type as criteria for permitting or denying that type of ICMP traffic in an ACE.

- **icmp-type** — This value is in the range of 0 - 255 and corresponds to an ICMP packet type.
- **icmp-code** — This value is in the range of 0 - 255 and corresponds to an ICMP code for an ICMP packet type.

For more information on ICMP type names, visit the Internet Assigned Numbers Authority (IANA) website at [www.iana.com](http://www.iana.com), click on “Protocol Number Assignment Services”, and then go to the selections under “Internet Control Message Protocol (ICMP) Parameters”.
These name options are an alternative to the \texttt{[icmp-type [icmp-code]]} methodology described above. For more information, visit the IANA website cited above.

<table>
<thead>
<tr>
<th>icmp-type-name</th>
<th>action-type</th>
</tr>
</thead>
<tbody>
<tr>
<td>administratively-prohibited</td>
<td>net-tos-unreachable</td>
</tr>
<tr>
<td>alternate-address</td>
<td>net-unreachable</td>
</tr>
<tr>
<td>conversion-error</td>
<td>network-unreachable</td>
</tr>
<tr>
<td>dod-host-prohibited</td>
<td>no-room-for-option</td>
</tr>
<tr>
<td>dod-net-prohibited</td>
<td>option-missing</td>
</tr>
<tr>
<td>echo</td>
<td>packet-too-big</td>
</tr>
<tr>
<td>echo-reply</td>
<td>parameter-problem</td>
</tr>
<tr>
<td>general-parameter-problem</td>
<td>port-unreachable</td>
</tr>
<tr>
<td>host-isolated</td>
<td>precedence-unreachable</td>
</tr>
<tr>
<td>host-precedence-unreachable</td>
<td>protocol-unreachable</td>
</tr>
<tr>
<td>host-redirect</td>
<td>reassembly-timeout</td>
</tr>
<tr>
<td>host-tos-redirect</td>
<td>redirect</td>
</tr>
<tr>
<td>host-tos-unreachable</td>
<td>router-advertisement</td>
</tr>
<tr>
<td>host-unknown</td>
<td>router-solicitation</td>
</tr>
<tr>
<td>host-unreachable</td>
<td>source-quench</td>
</tr>
<tr>
<td>information-reply</td>
<td>source-route-failed</td>
</tr>
<tr>
<td>information-request</td>
<td>time-exceeded</td>
</tr>
<tr>
<td>mask-reply</td>
<td>timestamp-reply</td>
</tr>
<tr>
<td>mask-request</td>
<td>timestamp-request</td>
</tr>
<tr>
<td>mobile-redirect</td>
<td>traceroute</td>
</tr>
<tr>
<td>net-redirect</td>
<td>ttl-exceeded</td>
</tr>
<tr>
<td>net-tos-redirect</td>
<td>unreachable</td>
</tr>
</tbody>
</table>
IPv4 Access Control Lists (ACLs)
Configuring Extended ACLs

Option for IGMP in Extended ACLs. This option is useful where it is necessary to permit some types of IGMP traffic and deny other types instead of simply permitting or denying all types of IGMP traffic. That is, an ACE designed to permit or deny IGMP traffic can optionally include an IGMP packet type to permit or deny an individual type of IGMP packet while not addressing other IGMP traffic types in the same ACE. (For a summary of the extended ACL syntax options, refer to table 9-7 on page 9-50.)

Syntax:  \(< \text{permit|deny} > \text{igmp} < \text{SA} > \text{DA} >[ \text{igmp-type} ]\)

In an extended ACL using igmp as the packet protocol type, you can optionally specify an individual IGMP packet type to further define the criteria for a match. This option, if used, is entered immediately after the destination addressing entry. The following example shows an IGMP ACE entered in the Named ACL context:

HP Switch(config-ext-nacl)# permit igmp any any host-query[ igmp-type ]

The complete list of IGMP packet-type options includes:

dvmrp  trace  mtrace-request
host-query  v2-host-report  v3-host-report
host-report  v2-host-leave
pim  mtrace-reply

For more information on IGMP packet types, visit the Internet Assigned Numbers Authority (IANA) website at www.iana.com, click on “Protocol Number Assignment Services”, and then go to the selections under “Internet Group Management Protocol (IGMP) Type Numbers”.

Configuring Numbered, Extended ACLs

This section describes the commands for performing the following in a numbered, extended ACL:

- creating the ACL by entering the first ACE in the list
- appending a new ACE to the end of an existing ACL
For other IPv4 ACL topics, refer to the following:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuring named, standard ACLs</td>
<td>9-43</td>
</tr>
<tr>
<td>configuring numbered, standard ACLs</td>
<td>9-46</td>
</tr>
<tr>
<td>configuring named, extended ACLs</td>
<td>9-52</td>
</tr>
<tr>
<td>applying or removing an ACL on an interface</td>
<td>9-70</td>
</tr>
<tr>
<td>deleting an ACL</td>
<td>9-71</td>
</tr>
<tr>
<td>editing an ACL</td>
<td>9-72</td>
</tr>
<tr>
<td>sequence numbering in ACLs</td>
<td>9-73</td>
</tr>
<tr>
<td>including remarks in an ACL</td>
<td>9-78</td>
</tr>
<tr>
<td>displaying ACL configuration data</td>
<td>9-82</td>
</tr>
<tr>
<td>creating or editing ACLs offline</td>
<td>9-91</td>
</tr>
<tr>
<td>enabling ACL “Deny” logging</td>
<td>9-93</td>
</tr>
</tbody>
</table>

**Creating or Adding to an Extended, Numbered ACL.** This command is an alternative to using `ip access-list extended < name-str >` and does not use the Named ACL (nacl) context. (For an extended ACL syntax summary, refer to table 9-7 on page 9-50.)

**Syntax:**

```
access-list <100-199> < deny | permit > < ip | ip-protocol | ip-protocol-nbr >
< any | host < SA > | SA/mask-length | SA < mask >>
< any | host < DA > | DA/mask-length | DA < mask >>
[ precedence < 0 - 7 | precedence-name >]
[ tos < tos-bit-setting >]
[ log ]
```
If the ACL does not already exist, this command creates the specified ACL and its first ACE. If the ACL already exists, the new ACE is appended to the end of the configured list of explicit ACEs. In the default configuration, the ACEs in an ACL will automatically be assigned consecutive sequence numbers in increments of 10 and can be renumbered with resequence (page 9-77).

**Note:** To insert a new ACE between two existing ACEs in an extended, numbered ACL:

a. Use `ip access list extended < 100 - 199 >` to open the ACL as a named ACL.

b. Enter the desired sequence number along with the ACE statement you want.

(Refer to the “Numbered ACLs” list item on page 9-39.)

For a match to occur, a packet must have the source and destination addressing criteria specified in the ACE, as well as:

- the protocol-specific criteria configured in the ACE, including any included, optional elements (described later in this section)
- any (optional) precedence and/or ToS settings configured in the ACE

< 100-199 >

Specifies the ACL ID number. The switch interprets a numeric ACL with a value in this range as an extended ACL.

< deny | permit >

Specifies whether to deny (drop) or permit (forward) a packet that matches the criteria specified in the ACE, as described below.
< ip | ip-protocol | ip-protocol-nbr >

Specifies the packet protocol type required for a match. An extended ACL must include one of the following:

- **ip** — any IPv4 packet.
- **ip-protocol** — any one of the following IPv4 protocol names:
  - ip
  - ip-in-ip
  - ipv6-in-ip
  - gre
  - esp
  - ah
  - ospf
  - pim
  - vrrp
  - sctp
  - tcp*
  - udp*
  - icmp*
  - igmp*
  - any
  - host < SA >
  - SA/mask-length
  - SA < mask >

In an extended ACL, this parameter defines the source address (SA) that a packet must carry in order to have a match with the ACE.

- **any** — Specifies all inbound IPv4 packets.
- **host < SA >** — Specifies only inbound IPv4 packets from a single address. Use this option when you want to match only the IPv4 packets from a single source address.
- **SA/mask-length or SA < mask >** — Specifies packets received from an SA, where the SA is either a subnet or a group of IPv4 addresses. The mask can be in either dotted-decimal format or CIDR format with the number of significant bits. Refer to “Using CIDR Notation To Enter the IPv4 ACL Mask” on page 9-40.
IPv4 Access Control Lists (ACLs)
Configuring Extended ACLs

**SA Mask Application:** The mask is applied to the SA in the ACL to define which bits in a packet's source SA must exactly match the address configured in the ACL and which bits need not match.

**Example:** 10.10.10.1/24 and 10.10.10.1 0.0.0.255 both define any IP address in the range of 10.10.10.(1-255).

**Note:** Specifying a group of contiguous IPv4 addresses may require more than one ACE. For more on how masks operate in ACLs, refer to “How an ACE Uses a Mask To Screen Packets for Matches” on page 9-25.

< any | host < DA > | DA/mask-length >

This is the second instance of addressing in an extended ACE. It follows the first (SA) instance, described earlier, and defines the destination address (DA) that a packet must carry in order to have a match with the ACE. The options are the same as shown for < SA >.

- **any** — Allows routed IPv4 packets to any DA.
- **host < DA >** — Specifies only the packets having DA as the destination address. Use this criterion when you want to match only the IPv4 packets for a single DA.
- **DA/mask-length or DA < mask >** — Specifies packets intended for a destination address, where the address is either a subnet or a group of IPv4 addresses. The mask format can be in either dotted-decimal format or CIDR format (number of significant bits). Refer to “Using CIDR Notation To Enter the IPv4 ACL Mask” on page 9-40.

**DA Mask Application:** The mask is applied to the DA in the ACL to define which bits in a packet's DA must exactly match the DA configured in the ACL and which bits need not match. See also the above example and note.
IPv4 Access Control Lists (ACLs)
Configuring Extended ACLs

[precedence < 0 - 7 | precedence-name>]

This option causes the ACE to match packets with the specified IP precedence value. Values can be entered as the following IP precedence numbers or alphanumeric names:

- 0 or routine
- 1 “priority
- 2 “immediate
- 3 “flash
- 4 “flash-override
- 5 “critical
- 6 “internet (for internetwork control)
- 7 “network (for network control)

Note: The precedence criteria described in this section are applied in addition to any other selection criteria configured in the same ACE.

[tos]

This option can be used after the DA to cause the ACE to match packets with the specified Type-of-Service (ToS) setting. ToS values can be entered as the following numeric settings or, in the case of 0, 2, 4, and 8, as alphanumeric names:

- 0 or normal
- 2 “max-reliability
- 4 “max-throughput
- 6
- 8 “minimize-delay
- 10
- 12
- 14

Note: The ToS criteria in this section are applied in addition to any other criteria configured in the same ACE.

[log]

Optional; generates an Event Log message if:

- The action is deny. (This option is not configurable for Permit.)
- There is a match.
- ACL logging is enabled on the switch. (Refer to “Enabling ACL Logging on the Switch” on page 9-95)
Additional Options for TCP and UDP Traffic. An ACE designed to permit or deny TCP or UDP traffic can optionally include port number criteria for either the source or destination, or both. Use of TCP criteria also allows the established option for controlling TCP connection traffic. (For a summary of the extended ACL syntax options, refer to table 9-7 on page 9-50.)

Syntax: access-list < 100 - 199 > < deny | permit > < tcp | udp >
< SA > [comparison-operator < tcp/udp-src-port >]
< DA > [comparison-operator < tcp-dest-port >] [established]
< DA > [comparison-operator < udp-dest-port >]

This source-port and destination-port TCP/UDP criteria is identical to the criteria described for TCP/UDP use in named, extended ACLs, beginning on page 9-58.

Additional Options for ICMP Traffic. This option is useful where it is necessary to permit some types of ICMP traffic and deny other types, instead of simply permitting or denying all types of ICMP traffic. That is, an ACE designed to permit or deny ICMP traffic can optionally include an ICMP type and code value to permit or deny an individual type of ICMP packet while not addressing other ICMP traffic types in the same ACE. As an optional alternative, the ACE can include the name of an ICMP packet type. (For a summary of the extended ACL syntax options, refer to table 9-7 on page 9-50.)

Syntax: access-list < 100 - 199 > < deny | permit > icmp < SA > < DA >
[ [ icmp-type [ icmp-code ] ] | [ icmp-type-name ] ]

The ICMP “type” and “code” criteria are identical to the criteria described for ICMP in named, extended ACLs, beginning on page 9-60.

Additional Option for IGMP. This option is useful where it is necessary to permit some types of IGMP traffic and deny other types, instead of simply permitting or denying all types of IGMP traffic. That is, an ACE designed to permit or deny IGMP traffic can optionally include an IGMP packet type to permit or deny an individual type of IGMP packet while not addressing other IGMP traffic types in the same ACE. (For a summary of the extended ACL syntax options, refer to table 9-7 on page 9-50.)
Syntax:  access-list < 100 - 199 >
< deny | permit > igmp < src-ip > < dest-ip > [ igmp-type ]

The IGMP “type” criteria is identical to the criteria described for IGMP in named, extended ACLs, beginning on page 9-62.
Adding or Removing an ACL Assignment On an Interface

Filtering Inbound IPv4 Traffic Per Port

For a given port, port list, or static port trunk, you can assign an ACL as a static port ACL to filter any IPv4 traffic entering the switch on that interface. You can also use the same ACL for assignment to multiple interfaces. For limits and operating rules, refer to “IPv4 ACL Configuration and Operating Rules” on page 9-24.

**Syntax:**

```
[no] interface <port-list | Trk x> ip access-group <identifier> in
```

where: `<identifier>` = either a ACL name or an ACL ID number.

Assigns an ACL as a static port ACL to a port, port list, or static trunk to filter any IPv4 traffic entering the switch on that interface. You can use either the global configuration level or the interface context level to assign or remove a static port ACL.

**Note:** The switch allows you to assign a nonexistent ACL name or number to an interface. In this case, if you subsequently configure an ACL with that name or number, it automatically becomes active on the assigned interface. Also, if you delete an assigned ACL from the switch without subsequently using the "no" form of this command to remove the assignment to an interface, the ACL assignment remains and will automatically activate any new ACL you create with the same identifier (name or number).
Deleting an ACL

**Syntax:**

```
no ip access-list standard < name-str | 1-99 >

no ip access-list extended < name-str | 100-199 >

no access-list < 1 - 99 | 100 - 199 >
```

Removes the specified ACL from the switch’s running-config file.

**Note:** Deleting an ACL does not delete any assignment of that ACL’s identifier on a specific interface. Creating a new ACL using an identifier that is already configured on an interface causes the switch to automatically activate that ACL. If you need to remove an ACL identifier assignment on an interface, refer to “Adding or Removing an ACL Assignment On an Interface” on page 9-70.

---

**Figure 9-15. Methods for Enabling and Disabling ACLs**

```
HP Switch(config)# interface b10 ip access-group My-List in
HP Switch(config)# interface b10
HP Switch(eth-b10)# ip access-group 155 in
HP Switch(eth-b10)# exit
HP Switch(config)# no interface b10 ip access-group My-List in
HP Switch(config)# interface b10
HP Switch(eth-b10)# no ip access-group 155 in
HP Switch(eth-b10)# exit
```
IPv4 Access Control Lists (ACLs)

Editing an Existing ACL

The CLI provides the capability for editing in the switch by using sequence numbers to insert or delete individual ACEs. An offline method is also available. This section describes using the CLI for editing ACLs. To use the offline method for editing ACLs, refer to “Creating or Editing ACLs Offline” on page 9-91.

Using the CLI To Edit ACLs

You can use the CLI to delete individual ACEs from anywhere in an ACL, append new ACEs to the end of an ACL, and insert new ACEs anywhere within an ACL.

General Editing Rules

- **Named ACLs:**
  - When you enter a new ACE in a named ACL without specifying a sequence number, the switch inserts the ACE as the last entry in the ACL.
  - When you enter a new ACE in a named ACL and include a sequence number, the switch inserts the ACE according to the position of the sequence number in the current list of ACEs.

- **Numbered ACLs:** When using the `access-list < 1 - 99 | 100 - 199 >` command to create or add ACEs to a numbered ACL, each new ACE you enter is added to the end of the current list. (This command does not offer a `<seq-#>` option for including a sequence number to enable inserting an ACE at other points in the list.) Note, however, that once a numbered list has been created, you have the option of accessing it in the same way as a named list by using the `ip access-list < standard | extended >` command. This enables you to edit a numbered list in the same way that you would edit a named list. (See the next item in this list.)
IPv4 Access Control Lists (ACLs)
Editing an Existing ACL

- You can delete any ACE from any ACL (named or numbered) by using the `ip access-list` command to enter the ACLs context, and then using the `no < seq-#>` command (page 9-76).

- Deleting the last ACE from an ACL leaves the ACL in memory. In this case, the ACL is “empty” and cannot perform any filtering tasks. (In any ACL the Implicit Deny does not apply unless the ACL includes at least one explicit ACE.)

Sequence Numbering in ACLs

The ACEs in any ACL are sequentially numbered. In the default state, the sequence number of the first ACE in a list is “10” and subsequent ACEs are numbered in increments of 10. For example, the following `show run` output lists three ACEs with default numbering in a list named “My-List”:

```plaintext
ip access-list standard "My-List"
  10 permit 10.10.10.25 0.0.0.0
  20 permit 10.20.10.117 0.0.0.0
  30 deny 10.20.10.1 0.0.0.255
exit
```

Figure 9-16. Example of the Default Sequential Numbering for ACEs

You can add an ACE to the end of a named or numbered ACL by using either `access-list` for numbered ACLs or `ip access-list` for named ACLs:

```plaintext
HP Switch(config)# access-list 2 permit any
```

**Enters the context of an extended ACL and appends an ACE to the end of the list.**

```plaintext
HP Switch(Config)# ip access-list standard My-list
HP Switch(Config-ext-nacl)# permit ip any host 10.10.10.125
```

**Appends an ACE to the end of a standard, numbered ACL.**

Figure 9-17. Examples of Adding an ACE to the end of Numbered or Named ACLs
IPv4 Access Control Lists (ACLs)

Editing an Existing ACL

For example, to append a fourth ACE to the end of the ACL in figure 9-16:

```
HP Switch(config)# ip access-list standard My-List
HP Switch(config-std-nacl)# permit any
HP Switch(config-std-nacl)# show run
.
.
ip access-list standard "My-List"
  10 permit 10.10.10.25 0.0.0.0
  20 permit 10.20.10.117 0.0.0.0
  30 deny 10.20.10.1 0.0.0.255
  40 permit 0.0.0.0 255.255.255.255
exit
```

Figure 9-18. Example of Appending an ACE to an Existing List

**Note**

When using the `access-list < 1 - 99 | 100 - 199 > < permit | deny > < SA >` command to create an ACE for a numbered ACL, the ACE is always added to the end of the current list and given the appropriate sequence number. However, once a numbered list has been created, you can use the `ip access-list` command to open it as a named ACL and specify a nondefault sequence number, as described in the next section.

Inserting an ACE in an Existing ACL

This action uses a sequence number to specify where to insert a new ACE into an existing sequence of ACLs.

**Syntax:**

`ip access-list < standard | extended > < name-str | 1 - 99 | 100 - 199 >
<1-2147483647> < permit | deny > < standard-acl-ip-criteria > [ log ]
<1-2147483647> < permit | deny > < extended-acl-ip-criteria > [ options ]`

The first command enters the “Named-ACL” context for the specified ACL. The remaining two commands insert a new ACE in a standard or extended ACL, respectively. (For details on these criteria and options, refer to table 9-1, “Command Summary for Standard IPv4 ACLs”—page 9-4, and table 9-2, “Command Summary for IPv4 Extended ACLs”—page 9-5.)

To insert a new ACE between existing ACEs in a list:

1. Use `ip access-list` to enter the “Named-ACL” (nacl) context of the ACE. 
   This applies regardless of whether the ACE was originally created as a numbered ACL or a named ACL.
IPv4 Access Control Lists (ACLs)
Editing an Existing ACL

2. Begin the ACE command with a sequence number that identifies the position you want the ACE to occupy. (The sequence number range is 1-2147483647.)

3. Complete the ACE with the command syntax appropriate for the type of ACL you are editing.

For example, inserting a new ACE between the ACEs numbered 10 and 20 in figure 9-18 requires a sequence number in the range of 11-19 for the new ACE.

```
HP Switch(config)# ip access-list standard My-List
HP Switch(config-std-nacl)# 15 deny 10.10.10.1/24
HP Switch(config-std-nacl)# show run

ip access-list standard "My-List"
10 permit 10.10.10.25 0.0.0.0
15 deny 10.10.10.1 0.0.0.255
20 permit 10.20.10.117 0.0.0.0
30 deny 10.20.10.1 0.0.0.255
40 permit 0.0.0.0 255.255.255.255
exit
```

Figure 9-19. Example of Inserting an ACE in an Existing ACL

In the following example, the first two ACEs entered become lines 10 and 20 in the list. The third ACE entered is configured with a sequence number of 15 and is inserted between lines 10 and 20.

```
HP Switch(config)# ip access-list standard List-01
HP Switch(config-std-nacl)# permit 10.10.10.1/24
HP Switch(config-std-nacl)# deny 10.10.1.1/16
HP Switch(config-std-nacl)# 15 permit 10.10.20.1/24
HP Switch(config-std-nacl)# show run

Running configuration:
....
ip access-list standard "List-01"
10 permit 10.10.10.25 0.0.0.0
15 permit 10.10.10.1 0.0.0.255
15 permit 10.10.20.1 0.0.0.255
20 deny 10.10.1.1 0.0.255.255
exit
```

Figure 9-20. Example of Inserting an ACE into an Existing Sequence
Deleting an ACE from an Existing ACL

This action uses ACL sequence numbers to delete ACEs from an ACL.

**Syntax:**

```
ip access-list < standard | extended > < name-str | 1 - 99 | 100 - 199 >
no < seq-#>
```

*The first command enters the “Named-ACL” context for the specified ACL. The no command deletes the ACE corresponding to the sequence number entered. (Range: 1 - 2147483647)*

1. To find the sequence number of the ACE you want to delete, use `show run` or `show access-list < name-str | 1 - 99 | 100-199 >` to view the ACL.
2. Use `ip access-list` to enter the “Named-ACL” (nacl) context of the ACE. *This applies regardless of whether the ACE was originally created as a numbered ACL or a named ACL.*
3. In the “Named-ACL” context, type `no` and enter the sequence number of the ACE you want to delete.

Figure 9-21 illustrates the process for deleting an ACE from a list:

```
HP Switch(config)# show run
...
ACL Before Deleting an ACE
ip access-list standard "My-List"
  10 permit 10.10.10.25 0.0.0.0
  15 deny 10.10.10.1 0.0.0.255
  20 permit 10.20.10.117 0.0.0.0
  30 deny 10.20.10.1 0.0.0.255
  40 permit 0.0.0.0 255.255.255.255
exit
HP Switch(config)# ip access-list standard My-List
HP Switch(config-std-nacl)# no 20
HP Switch(config-std-nacl)# show run
...
ACL After Deleting the ACE at Line 20
ip access-list standard "My-List"
  10 permit 10.10.10.25 0.0.0.0
  15 deny 10.10.10.1 0.0.0.255
  30 deny 10.20.10.1 0.0.0.255
  40 permit 0.0.0.0 255.255.255.255
exit
```

**Figure 9-21. Example of Deleting an ACE from Any ACL**
Resequencing the ACEs in an ACL

This action reconfigures the starting sequence number for ACEs in an ACL, and resets the numeric interval between sequence numbers for ACEs configured in the ACL.

**Syntax:** ip access-list resequence < name-str | 1 - 99 | 100 - 199 > < starting-seq-# > < interval >

*Resets the sequence numbers for all ACEs in the ACL.*

*< starting-seq-# >*: Specifies the sequence number for the first ACE in the list. (*Default: 10; Range: 1 - 2147483647*)

*< interval >*: Specifies the interval between sequence numbers for the ACEs in the list. (*Default: 10; Range: 1 - 2147483647*)

1. To view the current sequence numbering in an ACE, use `show run` or `show access-list < name-str | 1 - 99 | 100-199 >`.
2. Use the command syntax (above) to change the sequence numbering.

This example resequences the “My-List” ACL at the bottom of figure 9-21 so that the list begins with line 100 and uses a sequence interval of 100.

```
HP Switch(config)# show run
...
ip access-list standard "My-List"
  10 permit 10.10.10.25 0.0.0.0
  15 deny 10.10.10.1 0.0.0.255
  30 deny 10.20.10.1 0.0.0.255
  40 permit 0.0.0.0 255.255.255.255
exit
...
HP Switch(config)# ip access-list resequence My-List 100 100
HP Switch(config)# show run
...
ip access-list standard "My-List"
  100 permit 10.10.10.25 0.0.0.0
  200 deny 10.10.10.1 0.0.0.255
  300 deny 10.20.10.1 0.0.0.255
  400 permit 0.0.0.0 255.255.255.255
exit
```

**Figure 9-22. Example of Viewing and Resequencing an ACL**
Attaching a Remark to an ACE

A remark is numbered in the same way as an ACE, and uses the same sequence number as the ACE to which it refers. This operation requires that the remark for a given ACE be entered prior to entering the ACE itself.

**Syntax:** access-list < 1 - 99 | 100 - 199 > remark < remark-str >

This syntax appends a remark to the end of a numbered ACL and automatically assigns a sequence number to the remark. The next command entry should be the ACE to which the remark belongs. (The new ACE will automatically be numbered with the same sequence number as was used for the preceding remark.)

**Syntax:** ip access-list < standard | extended > < name-str | 1-99 | 100-199 > [ seq-# ] remark < remark-str >

This syntax applies to both named and numbered ACLs. Without an optional sequence number, the remark is appended to the end of the list and automatically assigned a sequence number. When entered with an optional sequence number, the remark is inserted in the list according to the numeric precedence of the sequence number. The no form of the command deletes the indicated remark, but does not affect the related ACE.

To associate a remark with a specific ACE, enter the remark first, and then enter the ACE.

- Entering a remark without a sequence number and then entering an ACE without a sequence number results in the two entries being automatically paired with the same sequence number and appended to the end of the current ACL.
- Entering a remark with a sequence number and then entering an ACE with the same sequence number results in the two entries being paired together and positioned in the list according to the sequence number they share.
Note

After a numbered ACL has been created (using `access-list < 1 - 99 | 100 - 199>`), it can be managed as either a named or numbered ACL. For example, in an existing ACL with a numeric identifier of “115”, either of the following command sets adds an ACE denying IP traffic from any IP source to a host at 10.10.10.100:

```
HP Switch(config)# access-list 115 deny ip host 10.10.10.100
HP Switch(config)# ip access-list extended 115
HP Switch(config-ext-nacl)# deny ip any 10.10.10.100
```

Appending Remarks and Related ACEs to the End of an ACL. To include a remark for an ACE that will be appended to the end of the current ACL, enter the remark first, then enter the related ACE. This results in the remark and the subsequent ACE having the same sequence number. For example, to add remarks using the “Named-ACL” (`nacl`) context:

```
HP Switch(config)# ip access-list standard My-List
HP Switch(config-std-nacl)# permit host 10.10.10.15
HP Switch(config-std-nacl)# deny 10.10.10.1/24
HP Switch(config-std-nacl)# remark HOST-10.20.10.34
HP Switch(config-std-nacl)# permit host 10.20.10.34
HP Switch(config-std-nacl)# show run
... hostname "HP Switch"
ip access-list standard "My-List"
  10 permit 10.10.10.15 0.0.0.0
  20 deny 10.10.10.1 0.0.0.255
  30 remark "HOST-10.20.10.34"
  30 permit 10.20.10.34 0.0.0.0
exit
```

Figure 9-23. Example of Appending a Remark and Its Related ACE to the End of an ACL

(You can also perform the operation illustrated in figure 9-23 by using the numbered, `access-list < 1 - 99 | 100 - 199>` syntax shown at the beginning of this section.)
Inserting Remarks and Related ACEs Within an Existing List. To insert an ACE with a remark within an ACL by specifying a sequence number, insert the numbered remark first, then, using the same sequence number, insert the ACE. (This operation applies only to ACLs accessed using the "Named-ACL" (nacl) context.) For example:

```
HP Switch(config-std-nacl)# 15 remark "HOST 10.10.10.21"
HP Switch(config-std-nacl)# 15 permit host 10.10.10.21
HP Switch(config-std-nacl)# show run
ip access-list standard "My-List"
  10 permit 10.10.10.15 0.0.0.0
  15 remark "HOST 10.10.10.21"
  15 permit 10.10.10.21 0.0.0.0
  20 deny 10.10.10.1 0.0.0.255
  30 remark "HOST-10.20.10.34"
  30 permit 10.20.10.34 0.0.0.0
exit
```

**Figure 9-24. Example of Inserting a Remark**

Inserting a Remark for an ACE that Already Exists in an ACL. If a sequence number is already assigned to an ACE in a list, you cannot insert a remark by assigning it to the same number. (To configure a remark with the same number as a given ACE, the remark must be configured first.) To assign a remark to the same number as an existing ACE:

1. Delete the ACE.
2. Configure the remark with the number you want assigned to the pair.
3. Re-Enter the deleted ACE with the number used to enter the remark.

Removing a Remark from an Existing ACE. If you want to remove a remark, but want to retain the ACE, do the following:

1. Use the Named ACL context to enter the ACL.
2. Using `show run` or `show access-list <list-name>`, note the sequence number and content of the ACE having a remark you want to remove.
3. Delete the ACE.
4. Using the same sequence number, re-enter the ACE.
Operating Notes for Remarks

- The `resequence` command ignores “orphan” remarks that do not have an ACE counterpart with the same sequence number. For example, if:
  - a remark numbered “55” exists in an ACE
  - there is no ACE numbered “55” in the same ACL
  - `resequence` is executed on an ACL

  then the remark retains “55” as its sequence number and will be placed in the renumbered version of the ACL according to that sequence number.

- Entering an unnumbered remark followed by a numbered ACE, or the reverse, creates an “orphan” remark. The unnumbered entry will be assigned a sequence number that is an increment from the last ACE in the list. The numbered entry will then be placed sequentially in the list according to the sequence number used.

- Configuring two remarks without either sequence numbers or an intervening, unnumbered ACE results in the second remark overwriting the first.

```
HP Switch(config)# ip access-list standard Accounting
HP Switch(config-std-nacl)# permit host 10.10.10.115
HP Switch(config-std-nacl)# deny 10.10.10.1/24
HP Switch(config-std-nacl)# remark Marketing
HP Switch(config-std-nacl)# remark Channel_Mktg
HP Switch(config-std-nacl)# show run . . .
   ip access-list standard "Accounting"
      10 permit 10.10.10.115 0.0.0.0
      20 deny 10.10.10.1 0.0.0.255
      30 remark "Channel_Mktg"
exit
```

Where multiple remarks are sequentially entered for automatic inclusion at the end of an ACL, each successive remark replaces the previous one until an ACE is configured for automatic inclusion at the end of the list.

**Figure 9-25. Example of Overwriting One Remark with Another**
# Displaying ACL Configuration Data

<table>
<thead>
<tr>
<th>ACL Commands</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-list</td>
<td>Displays a brief listing of all IPv4 ACLs on the switch.</td>
<td>9-83</td>
</tr>
<tr>
<td>show access-list config</td>
<td>Display the type, identifier, and content of all IPv4 ACLs configured in the switch.</td>
<td>9-84</td>
</tr>
<tr>
<td>show access-list ports &lt; all</td>
<td>port-list &gt;</td>
<td>Lists the IPv4 ACL static port assignment for either all ports and trunks, or for the specified ports and/or trunks.</td>
</tr>
<tr>
<td>show access-list &lt; acl-name- str &gt;</td>
<td>Display detailed content information for a specific IPv4 ACL.</td>
<td>9-86</td>
</tr>
<tr>
<td>show access-list resources</td>
<td>Displays information on the resources currently available in the switch. Refer to the appendix titled “Monitoring Resources” in the latest Management and Configuration Guide for your switch.</td>
<td>—</td>
</tr>
<tr>
<td>show access-list radius &lt; all</td>
<td>port-list &gt;</td>
<td>Lists the RADIUS ACL(s) currently assigned for either all ports and trunks, or for the specified ports and/or trunks. For more on this topic, refer to chapter 6, “Configuring RADIUS Server Support for Switch Services”.</td>
</tr>
<tr>
<td>show config</td>
<td>show config includes configured ACLs and assignments existing in the startup-config file.</td>
<td>—</td>
</tr>
<tr>
<td>show running</td>
<td>show running includes configured ACLs and assignments existing in the running-config file. For more on these commands, refer to “Using the CLI To Implement Configuration Changes” in the chapter titled “Switch Memory and Configuration” in the latest Management and Configuration Guide for your switch.</td>
<td>—</td>
</tr>
</tbody>
</table>
Display an ACL Summary

This command lists the configured IPv4 ACLs.

**Syntax:** show access-list

List a summary table of the name, type, and application status of IPv4 ACLs configured on the switch.

For example:

```
HP Switch(config)# show access-list
Access Control Lists
Type  Appl  Name
----  ----  ------------------------------------------
std   yes  List-01-v4 IN
ext   no   List-02-v4 OUT
std   yes  55
```

In this switch, the ACL named “List-02-v4-OUT” exists in the configuration.

**Figure 9-26. Example of show access-list Command**

**Figure 9-27. Example of a Summary Table of Access lists**

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Shows whether the listed ACL is an IPv4 <strong>std</strong> AC or an IPv4 <strong>ext</strong> AC.</td>
</tr>
<tr>
<td>Appl</td>
<td>Shows whether the listed ACL has been applied to an interface (<strong>yes/no</strong>).</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the identifier (name or number) assigned to each ACL configured in the switch.</td>
</tr>
</tbody>
</table>
Display the Content of All ACLs on the Switch

This command lists the configuration details for the IPv4 ACLs in the running-config file.

**Syntax:**  
```
show access-list config
```

*List the configured syntax for all IPv4 ACLs currently configured on the switch.*

**Note**

Notice that you can use the output from this command for input to an offline text file in which you can edit, add, or delete ACL commands. Refer to “Creating or Editing ACLs Offline” on page 9-91.

This information also appears in the `show running` display. If you executed `write memory` after configuring an ACL, it appears in the `show config` display.

For example, with two ACLs configured in the switch, you will see results similar to the following:

```
HP Switch(config)# show access-list config

ip access-list standard "List-43"
  10 deny 10.28.236.77 0.0.0.0
  20 deny 10.29.140.107 0.0.0.0
  30 permit 0.0.0.0 255.255.255.255
  exit

ip access-list extended "111"
  10 permit tcp 10.30.133.27 0.0.0.0 0.0.0.0 255.255.255.255
  20 permit tcp 10.30.155.101 0.0.0.0 0.0.0.0 255.255.255.255
  30 deny ip 10.30.133.1 0.0.0.0 0.0.0.0 255.255.255.255 log
  40 deny ip 10.30.155.1 0.0.0.255 0.0.0.0 255.255.255.255
  exit
```

**Figure 9-28. Example of an ACL Configured Syntax Listing**
IPv4 Access Control Lists (ACLs)
Displaying ACL Configuration Data

Display Static Port ACL Assignments

This command briefly lists the identification and type(s) of current static port ACL assignments to individual switch ports and trunks, as configured in the running-config file. (The switch allows one static port ACL assignment per port.)

**Syntax:**
```
show access-list ports < all | interface >
```

Lists the current static port ACL assignments for ports and trunks in the running config file.

**Note**
This information also appears in the show running display. If you execute `write memory` after configuring an ACL, it appears in the show config display.

For example, if you assigned a standard ACL with an ACL-ID of “Port-10” to filter inbound IP traffic on switch ports B10-B11 and trunk trk1, you could verify these assignments as shown in figure 9-29.

```
HP Switch(config)# show access-list ports all
Access Lists for Port B10
  Inbound  : 15
  Type     : Standard

Access Lists for Port B11
  Inbound  : 15
  Type     : Standard

Access Lists for Port Trk1
  Inbound  : 15
  Type     : Standard
```

Figure 9-29. Example of Listing the ACL Assignments for Ports and Trunks
IPv4 Access Control Lists (ACLs)
Displaying ACL Configuration Data

Displaying the Content of a Specific ACL
This command displays a specific ACL configured in the running config file in an easy-to-read tabular format.

Note
This information also appears in the show running display. If you execute write memory after configuring an ACL, it also appears in the show config display.

Syntax:  show access-list <acl-id>
Display detailed information on the content of a specific ACL configured in the running-config file.

For example, suppose you configured the following two ACLs in the switch:

<table>
<thead>
<tr>
<th>ACL ID</th>
<th>Type</th>
<th>Desired Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Standard</td>
<td>• Deny IP traffic from 18.28.236.77 and 18.29.140.107.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Permit IP traffic from all other sources.</td>
</tr>
<tr>
<td>105</td>
<td>Extended</td>
<td>• Permit any TCP traffic from 18.30.133.27 to any destination.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deny any other IP traffic from 18.30.133.(1-255).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Permit all other IP traffic from any source to any destination.</td>
</tr>
</tbody>
</table>

Inspect the ACLs as follows:

```
HP Switch(config)# show access-list 1
Access Control Lists
Name: 1
Type: Standard
Applied: Yes

SEQ Entry
------------------------------------------------------------------------------
10   Action: deny (log)
     IP : 10.28.236.77     Mask: 0.0.0.0
20   Action: deny
     IP : 10.29.140.107    Mask: 0.0.0.0
30   Action: permit
     IP : 0.0.0.0          Mask: 255.255.255.255
```

Figure 9-30. Example of a Listing a Standard ACL
IPv4 Access Control Lists (ACLs)

Displaying ACL Configuration Data

Figure 9-31. Examples of Listings Showing the Content of Standard and Extended ACLs

<table>
<thead>
<tr>
<th>SEQ</th>
<th>Entry</th>
</tr>
</thead>
</table>
| 10  | Action: permit  
Remark: Telnet Allowed  
Src IP: 10.30.133.27  
Mask: 0.0.0.0  
Port(s): eq 23  
Dst IP: 0.0.0.0  
Mask: 255.255.255.255  
Proto : TCP (Established)  
TOS : -  
Precedence: routine |
| 20  | Action: deny (log)  
Src IP: 10.30.133.1  
Mask: 0.0.0.255  
Port(s):  
Dst IP: 0.0.0.0  
Mask: 255.255.255.255  
Proto : IP  
TOS : -  
Precedence: - |
| 30  | Action: permit  
Src IP: 0.0.0.0  
Mask: 255.255.255.255  
Port(s):  
Dst IP: 0.0.0.0  
Mask: 255.255.255.255  
Proto : IP  
TOS : -  
Precedence: - |

Table 9-8. Descriptions of Data Types Included in Show Access-List < acl-id > Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The ACL identifier. Can be a number from 1 to 199, or a name.</td>
</tr>
<tr>
<td>Type</td>
<td>Standard or Extended. The former uses only source IP addressing. The latter uses both source and destination IP addressing and also allows TCP or UDP port specifiers.</td>
</tr>
<tr>
<td>Applied</td>
<td>“Yes” means the ACL has been applied to a port. “No” means the ACL exists in the switch configuration, but has not been applied to any interface, and is therefore not in use.</td>
</tr>
<tr>
<td>SEQ</td>
<td>The sequential number of the Access Control Entry (ACE) in the specified ACL.</td>
</tr>
<tr>
<td>Entry</td>
<td>Lists the content of the ACEs in the selected ACL.</td>
</tr>
<tr>
<td>Action</td>
<td>Permit (forward) or deny (drop) a packet when it is compared to the criteria in the applicable ACE and found to match. Includes the optional log option, if used, in deny actions.</td>
</tr>
<tr>
<td>Remark</td>
<td>Displays any optional remark text configured for the selected ACE.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP</td>
<td>Used for Standard ACLs: The source IP address to which the configured mask is applied to determine whether there is a match with a packet.</td>
</tr>
<tr>
<td>Src IP</td>
<td>Used for Extended ACLs: Same as above.</td>
</tr>
<tr>
<td>Dst IP</td>
<td>Used for Extended ACLs: The source and destination IP addresses to which the corresponding configured masks are applied to determine whether there is a match with a packet.</td>
</tr>
<tr>
<td>Mask</td>
<td>The mask configured in an ACE and applied to the corresponding IP address in the ACE to determine whether a packet matches the filtering criteria.</td>
</tr>
<tr>
<td>Proto</td>
<td>Used only in extended ACLs to specify the packet protocol type to filter. Must be either IP, TCP, or UDP. For TCP protocol selections, includes the established option, if configured.</td>
</tr>
<tr>
<td>Port(s)</td>
<td>Used only in extended ACLs to show any TCP or UDP operator and port number(s) included in the ACE.</td>
</tr>
<tr>
<td>TOS</td>
<td>Used only in extended ACLs to indicate Type-of-Service setting, if any.</td>
</tr>
<tr>
<td>Precedence</td>
<td>Used only in extended ACLs to indicate the IP precedence setting, if any.</td>
</tr>
</tbody>
</table>

Display All ACLs and Their Assignments in the Routing Switch Startup-Config File and Running-Config File

The show config and show running commands include in their listings any configured ACLs. Refer to figure 9-9 (page 9-36) for an example. Remember that show config lists the startup-config file and show running lists the running-config file.
Monitoring Static ACL Performance

ACL statistics counters provide a means for monitoring ACL performance by using counters to display the current number of matches the switch has detected for each ACE in an ACL assigned to a switch interface. This can help, for example, to determine whether a particular traffic type is being filtered by the intended ACE in an assigned list, or if traffic from a particular device or network is being filtered as intended.

Note

This section describes the command for monitoring static ACL performance. To monitor RADIUS-assigned ACL performance, use either of the following commands:

```
show access-list radius < all | port-list >
show port-access < authenticator | mac-based | web-based > clients < port-list > detailed
```

Refer to “Displaying the Current RADIUS-Assigned ACL Activity on the Switch” on page 6-24.

Syntax: show statistics aclv4 < acl-name-str > port < port-# > aclv4 < acl-name-str > vlan < vid > < in | out | vlan >

Displays the current match (hit) count per ACE for the specified IPv4 static ACL assignment on a specific interface:

Total: This column lists the running total of the matches the switch has detected for the ACEs in an applied ACL since the ACL's counters were last reset to 0 (zero)
**ACE Counter Operation:** For a given ACE in an assigned ACL, the counter increments by 1 each time the switch detects a packet that matches the criteria in that ACE, and maintains a running total of the matches since the last counter reset.

For example, in ACL line 10 below, there has been a total of 37 matches on the ACE since the last time the ACL's counters were reset.

```
  Total
  ( 37)  10 permit icmp 10.10.20.3
```

**Note:** This ACL monitoring feature does not include hits on the “implicit deny” that is included at the end of all ACLs.

**Resetting ACE Hit Counters to Zero:**
- Removing an ACL from an interface zeros the ACL's ACE counters for that interface only.
- For a given ACL, either of the following actions clear the ACE counters to zero for all interfaces to which the ACL is assigned.
  - adding or removing a permit or deny ACE in the ACL
  - rebooting the switch
Creating or Editing ACLs Offline

The section titled “Editing an Existing ACL” on page 9-72 describes how to use the CLI to edit an ACL, and is most applicable in cases where the ACL is short or there is only a minor editing task to perform. The offline method provides a useful alternative to using the CLI for creating or extensively editing a large ACL. This section describes how to:

■ move an existing ACL to a TFTP server
■ use a text (.txt) file format to create a new ACL or edit an existing ACL offline
■ use TFTP to load an offline ACL into the switch’s running-config

For longer ACLs that may be difficult or time-consuming to accurately create or edit in the CLI, you can use the offline method described in this section.

**Note**

Copy commands that used either tftp or xmodem, also include an option to use usb as a source or destination device for file transfers. So although the following example highlights tftp, bear in mind that xmodem or usb can also be used to transfer ACLs to and from the switch.

Creating or Editing an ACL Offline

The Offline Process

1. Begin by doing one of the following:
   • To edit one or more existing ACLs, use `copy command-output tftp` to copy the current version of the ACL configuration to a file in your TFTP server. For example, to copy the ACL configuration to a file named `acl-02.txt` in the TFTP directory on a server at 10.28.227.2:

     ```
     HP Switch# copy command-output 'show access-list config' tftp 10.28.227.2 acl02.txt pc
     ```
   • To create a new ACL, just open a text (.txt) file in the appropriate directory on a TFTP server accessible to the switch.

2. Use a text editor to create or edit the ACL(s) in the *.txt ASCII file format.
IPv4 Access Control Lists (ACLs)
Creating or Editing ACLs Offline

If you are replacing an ACL on the switch with a new ACL that uses the same number or name syntax, begin the command file with a `no ip access-list` command to remove the earlier version of the ACL from the switch’s running-config file. Otherwise, the switch will append the new ACEs in the ACL you download to the existing ACL. For example, if you planned to use the `copy` command to replace ACL “List-120”, you would place this command at the beginning of the edited file:

```
no ip access-list extended List-120
```

Figure 9-32. Example of an Offline ACL File Designed To Replace An Existing ACL

```
no ip access-list extended List-120
ip access-list extended "List-120"
  10 remark "THIS ACE ALLOWS TELNET"
  10 permit tcp 10.30.133.27 0.0.0.0 eq 23 0.0.0.0 255.255.255.255
  20 deny ip 10.30.133.1 0.0.0.255 0.0.0.0 255.255.255.255
  30 deny ip 10.30.155.1 0.0.0.255 0.0.0.0 255.255.255.255
  40 remark "THIS IS THE FINAL ACE IN THE LIST"
  40 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit
```

3. Use `copy tftp command-file` to download the file as a list of commands to the switch.

4. Use the `show run` or `show access-list config` command to inspect the switch configuration to ensure that the ACL was properly downloaded.

**Note**

If a transport error occurs, the switch does not execute the command and the ACL is not configured.
Enable ACL “Deny” Logging

ACL logging enables the switch to generate a message when IP traffic meets the criteria for a match with an ACE that results in an explicit “deny” action. You can use ACL logging to help:

- Test your network to ensure that your ACL configuration is detecting and denying the IP traffic you do not want forwarded
- Receive notification when the switch detects attempts to forward IP traffic you have designed your ACLs to reject (deny)

The switch sends ACL messages to Syslog and optionally to the current console, Telnet, or SSH session. You can use `logging < >` to configure up to six Syslog server destinations.

Requirements for Using ACL Logging

- The switch configuration must include an ACL (1) assigned to a port or trunk and (2) containing an ACE configured with the `deny` action and the `log` option.
- For ACL logging to a Syslog server:
  - The server must be accessible to the switch and identified in the running configuration.
  - The logging facility must be enabled for Syslog.
  - Debug must be configured to:
    - support ACL messages
    - send debug messages to the desired debug destination

These requirements are described in more detail under “Enabling ACL Logging on the Switch” on page 9-95.
IPv4 Access Control Lists (ACLs)
Enable ACL "Deny" Logging

ACL Logging Operation

When the switch detects a packet match with an ACE and the ACE includes both the deny action and the optional log parameter, an ACL log message is sent to the designated debug destination. The first time a packet matches an ACE with deny and log configured, the message is sent immediately to the destination and the switch starts a wait-period of approximately five minutes. (The exact duration of the period depends on how the packets are internally routed.) At the end of the collection period, the switch sends a single-line summary of any additional “deny” matches for that ACE (and any other “deny” ACEs for which the switch detected a match). If no further log messages are generated in the wait-period, the switch suspends the timer and resets itself to send a message as soon as a new “deny” match occurs. The data in the message includes the information illustrated in figure 9-33.

<table>
<thead>
<tr>
<th>Feb 1 10:04:45 10.10.20.1 ACL:</th>
<th>Example Syslog report of the first deny event detected by the switch for this ACE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL 02/01/07 10:04:45 List NO-TELNET, seq#10 denied</td>
<td></td>
</tr>
<tr>
<td>tcp 10.10.10.3(1612)-&gt;10.10.20.2(23) on vlan 1, port A7</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feb 1 10:04:45 10.10.20.1 ACL:</th>
<th>Example of subsequent deny events detected by the switch for the same ACE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL 02/01/07 10:04:45 : ACL NO-TELNET seq#10 denied 6 packets</td>
<td></td>
</tr>
</tbody>
</table>

Figure 9-33. Content of a Message Generated by an ACL-Deny Action
IPv4 Access Control Lists (ACLs)
Enable ACL “Deny” Logging

Enabling ACL Logging on the Switch

1. If you are using a Syslog server, use the `logging < ip-addr >` command to configure the Syslog server IP address(es). Ensure that the switch can access any Syslog server(s) you specify.

2. Use `logging facility syslog` to enable the logging for Syslog operation.

3. Use the `debug destination` command to configure one or more log destinations. (Destination options include `logging` and `session`. For more information on debug, refer to “Debug and Syslog Messaging Operation” in appendix C, “Troubleshooting”, in the Management and Configuration Guide for your switch.)

4. Use `debug acl` or `debug all` to configure the debug operation to include ACL messages.

5. Configure one or more ACLs with the `deny` action and the `log` option.
General ACL Operating Notes

**ACLS do not provide DNS hostname support.** ACLs cannot be configured to screen hostname IP traffic between the switch and a DNS.

**ACLS Do Not Affect Serial Port Access.** ACLs do not apply to the switch's serial port.

**ACL Screening of IPv4 Traffic Generated by the Switch.** ACLs applied on the switch screen IP traffic when other devices generate it. Similarly, ACL applications can screen responses from other devices to unscreened IP traffic the switch generates.

**ACL Logging.**

- The ACL logging feature generates a message only when packets are explicitly denied as the result of a match, and not when explicitly permitted or implicitly denied. To help test ACL logging, configure the last entry in an ACL as an explicit `deny` statement with a `log` statement included.

- Logging enables you to selectively test specific devices or groups. However, excessive logging can affect switch performance. For this reason, HP recommends that you remove the logging option from ACEs for which you do not have a present need. Also, avoid configuring logging where it does not serve an immediate purpose. (Note that ACL logging is not designed to function as an accounting method.) See also “Apparent Failure To Log All ‘Deny’ Matches” in the section titled “ACL Problems”, found in appendix C, “Troubleshooting” of the Management and Configuration Guide for your switch.

- When configuring logging, you can reduce excessive resource use by configuring the appropriate ACEs to match with specific hosts instead of entire subnets. (For more on resource usage, refer to “Monitoring Shared Resources” on page 9-97.)

**Minimum Number of ACEs in an ACL.** Any ACL must include at least one ACE to enable IP traffic screening. A numbered ACL cannot be created without at least one ACE. A named ACL can be created “empty”; that is, without any ACEs. However in an empty ACL applied to an interface, the Implicit Deny function does not operate, and the ACL has no effect on traffic.
**Monitoring Shared Resources.** Applied ACLs share internal switch resources with several other features. The switch provides ample resources for all features. However, if the internal resources become fully subscribed, additional ACLs cannot be applied until the necessary resources are released from other applications. For information on determining current resource availability and usage, refer to appendix E, “Monitoring Resources” in the Management and Configuration Guide for your switch.

**Protocol Support.** ACL criteria does not include use of MAC information or QoS.

**Replacing or Adding To an Active ACL Policy.** If you assign an ACL to an interface and subsequently add or replace ACEs in that ACL, each new ACE becomes active when you enter it. If the ACL is configured on multiple interfaces when the change occurs, then the switch resources must accommodate all applications of the ACL. If there are insufficient resources to accommodate one of several ACL applications affected by the change, then the change is not applied to any of the interfaces and the previous version of the ACL remains in effect. Refer to “Monitoring Shared Resources”, above.

**“Strict” TCP and UDP.** When the ACL configuration includes TCP or UDP options, the switch operates in “strict” TCP and UDP mode for increased control. In this case, the switch compares all TCP and UDP packets against the ACLs. (In the HP 9300m and 9404sl Routing Switches, the Strict TCP and Strict UDP modes are optional and must be specifically invoked.)
Configuring Advanced Threat Protection

Introduction

As your network expands to include an increasing number of mobile devices, continuous Internet access, and new classes of users (such as partners, temporary employees, and visitors), additional protection from attacks launched from both inside and outside your internal network is often necessary.

Advanced threat protection can detect port scans and hackers who try to access a port or the switch itself. The following software features provide advanced threat protection and are described in this chapter:

■ DHCP snooping: Protects your network from common DHCP attacks, such as:
  • Address spoofing in which an invalid IP address or network gateway address is assigned by a rogue DHCP server.
  • Address exhaustion of available addresses in the network DHCP server, caused by repeated attacker access to the network and numerous IP address requests.

■ Dynamic ARP protection: Protects your network from ARP cache poisoning as in the following cases:
  • An unauthorized device forges an illegitimate ARP response and network devices use the response to update their ARP caches.
  • A denial-of-service (DoS) attack from unsolicited ARP responses changes the network gateway IP address so that outgoing traffic is prevented from leaving the network and overwhelms network devices.

■ Instrumentation monitor: Protects your network from a variety of other common attacks besides DHCP and ARP attacks, including:
  • Attempts at a port scan to expose a vulnerability in the switch, indicated by an excessive number of packets sent to closed TCP/UDP ports
Configuring Advanced Threat Protection

Introduction

- Attempts to fill all IP address entries in the switch’s forwarding table and cause legitimate traffic to be dropped, indicated by an increased number of learned IP destination addresses
- Attempts to spread viruses, indicated by an increased number of ARP request packets
- Attempts to exhaust system resources so that sufficient resources are not available to transmit legitimate traffic, indicated by an unusually high use of specific system resources
- Attempts to attack the switch’s CPU and introduce delay in system response time to new network events
- Attempts by hackers to access the switch, indicated by an excessive number of failed logins or port authentication failures
- Attempts to deny switch service by filling the forwarding table, indicated by an increased number of learned MAC addresses or a high number of MAC address moves from one port to another
- Attempts to exhaust available CPU resources, indicated by an increased number of learned MAC address events being discarded
## DHCP Snooping

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp-snooping</td>
<td>page 10-5</td>
</tr>
<tr>
<td>authorized-server</td>
<td>page 10-8</td>
</tr>
<tr>
<td>database</td>
<td>page 10-12</td>
</tr>
<tr>
<td>option</td>
<td>page 10-9</td>
</tr>
<tr>
<td>trust</td>
<td>page 10-7</td>
</tr>
<tr>
<td>verify</td>
<td>page 10-11</td>
</tr>
<tr>
<td>vlan</td>
<td>page 10-7</td>
</tr>
<tr>
<td>show dhcp-snooping</td>
<td>page 10-5</td>
</tr>
<tr>
<td>show dhcp-snooping stats</td>
<td>page 10-6</td>
</tr>
<tr>
<td>dhcp-snooping binding</td>
<td>page 10-13</td>
</tr>
<tr>
<td>debug dhcp-snooping</td>
<td>page 10-13</td>
</tr>
</tbody>
</table>
Overview

You can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP snooping accomplishes this by allowing you to distinguish between trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped. Conditions for dropping packets are shown below.

<table>
<thead>
<tr>
<th>Condition for Dropping a Packet</th>
<th>Packet Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>A packet from a DHCP server received on an untrusted port</td>
<td>DHCP OFFER, DHCP ACK, DHCP NACK</td>
</tr>
<tr>
<td>If the switch is configured with a list of authorized DHCP server addresses and a packet is received from a DHCP server on a trusted port with a source IP address that is not in the list of authorized DHCP server addresses.</td>
<td>DHCP OFFER, DHCP ACK, DHCP NACK</td>
</tr>
<tr>
<td>Unless configured to not perform this check, a DHCP packet received on an untrusted port where the DHCP client hardware address field does not match the source MAC address in the packet</td>
<td>N/A</td>
</tr>
<tr>
<td>Unless configured to not perform this check, a DHCP packet containing DHCP relay information (option 82) received from an untrusted port</td>
<td>N/A</td>
</tr>
<tr>
<td>A broadcast packet that has a MAC address in the DHCP binding database, but the port in the DHCP binding database is different from the port on which the packet is received</td>
<td>DHCP RELEASE, DHCPDECLINE</td>
</tr>
</tbody>
</table>
Enabling DHCP Snooping

DHCP snooping is enabled globally by entering this command:

```
HP Switch(config)# dhcp-snooping
```

Use the `no` form of the command to disable DHCP snooping.

**Syntax:**  `[no] dhcp-snooping [authorized-server | database | option | trust | verify | vlan]`

- **authorized server:** Enter the IP address of a trusted DHCP server. If no authorized servers are configured, all DHCP server addresses are considered valid. Maximum: 20 authorized servers.
- **database:** To configure a location for the lease database, enter a URL in the format `tftp://ip-addr/ascii-string`. The maximum number of characters for the URL is 63.
- **option:** Add relay information option (Option 82) to DHCP client packets that are being forwarded out trusted ports. The default is `yes`, add relay information.
- **trust:** Configure trusted ports. Only server packets received on trusted ports are forwarded. Default: `untrusted`.
- **verify:** Enables DHCP packet validation. The DHCP client hardware address field and the source MAC address must be the same for packets received on untrusted ports or the packet is dropped. Default: `Yes`.
- **vlan:** Enable DHCP snooping on a vlan. DHCP snooping must be enabled already. Default: `No`.

To display the DHCP snooping configuration, enter this command:

```
HP Switch(config)# show dhcp-snooping
```

An example of the output is shown below.
To display statistics about the DHCP snooping process, enter this command:

HP Switch(config)# show dhcp-snooping stats

An example of the output is shown below:

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Action</th>
<th>Reason</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>forward</td>
<td>from trusted port</td>
<td>8</td>
</tr>
<tr>
<td>client</td>
<td>forward</td>
<td>to trusted port</td>
<td>8</td>
</tr>
<tr>
<td>server</td>
<td>drop</td>
<td>received on untrusted port</td>
<td>2</td>
</tr>
<tr>
<td>server</td>
<td>drop</td>
<td>unauthorized server</td>
<td>0</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>destination on untrusted port</td>
<td>0</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>untrusted option 82 field</td>
<td>0</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>bad DHCP release request</td>
<td>0</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>failed verify MAC check</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 10-1. An Example of the DHCP Snooping Command Output

Figure 10-2. Example of Show DHCP Snooping Statistics
Enabling DHCP Snooping on VLANS

DHCP snooping on VLANS is disabled by default. To enable DHCP snooping on a VLAN or range of VLANS enter this command:

```plaintext
HP Switch(config)# dhcp-snooping vlan <vlan-id-range>
```

You can also use this command in the vlan context, in which case you cannot enter a range of VLANS for snooping.

Below is an example of DHCP snooping enabled on VLAN 4.

```
HP Switch(config)# dhcp-snooping vlan 4
HP Switch(config)# show dhcp-snooping

DHCP Snooping Information

<table>
<thead>
<tr>
<th>DHCP Snooping</th>
<th>Enabled Vlans</th>
<th>Verify MAC</th>
<th>Option 82 untrusted policy</th>
<th>Option 82 Insertion</th>
<th>Option 82 remote-id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>4</td>
<td>Yes</td>
<td>drop</td>
<td>Yes</td>
<td>mac</td>
</tr>
</tbody>
</table>
```

**Figure 10-3. Example of DHCP Snooping on a VLAN**

Configuring DHCP Snooping Trusted Ports

By default, all ports are untrusted. To configure a port or range of ports as trusted, enter this command:

```plaintext
HP Switch(config)# dhcp-snooping trust <port-list>
```

You can also use this command in the interface context, in which case you are not able to enter a list of ports.
Configuring Advanced Threat Protection

DHCP Snooping

Figure 10-4. Example of Setting Trusted Ports

DHCP server packets are forwarded only if received on a trusted port; DHCP server packets received on an untrusted port are dropped.

Use the no form of the command to remove the trusted configuration from a port.

Configuring Authorized Server Addresses

If authorized server addresses are configured, a packet from a DHCP server must be received on a trusted port AND have a source address in the authorized server list in order to be considered valid. If no authorized servers are configured, all servers are considered valid. You can configure a maximum of 20 authorized servers.

To configure a DHCP authorized server address, enter this command in the global configuration context:

HP Switch(config)# dhcp-snooping authorized-server <ip-address>
Configuring Advanced Threat Protection
DHCP Snooping

Using DHCP Snooping with Option 82

DHCP adds Option 82 (relay information option) to DHCP request packets received on untrusted ports by default. (See “Configuring DHCP Relay” in the Management and Configuration Guide for more information on Option 82.)

When DHCP is enabled globally and also enabled on a VLAN, and the switch is acting as a DHCP relay, the settings for the DHCP relay Option 82 command are ignored when snooping is controlling Option 82 insertion. Option 82 inserted in this manner allows the association of the client’s lease with the correct port, even when another device is acting as a DHCP relay or when the server is on the same subnet as the client.

**Note**

DHCP snooping only overrides the Option 82 settings on a VLAN that has snooping enabled, not on VLANS without snooping enabled.
Configuring Advanced Threat Protection
DHCP Snooping

If DHCP snooping is enabled on a switch where an edge switch is also using DHCP snooping, it is desirable to have the packets forwarded so the DHCP bindings are learned. To configure the policy for DHCP packets from untrusted ports that already have Option 82 present, enter this command in the global configuration context.

Syntax:  [no] dhcp-snooping option 82 [remote-id <mac | subnet-ip | mgmt-ip>] [untrusted-policy <drop | keep | replace>]

Enables DHCP Option 82 insertion in the packet.

remote-id  Set the value used for the remote-id field of the relay information option.

mac: The switch mac address is used for the remote-id. This is the default.

subnet-ip: The IP address of the VLAN the packet was received on is used for the remote-id. If subnet-ip is specified but the value is not set, the MAC address is used.

mgmt-ip: The management VLAN IP address is used as the remote-id. If mgmt-ip is specified but the value is not set, the MAC address is used.

untrusted-policy  Configures DHCP snooping behavior when forwarding a DHCP packet from an untrusted port that already contains DHCP relay information (Option 82). The default is drop.

drop: The packet is dropped.

keep: The packet is forwarded without replacing the option information.

replace: The existing option is replaced with a new Option 82 generated by the switch.

Note  The default drop policy should remain in effect if there are any untrusted nodes, such as clients, directly connected to this switch.
Changing the Remote-id from a MAC to an IP Address

By default, DHCP snooping uses the MAC address of the switch as the remote-id in Option 82 additions. The IP address of the VLAN the packet was received on or the IP address of the management VLAN can be used instead by entering this command with the associated parameter:

```
HP Switch(config)# dhcp-snooping option 82 remote-id <mac|subnet-ip|mgmt-ip>
```

Figure 10-6. Example of DHCP Snooping Option 82 using the VLAN IP Address

Disabling the MAC Address Check

DHCP snooping drops DHCP packets received on untrusted ports when the check address (chaddr) field in the DHCP header does not match the source MAC address of the packet (default behavior). To disable this checking, use the `no` form of this command.

```
HP Switch(config)# dhcp-snooping verify mac
```
The DHCP Binding Database

DHCP snooping maintains a database of up to 8192 DHCP bindings on untrusted ports. Each binding consists of:

- Client MAC address
- Port number
- VLAN identifier
- Leased IP address
- Lease time

The switch can be configured to store the bindings at a specific URL so they will not be lost if the switch is rebooted. If the switch is rebooted, it will read its binding database from the specified location. To configure this location use this command.

**Syntax:**

```
[no] dhcp-snooping database [file<tftp://<ip-address>/<ascii-string>>] [delay<15-86400>][ time out<0-86400>]
```

- **file**  
  Must be in Uniform Resource Locator (URL) format — “tftp://ip-address/ascii-string”. The maximum filename length is 63 characters.

- **delay**  
  Number of seconds to wait before writing to the database. Default = 300 seconds.

- **timeout**  
  Number of seconds to wait for the database file transfer to finish before returning an error. A value of zero (0) means retry indefinitely. Default = 300 seconds.

---

HP Switch(config)# dhcp-snooping verify mac
HP Switch(config)# show dhcp-snooping

DHCP Snooping Information

DHCP Snooping : Yes
Enabled Vlans : 4
Verify MAC : yes
Option 82 untrusted policy : drop
Option 82 Insertion : Yes
Option 82 remote-id : subnet-ip

Figure 10-7. Example Showing the DHCP Snooping Verify MAC Setting
A message is logged in the system event log if the DHCP binding database fails to update.

To display the contents of the DHCP snooping binding database, enter this command.

**Syntax:**  
```
show dhcp-snooping binding
```

![Figure 10-8. Example Showing DHCP Snooping Binding Database Contents](image)

**Note**  
If a lease database is configured, the switch drops all DHCP packets until the lease database is read. This only occurs when the switch reboots and is completed quickly. If the switch is unable to read the lease database from the tftp server, it waits until that operation times out and then begins forwarding DHCP packets.

**Enabling Debug Logging**

To enable debug logging for DHCP snooping, use this command.

**Syntax:**  
```
[no] debug dhcp-snooping [agent | event | packet]
```

- **agent**  
  *Displays DHCP snooping agent messages.*
- **event**  
  *Displays DHCP snooping event messages.*
- **packet**  
  *Displays DHCP snooping packet messages.*

**Operational Notes**

- DHCP is not configurable from the WebAgent or menu interface.
- If packets are received at too high a rate, some may be dropped and need to be re-transmitted.
HP recommends running a time synchronization protocol such as SNTP in order to track lease times accurately.

A remote server must be used to save lease information or there may be a loss of connectivity after a switch reboot.

Log Messages

Server `<ip-address>` packet received on untrusted port `<port-number>` dropped. Indicates a DHCP server on an untrusted port is attempting to transmit a packet. This event is recognized by the reception of a DHCP server packet on a port that is configured as untrusted.

Ceasing untrusted server logs for `<duration>`. More than one packet was received from a DHCP server on an untrusted port. To avoid filling the log file with repeated attempts, untrusted server drop packet events will not be logged for the specified `<duration>`.

Client packet destined to untrusted port `<port-number>` dropped. Indicates that the destination of a DHCP client unicast packet is on an untrusted port. This event is recognized when a client unicast packet is dropped because the destination address is out a port configured as untrusted.

Ceasing untrusted port destination logs for `<duration>`. More than one client unicast packet with an untrusted port destination was dropped. To avoid filling the log file with repeated attempts, untrusted port destination attempts will not be logged for the specified `<duration>`.

Unauthorized server `<ip-address>` detected on port `<port-number>`. Indicates that an unauthorized DHCP server is attempting to send packets. This event is recognized when a server packet is dropped because there are configured authorized servers and a server packet is received from a server that is not configured as an authorized server.

Ceasing unauthorized server logs for `<duration>`. More than one unauthorized server packet was dropped. To avoid filling the log file with repeated attempts, unauthorized server transmit attempts will not be logged for the specified `<duration>`.

Received untrusted relay information from client `<mac-address>` on port `<port-number>`. Indicates the reception on an untrusted port of a client packet containing a relay information option field. This event is recognized when a client packet containing a relay information option field is dropped because it was received on a port configured as untrusted.
Ceasing untrusted relay information logs for <duration>. More than one DHCP client packet received on an untrusted port with a relay information field was dropped. To avoid filling the log file with repeated attempts, untrusted relay information packets will not be logged for the specified <duration>.

Client address <mac-address> not equal to source MAC <mac-address> detected on port <port-number>. Indicates that a client packet source MAC address does not match the “chaddr” field. This event is recognized when the dhcp-snooping agent is enabled to filter DHCP client packets that do not have a matching “chaddr” field and source MAC address.

Ceasing MAC mismatch logs for <duration>. More than one DHCP client packet with a mismatched source MAC and chaddr field was dropped. To avoid filling the log file with repeated attempts, client address mismatch events will not be logged for the specified <duration>.

Attempt to release address <ip-address> leased to port <port-number> detected on port <port-number> dropped. Indicates an attempt by a client to release an address when a DHCPRELEASE or DHCPDECLINE packet is received on a port different from the port the address was leased to.

Ceasing bad release logs for %s. More than one bad DHCP client release packet was dropped. To avoid filling the log file with repeated bad release dropped packets, bad releases will not be logged for <duration>.

Lease table is full, DHCP lease was not added. The lease table is full and this lease will not be added to it.

Write database to remote file failed errno (error-num). An error occurred while writing the temporary file and sending it using tftp to the remote server.

DHCP packets being rate-limited. Too many DHCP packets are flowing through the switch and some are being dropped.

Snooping table is full. The DHCP binding table is full and subsequent bindings are being dropped.
Dynamic ARP Protection

Introduction

On the VLAN interfaces of a routing switch, dynamic ARP protection ensures that only valid ARP requests and responses are relayed or used to update the local ARP cache. ARP packets with invalid IP-to-MAC address bindings advertised in the source protocol address and source physical address fields are discarded. For more information about the ARP cache, refer to “ARP Cache Table” in the Multicast and Routing Guide.

ARP requests are ordinarily broadcast and received by all devices in a broadcast domain. Most ARP devices update their IP-to-MAC address entries each time they receive an ARP packet even if they did not request the information. This behavior makes an ARP cache vulnerable to attacks.

Because ARP allows a node to update its cache entries on other systems by broadcasting or unicasting a gratuitous ARP reply, an attacker can send his own IP-to-MAC address binding in the reply that causes all traffic destined for a VLAN node to be sent to the attacker’s MAC address. As a result, the attacker can intercept traffic for other hosts in a classic ”man-in-the-middle” attack. The attacker gains access to any traffic sent to the poisoned address and can capture passwords, e-mail, and VoIP calls or even modify traffic before resending it.

Another way in which the ARP cache of known IP addresses and associated MAC addresses can be poisoned is through unsolicited ARP responses. For example, an attacker can associate the IP address of the network gateway with the MAC address of a network node. In this way, all outgoing traffic is prevented from leaving the network because the node does not have access to outside networks. As a result, the node is overwhelmed by outgoing traffic destined to another network.

Dynamic ARP protection is designed to protect your network against ARP poisoning attacks in the following ways:

- Allows you to differentiate between trusted and untrusted ports.
- Intercepts all ARP requests and responses on untrusted ports before forwarding them.
- Verifies IP-to-MAC address bindings on untrusted ports with the information stored in the lease database maintained by DHCP snooping and user-configured static bindings (in non-DHCP environments):
Configuring Advanced Threat Protection
Dynamic ARP Protection

- If a binding is valid, the switch updates its local ARP cache and forwards the packet.
- If a binding is invalid, the switch drops the packet, preventing other network devices from receiving the invalid IP-to-MAC information.

DHCP snooping intercepts and examines DHCP packets received on switch ports before forwarding the packets. DHCP packets are checked against a database of DHCP binding information. Each binding consists of a client MAC address, port number, VLAN identifier, leased IP address, and lease time. The DHCP binding database is used to validate packets by other security features on the switch. For more information, refer to “DHCP Snooping” in the Access Security Guide.

If you have already enabled DHCP snooping on a switch, you may also want to add static IP-to-MAC address bindings to the DHCP snooping database so that ARP packets from devices that have been assigned static IP addresses are also verified.

- Supports additional checks to verify source MAC address, destination MAC address, and IP address.
  
  ARP packets that contain invalid IP addresses or MAC addresses in their body that do not match the addresses in the Ethernet header are dropped.

When dynamic ARP protection is enabled, only ARP request and reply packets with valid IP-to-MAC address bindings in their packet header are relayed and used to update the ARP cache.

Dynamic ARP protection is implemented in the following ways on a switch:

- You can configure dynamic ARP protection only from the CLI; you cannot configure this feature from the WebAgent or menu interfaces.
- Line rate—Dynamic ARP protection copies ARP packets to the switch CPU, evaluates the packets, and then re-forwards them through the switch software. During this process, if ARP packets are received at too high a line rate, some ARP packets may be dropped and will need to be retransmitted.
- The SNMP MIB, HP-ICF-ARP-PROTECT-MIB, is created to configure dynamic ARP protection and to report ARP packet-forwarding status and counters.
Enabling Dynamic ARP Protection

To enable dynamic ARP protection for VLAN traffic on a routing switch, enter the `arp-protect vlan` command at the global configuration level.

**Syntax:**

```
[no] arp-protect vlan [vlan-range]
```

- `vlan-range`: Specifies a VLAN ID or a range of VLAN IDs from one to 4094; for example, `1-200`.

An example of the `arp-protect vlan` command is shown here:

```
HP Switch(config)# arp-protect vlan 1-101
```

Configuring Trusted Ports

In a similar way to DHCP snooping, dynamic ARP protection allows you to configure VLAN interfaces in two categories: trusted and untrusted ports. ARP packets received on trusted ports are forwarded without validation.

By default, all ports on a switch are untrusted. If a VLAN interface is untrusted:

- The switch intercepts all ARP requests and responses on the port.
- Each intercepted packet is checked to see if its IP-to-MAC binding is valid. If a binding is invalid, the switch drops the packet.

You must configure trusted ports carefully. For example, in the topology in Figure 10-9, Switch B may not see the leased IP address that Host 1 receives from the DHCP server. If the port on Switch B that is connected to Switch A is untrusted and if Switch B has dynamic ARP protection enabled, it will see ARP packets from Host 1 as invalid, resulting in a loss of connectivity.

On the other hand, if Switch A does not support dynamic ARP protection and you configure the port on Switch B connected to Switch A as trusted, Switch B opens itself to possible ARP poisoning from hosts attached to Switch A.
Figure 10-9. Configuring Trusted Ports for Dynamic ARP Protection

Take into account the following configuration guidelines when you use dynamic ARP protection in your network:

- You should configure ports connected to other switches in the network as trusted ports. In this way, all network switches can exchange ARP packets and update their ARP caches with valid information.
- Switches that do not support dynamic ARP protection should be separated by a router in their own Layer 2 domain. Because ARP packets do not cross Layer 2 domains, the unprotected switches cannot unknowingly accept ARP packets from an attacker and forward them to protected switches through trusted ports.

To configure one or more Ethernet interfaces that handle VLAN traffic as trusted ports, enter the `arp-protect trust` command at the global configuration level. The switch does not check ARP requests and responses received on a trusted port.

**Syntax:**

```plaintext
[no] arp-protect trust <port-list>
```

- **port-list**: Specifies a port number or a range of port numbers. Separate individual port numbers or ranges of port numbers with a comma; for example: `c1-c3, c6`.

An example of the `arp-protect trust` command is shown here:

```plaintext
HP Switch(config)# arp-protect trust b1-b4, d1
```
Adding an IP-to-MAC Binding to the DHCP Database

A routing switch maintains a DHCP binding database, which is used for DHCP and ARP packet validation. Both the DHCP snooping and DHCP Option 82 insertion features maintain the lease database by learning the IP-to-MAC bindings on untrusted ports. Each binding consists of the client MAC address, port number, VLAN identifier, leased IP address, and lease time.

If your network does not use DHCP or if some network devices have fixed, user-configured IP addresses, you can enter static IP-to-MAC address bindings in the DHCP binding database. The switch uses manually configured static bindings for DHCP snooping and dynamic ARP protection.

To add the static configuration of an IP-to-MAC binding for a port to the database, enter the `ip source-binding` command at the global configuration level.

**Syntax:**

```
[no] ip source-binding <mac-address> vlan <vlan-id> <ip-address> interface <port-number>
```

- **mac-address**: Specifies a MAC address to bind with a VLAN and IP address on the specified port in the DHCP binding database.
- **vlan <vlan-id>**: Specifies a VLAN ID number to bind with the specified MAC and IP addresses on the specified port in the DHCP binding database.
- **ip-address**: Specifies an IP address to bind with a VLAN and MAC address on the specified port in the DHCP binding database.
- **interface <port-number>**: Specifies the port number on which the IP-to-MAC address and VLAN binding is configured in the DHCP binding database.

An example of the `ip source-binding` command is shown here:

```
 HP Switch(config)# ip source-binding 0030c1-7f49c0 interface vlan 100 10.10.20.1 interface A4
```

**Note**

Note that the `ip source-binding` command is the same command used by the Dynamic IP Lockdown feature to configure static bindings. The Dynamic ARP Protection and Dynamic IP Lockdown features share a common list of source IP-to-MAC bindings.
Configuring Additional Validation Checks on ARP Packets

Dynamic ARP protection can be configured to perform additional validation checks on ARP packets. By default, no additional checks are performed. To configure additional validation checks, enter the `arp-protect validate` command at the global configuration level.

**Syntax:**  
```
(no) arp-protect validate <[src-mac] | [dest-mac] | [ip]>
```

- **src-mac** *(Optional)* Drops any ARP request or response packet in which the source MAC address in the Ethernet header does not match the sender MAC address in the body of the ARP packet.

- **dest-mac** *(Optional)* Drops any unicast ARP response packet in which the destination MAC address in the Ethernet header does not match the target MAC address in the body of the ARP packet.

- **ip** *(Optional)* Drops any ARP packet in which the sender IP address is invalid. Drops any ARP response packet in which the target IP address is invalid. Invalid IP addresses include: 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all Class E IP addresses.

You can configure one or more of the validation checks. The following example of the `arp-protect validate` command shows how to configure the validation checks for source MAC address and destination MAC address:

```
HP Switch(config)# arp-protect validate src-mac dest-mac
```

Verifying the Configuration of Dynamic ARP Protection

To display the current configuration of dynamic ARP protection, including the additional validation checks and the trusted ports that are configured, enter the `show arp-protect` command:
Configuring Advanced Threat Protection
Dynamic ARP Protection

Figure 10-1. The show arp-protect Command

Displaying ARP Packet Statistics

To display statistics about forwarded ARP packets, dropped ARP packets, MAC validation failure, and IP validation failures, enter the `show arp-protect statistics <vid-range>` command:

```
HP Switch(config)# show arp-protect
ARP Protection Information

Enabled Vlans : 1-4094
Validate : dest-mac, src-mac

Port Trust
----- -----
B1    Yes
B2    Yes
B3    No
B4    No
B5    No
```

```
HP Switch(config)# show arp-protect statistics 1-2
Status and Counters - ARP Protection Counters for VLAN 1

Forwarded pkts : 10     Bad source mac : 2
Bad bindings    : 1      Bad destination mac: 1
Malformed pkts : 0      Bad IP address     : 0

Status and Counters - ARP Protection Counters for VLAN 2

Forwarded pkts : 1      Bad source mac : 1
Bad bindings    : 1      Bad destination mac: 1
Malformed pkts : 1      Bad IP address     : 1
```

Figure 10-2. Show arp-protect statistics Command
Monitoring Dynamic ARP Protection

When dynamic ARP protection is enabled, you can monitor and troubleshoot the validation of ARP packets with the `debug arp-protect` command. Use this command when you want to debug the following conditions:

- The switch is dropping valid ARP packets that should be allowed.
- The switch is allowing invalid ARP packets that should be dropped.

```
HP Switch(config)# debug arp-protect
1. ARP request is valid
   "DARPP: Allow ARP request 000000-000001, 10.0.0.1 for 10.0.0.2 port A1, vlan "

2. ARP request detected with an invalid binding
   "DARPP: Deny ARP request 000000-000003, 10.0.0.1 port A1, vlan 1"

3. ARP response with a valid binding
   "DARPP: Allow ARP reply 000000-000002, 10.0.0.2 port A2, vlan 1"

4. ARP response detected with an invalid binding
   "DARPP: Deny ARP reply 000000-000003, 10.0.0.2 port A2, vlan 1"
```

Figure 10-3. Example of `debug arp-protect` Command

Dynamic IP Lockdown

The Dynamic IP Lockdown feature is used to prevent IP source address spoofing on a per-port and per-VLAN basis. When dynamic IP lockdown is enabled, IP packets in VLAN traffic received on a port are forwarded only if they contain a known source IP address and MAC address binding for the port. The IP-to-MAC address binding can either be statically configured or learned by the DHCP Snooping feature.
Protection Against IP Source Address Spoofing

Many network attacks occur when an attacker injects packets with forged IP source addresses into the network. Also, some network services use the IP source address as a component in their authentication schemes. For example, the BSD “r” protocols (rlogin, rcp, rsh) rely on the IP source address for packet authentication. SNMPv1 and SNMPv2c also frequently use authorized IP address lists to limit management access. An attacker that is able to send traffic that appears to originate from an authorized IP source address may gain access to network services for which he is not authorized.

Dynamic IP lockdown provides protection against IP source address spoofing by means of IP-level port security. IP packets received on a port enabled for dynamic IP lockdown are only forwarded if they contain a known IP source address and MAC address binding for the port.

Dynamic IP lockdown uses information collected in the DHCP Snooping lease database and through statically configured IP source bindings to create internal, per-port lists. The internal lists are dynamically created from known IP-to-MAC address bindings to filter VLAN traffic on both the source IP address and source MAC address.

Prerequisite: DHCP Snooping

Dynamic IP lockdown requires that you enable DHCP snooping as a prerequisite for its operation on ports and VLAN traffic:

- Dynamic IP lockdown only enables traffic for clients whose leased IP addresses are already stored in the lease database created by DHCP snooping or added through a static configuration of an IP-to-MAC binding. Therefore, if you enable DHCP snooping after dynamic IP lockdown is enabled, clients with an existing DHCP-assigned address must either request a new leased IP address or renew their existing DHCP-assigned address. Otherwise, a client’s leased IP address is not contained in the DHCP binding database. As a result, dynamic IP lockdown will not allow inbound traffic from the client.

- It is recommended that you enable DHCP snooping a week before you enable dynamic IP lockdown to allow the DHCP binding database to learn clients’ leased IP addresses. You must also ensure that the lease time for the information in the DHCP binding database lasts more than a week. Alternatively, you can configure a DHCP server to re-allocate IP addresses to DHCP clients. In this way, you repopulate the lease database with current IP-to-MAC bindings.
The DHCP binding database allows VLANs enabled for DHCP snooping to be known on ports configured for dynamic IP lockdown. As new IP-to-MAC address and VLAN bindings are learned, a corresponding permit rule is dynamically created and applied to the port (preceding the final deny any vlan <VLAN_IDS> rule as shown in the example in Figure 10-4. These VLAN_IDs correspond to the subset of configured and enabled VLANS for which DHCP snooping has been configured.

For dynamic IP lockdown to work, a port must be a member of at least one VLAN that has DHCP snooping enabled.

Disabling DHCP snooping on a VLAN causes Dynamic IP bindings on Dynamic IP Lockdown-enabled ports in this VLAN to be removed. The port reverts back to switching traffic as usual.

Filtering IP and MAC Addresses Per-Port and Per-VLAN

This section contains an example that shows the following aspects of the Dynamic IP Lockdown feature:

- Internal Dynamic IP lockdown bindings dynamically applied on a per-port basis from information in the DHCP Snooping lease database and statically configured IP-to-MAC address bindings
- Packet filtering using source IP address, source MAC address, and source VLAN as criteria

In this example, the following DHCP leases have been learned by DHCP snooping on port 5. VLANs 2 and 5 are enabled for DHCP snooping.

**Table 1. Sample DHCP Snooping Entries**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.8.5</td>
<td>001122-334455</td>
<td>2</td>
</tr>
<tr>
<td>10.0.8.7</td>
<td>001122-334477</td>
<td>2</td>
</tr>
<tr>
<td>10.0.10.3</td>
<td>001122-334433</td>
<td>5</td>
</tr>
</tbody>
</table>

The following example shows an IP-to-MAC address and VLAN binding that have been statically configured in the lease database on port 5.

**Table 2. Sample Static DHCP Snooping Entries**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.10.1</td>
<td>001122-110011</td>
<td>5</td>
</tr>
</tbody>
</table>
Assuming that DHCP snooping is enabled and that port 5 is untrusted, dynamic IP lockdown applies the following dynamic VLAN filtering on port 5:

```plaintext
permit 10.0.8.5 001122-334455 vlan 2
permit 10.0.8.7 001122-334477 vlan 2
permit 10.0.10.3 001122-334433 vlan 5
permit 10.0.10.1 001122-110011 vlan 5
deny any vlan 1-10
permit any
```

**Figure 10-4. Example of Internal Statements used by Dynamic IP Lockdown**

Note that the `deny any` statement is applied only to VLANs for which DHCP snooping is enabled. The `permit any` statement is applied only to all other VLANs.

### Enabling Dynamic IP Lockdown

To enable dynamic IP lockdown on all ports or specified ports, enter the `ip source-lockdown` command at the global configuration level. Use the `no` form of the command to disable dynamic IP lockdown.

**Syntax:**  
```plaintext
[no] ip source-lockdown <port-list>
```

*Enables dynamic IP lockdown globally on all ports or on specified ports on the routing switch.*

### Operating Notes

- Dynamic IP lockdown is enabled at the port configuration level and applies to all bridged or routed IP packets entering the switch. The only IP packets that are exempt from dynamic IP lockdown are broadcast DHCP request packets, which are handled by DHCP snooping.
- DHCP snooping is a prerequisite for Dynamic IP Lockdown operation. The following restrictions apply:
  - DHCP snooping is required for dynamic IP lockdown to operate. To enable DHCP snooping, enter the `dhcp-snooping` command at the global configuration level.
• Dynamic IP lockdown only filters packets in VLANs that are enabled for DHCP snooping. In order for Dynamic IP lockdown to work on a port, the port must be configured for at least one VLAN that is enabled for DHCP snooping.

To enable DHCP snooping on a VLAN, enter the `dhcp-snooping vlan [vlan-id-range]` command at the global configuration level or the `dhcp-snooping` command at the VLAN configuration level.

• Dynamic IP lockdown is not supported on a trusted port. (However, note that the DHCP server must be connected to a trusted port when DHCP snooping is enabled.)

By default, all ports are untrusted. To remove the trusted configuration from a port, enter the `no dhcp-snooping trust <port-list>` command at the global configuration level.

For more information on how to configure and use DHCP snooping, see “DHCP Snooping” on page 10-3.

■ After you enter the `ip source-lockdown` command (enabled globally with the desired ports entered in `<port-list>`), the dynamic IP lockdown feature remains disabled on a port if any of the following conditions exist:
  • If DHCP snooping has not been globally enabled on the switch.
  • If the port is not a member of at least one VLAN that is enabled for DHCP snooping.
  • If the port is configured as a trusted port for DHCP snooping.

Dynamic IP lockdown is activated on the port only after you make the following configuration changes:
  • Enable DHCP snooping on the switch.
  • Configure the port as a member of a VLAN that has DHCP snooping enabled.
  • Remove the trusted-port configuration.

■ You can configure dynamic IP lockdown only from the CLI; this feature cannot be configured from the WebAgent or menu interface.

■ If you enable dynamic IP lockdown on a port, you cannot add the port to a trunk.

■ Dynamic IP lockdown must be removed from a trunk before the trunk is removed.
Configuring Advanced Threat Protection
Dynamic IP Lockdown

Adding an IP-to-MAC Binding to the DHCP Binding Database

A switch maintains a DHCP binding database, which is used for dynamic IP lockdown as well as for DHCP and ARP packet validation. The DHCP snooping feature maintains the lease database by learning the IP-to-MAC bindings of VLAN traffic on untrusted ports. Each binding consists of the client MAC address, port number, VLAN identifier, leased IP address, and lease time.

Dynamic IP lockdown supports a total of 4K static and dynamic bindings with up to 64 bindings per port. When DHCP snooping is enabled globally on a VLAN, dynamic bindings are learned when a client on the VLAN obtains an IP address from a DHCP server. Static bindings are created manually with the CLI or from a downloaded configuration file.

When dynamic IP lockdown is enabled globally or on ports the bindings associated with the ports are written to hardware. This occurs during these events:

- Switch initialization
- Hot swap
- A dynamic IP lockdown-enabled port is moved to a DHCP snooping-enabled VLAN
- DHCP snooping or dynamic IP lockdown characteristics are changed such that dynamic IP lockdown is enabled on the ports

Potential Issues with Bindings

- When dynamic IP lockdown enabled, and a port or switch has the maximum number of bindings configured, the client DHCP request will be dropped and the client will not receive an IP address through DHCP.
- When dynamic IP lockdown is enabled and a port is configured with the maximum number of bindings, adding a static binding to the port will fail.
- When dynamic IP lockdown is enabled globally, the bindings for each port are written to hardware. If global dynamic IP lockdown is enabled and disabled several times, it is possible to run out of buffer space for additional bindings. The software will delay adding the bindings to hardware until resources are available.
Adding a Static Binding

To add the static configuration of an IP-to-MAC binding for a port to the lease database, enter the `ip source-binding` command at the global configuration level. Use the `no` form of the command to remove the IP-to-MAC binding from the database.

**Syntax:**
```
[no] ip source-binding <vlan-id> <ip-address> <mac-address> <port-number>
```

- **vlan-id**  
  Specifies a valid VLAN ID number to bind with the specified MAC and IP addresses on the port in the DHCP binding database.

- **ip-address**  
  Specifies a valid client IP address to bind with a VLAN and MAC address on the port in the DHCP binding database.

- **mac-address**  
  Specifies a valid client MAC address to bind with a VLAN and IP address on the port in the DHCP binding database.

- **port-number**  
  Specifies the port number on which the IP-to-MAC address and VLAN binding is configured in the DHCP binding database.

**Note**

Note that the `ip source-binding` command is the same command used by the Dynamic ARP Protection feature to configure static bindings. The Dynamic ARP Protection and Dynamic IP Lockdown features share a common list of source IP-to-MAC address bindings.

Verifying the Dynamic IP Lockdown Configuration

To display the ports on which dynamic IP lockdown is configured, enter the `show ip source-lockdown status` command at the global configuration level.

**Syntax:**
```
show ip source-lockdown status
```
An example of the `show ip source-lockdown status` command output is shown in Figure 10-5. Note that the operational status of all switch ports is displayed. This information indicates whether or not dynamic IP lockdown is supported on a port.

![HP Switch(config)# show ip source-lockdown status]

Dynamic IP Lockdown (DIPLD) Information

<table>
<thead>
<tr>
<th>Port</th>
<th>Operational State</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Active</td>
</tr>
<tr>
<td>A2</td>
<td>Not in DHCP Snooping vlan</td>
</tr>
<tr>
<td>A3</td>
<td>Disabled</td>
</tr>
<tr>
<td>A4</td>
<td>Disabled</td>
</tr>
<tr>
<td>A5</td>
<td>Trusted port, Not in DHCP Snooping vlan</td>
</tr>
</tbody>
</table>

Figure 10-5. Example of show ip source-lockdown status Command Output

Displaying the Static Configuration of IP-to-MAC Bindings

To display the static configurations of IP-to-MAC bindings stored in the DHCP lease database, enter the `show ip source-lockdown bindings` command.

**Syntax:**

```
show ip source-lockdown bindings [port-number]
```

`port-number` *(Optional)* Specifies the port number on which source IP-to-MAC address and VLAN bindings are configured in the DHCP lease database.

An example of the `show ip source-lockdown bindings` command output is shown in Figure 10-6.
In the `show ip source-lockdown bindings` command output, the “Not in HW” column specifies whether or not (YES or NO) a statically configured IP-to-MAC and VLAN binding on a specified port has been combined in the lease database maintained by the DHCP Snooping feature.

### Debugging Dynamic IP Lockdown

To enable the debugging of packets dropped by dynamic IP lockdown, enter the `debug dynamic-ip-lockdown` command.

**Syntax:** `debug dynamic-ip-lockdown`

To send command output to the active CLI session, enter the `debug destination session` command.

Counters for denied packets are displayed in the `debug dynamic-ip-lockdown` command output. Packet counts are updated every five minutes. An example of the command output is shown in Figure 10-7.

When dynamic IP lockdown drops IP packets in VLAN traffic that do not contain a known source IP-to-MAC address binding for the port on which the packets are received, a message is entered in the event log.

---

**Figure 10-6. Example of show ip source-lockdown bindings Command Output**

<table>
<thead>
<tr>
<th>Mac Address</th>
<th>IP Address</th>
<th>VLAN</th>
<th>Port</th>
<th>Not in HW</th>
</tr>
</thead>
<tbody>
<tr>
<td>001122-334455</td>
<td>10.10.10.1</td>
<td>1111</td>
<td>X11</td>
<td></td>
</tr>
<tr>
<td>005544-332211</td>
<td>10.10.10.2</td>
<td>2222</td>
<td>Trk11</td>
<td>YES</td>
</tr>
</tbody>
</table>

---
Differences Between Switch Platforms

There are some differences in the feature set and operation of Dynamic IP Lockdown, depending on the switch on which it is implemented. These are listed below.

- There is no restriction on GVRP on 3500/5400 switches. On 2600/2800/3400 switches, Dynamic IP Lockdown is not supported if GVRP is enabled on the switch.

- Dynamic IP Lockdown has the host limits shown in the table below. There is a DHCP snooping limit of 8,192 entries.
Configuring Advanced Threat Protection
Dynamic IP Lockdown

<table>
<thead>
<tr>
<th>Switch</th>
<th>Number of Hosts</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>3500/5400</td>
<td>64 bindings per port  Up to 4096 manual bindings per switch</td>
<td>This limit is shared with DHCP snooping because they both use the snooping database.</td>
</tr>
<tr>
<td>3400/2800</td>
<td>32 bindings per port; up to 512 manual bindings  Up to 32 VLANs with DHCP snooping enabled</td>
<td>This is not guaranteed as the hardware resources are shared with QoS.</td>
</tr>
<tr>
<td>2610</td>
<td>8 bindings per port; up to 512 manual bindings  Globally 118 to 125 hosts  Up to 8 VLANs with DHCP snooping enabled</td>
<td>This is not guaranteed as the hardware resources are shared with IDM ACLs. The number of global bindings available is based on the number of DHCP snooping-enabled VLANs (1-8).</td>
</tr>
<tr>
<td>2600</td>
<td>8 bindings per port; up to 512 manual bindings  Up to 8 VLANs with DHCP snooping enabled</td>
<td>This is not guaranteed as the hardware resources are shared with QoS.</td>
</tr>
</tbody>
</table>

- A source is considered “trusted” for all VLANs if it is seen on any VLAN without DHCP snooping enabled.
- On the HP switch series 5400 and 3500, dynamic IP lockdown is supported on a port configured for statically configured port-based ACLs.
Using the Instrumentation Monitor

The instrumentation monitor can be used to detect anomalies caused by security attacks or other irregular operations on the switch. The following table shows the operating parameters that can be monitored at predetermined intervals, and the possible security attacks that may trigger an alert:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pkts-to-closed-ports</td>
<td>The count of packets per minute sent to closed TCP/UDP ports. An excessive amount of packets could indicate a port scan, in which an attacker is attempting to expose a vulnerability in the switch.</td>
</tr>
<tr>
<td>arp-requests</td>
<td>The count of ARP requests processed per minute. A large amount of ARP request packets could indicate an host infected with a virus that is trying to spread itself.</td>
</tr>
<tr>
<td>ip-address-count</td>
<td>The number of destination IP addresses learned in the IP forwarding table. Some attacks fill the IP forwarding table causing legitimate traffic to be dropped.</td>
</tr>
<tr>
<td>system-resource-usage</td>
<td>The percentage of system resources in use. Some Denial-of-Service (DoS) attacks will cause excessive system resource usage, resulting in insufficient resources for legitimate traffic.</td>
</tr>
<tr>
<td>login-failures/min</td>
<td>The count of failed CLI login attempts or SNMP management authentication failures. This indicates an attempt has been made to manage the switch with an invalid login or password. Also, it might indicate a network management station has not been configured with the correct SNMP authentication parameters for the switch.</td>
</tr>
<tr>
<td>port-auth-failures/min</td>
<td>The count of times a client has been unsuccessful logging into the network</td>
</tr>
<tr>
<td>system-delay</td>
<td>The response time, in seconds, of the CPU to new network events such as BPDU packets or packets for other network protocols. Some DoS attacks can cause the CPU to take too long to respond to new network events, which can lead to a breakdown of Spanning Tree or other features. A delay of several seconds indicates a problem.</td>
</tr>
<tr>
<td>mac-address-count</td>
<td>The number of MAC addresses learned in the forwarding table. Some attacks fill the forwarding table so that new conversations are flooded to all parts of the network.</td>
</tr>
<tr>
<td>mac-moves/min</td>
<td>The average number of MAC address moves from one port to another per minute. This usually indicates a network loop, but can also be caused by DoS attacks.</td>
</tr>
<tr>
<td>learn-discards/min</td>
<td>Number of MAC address learn events per minute discarded to help free CPU resources when busy.</td>
</tr>
</tbody>
</table>
Operating Notes

- To generate alerts for monitored events, you must enable the instrumentation monitoring log and/or SNMP trap. The threshold for each monitored parameter can be adjusted to minimize false alarms (see “Configuring Instrumentation Monitor” on page 10-36).

- When a parameter exceeds its threshold, an alert (event log message and/or SNMP trap) is generated to inform network administrators of this condition. The following example shows an event log message that occurs when the number of MAC addresses learned in the forwarding table exceeds the configured threshold:

<table>
<thead>
<tr>
<th>Standard Date/Time Prefix for Event Log Messages</th>
<th>“inst-mon” label indicates an Instrumentation Monitor event</th>
<th>Monitored Parameter</th>
<th>Threshold Value</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>W 05/27/06 12:10:16</td>
<td>inst-mon: Limit for MAC addr count (300) is exceeded (321)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 10-8. Example of Event Log Message generated by Instrumentation Monitor

- Alerts are automatically rate limited to prevent filling the log file with redundant information. The following is an example of alerts that occur when the device is continually subject to the same attack (too many MAC addresses in this instance):

| W 01/01/90 00:05:00 | inst-mon: Limit for MAC addr count (300) is exceeded (321) |
| W 01/01/90 00:10:00 | inst-mon: Limit for MAC addr count (300) is exceeded (323) |
| W 01/01/90 00:15:00 | inst-mon: Limit for MAC addr count (300) is exceeded (322) |
| W 01/01/90 00:20:00 | inst-mon: Limit for MAC addr count (300) is exceeded (324) |
| W 01/01/90 00:20:00 | inst-mon: Ceasing logs for MAC addr count for 15 minutes |

Figure 10-9. Example of rate limiting when multiple messages are generated

In the preceding example, if a condition is reported 4 times (persists for more than 15 minutes) then alerts cease for 15 minutes. If after 15 minutes the condition still exists, the alerts cease for 30 minutes, then for 1 hour, 2 hours, 4 hours, 8 hours, and after that the persisting condition is reported once a day. As with other event log entries, these alerts can be sent to a syslog server.

- Known Limitations: The instrumentation monitor runs once every five minutes. The current implementation does not track information such as the port, MAC, and IP address from which an attack is received.
Configuring Instrumentation Monitor

The following commands and parameters are used to configure the operational thresholds that are monitored on the switch. By default, the instrumentation monitor is disabled.

**Syntax:** [no] instrumentation monitor [parameterName|all] [<low|med|high|limitValue>]

- `[log]`: Enables/disables instrumentation monitoring log so that event log messages are generated every time there is an event which exceeds a configured threshold.
  (Default threshold setting when instrumentation monitoring is enabled: `enabled`)
- `[all]`: Enables/disables all counter types on the switch but does not enable/disable instrumentation monitor logging.
  (Default threshold setting when enabled: see parameter listings below)
- `[arp-requests]`: The number of arp requests that are processed each minute.
  (Default threshold setting when enabled: 1000 (med))
- `[ip-address-count]`: The number of destination IP addresses learned in the IP forwarding table.
  (Default threshold setting when enabled: 1000 (med))
- `[learn-discards]`: The number of MAC address learn events per minute discarded to help free CPU resources when busy.
  (Default threshold setting when enabled: 100 (med))
- `[login-failures]`: The count of failed CLI login attempts or SNMP management authentication failures per hour.
  (Default threshold setting when enabled: 10 (med))
- `[mac-address-count]`: The number of MAC addresses learned in the forwarding table.
  You must enter a specific value in order to enable this feature.
  (Default threshold setting when enabled: 1000 (med))
- `[mac-moves]`: The average number of MAC address moves per minute from one port to another.
  (Default threshold setting when enabled: 100 (med))
- `[pkts-to-closed-ports]`: The count of packets per minute sent to closed TCP/UDP ports.
  (Default threshold setting when enabled: 10 (med))
- `[port-auth-failures]`: The count of times per minute that a client has been unsuccessful logging into the network.
  (Default threshold setting when enabled: 10 (med))
- `[system-resource-usage]`: The percentage of system resources in use.
  (Default threshold setting when enabled: 50 (med))
- `[system-delay]`: The response time, in seconds, of the CPU to new network events such as BPDU packets or packets for other network protocols.
  (Default threshold setting when enabled: 3 seconds (med))
- `[trap]`: Enables or disables SNMP trap generation.
  (Default setting when instrumentation monitoring is enabled: disabled)
To enable instrumentation monitor using the default parameters and thresholds, enter the general `instrumentation monitor` command. To adjust specific settings, enter the name of the parameter that you wish to modify, and revise the threshold limits as needed.

**Examples**

To turn on monitoring and event log messaging with the default medium values:

```
HP Switch(config)# instrumentation monitor
```

To turn off monitoring of the system delay parameter:

```
HP Switch(config)# no instrumentation monitor system-delay
```

To adjust the alert threshold for the MAC address count to the low value:

```
HP Switch(config)# instrumentation monitor mac-address-count low
```

To adjust the alert threshold for the MAC address count to a specific value:

```
HP Switch(config)# instrumentation monitor mac-address-count 767
```

To enable monitoring of learn discards with the default medium threshold value:

```
HP Switch(config)# instrumentation monitor learn-discards
```

To disable monitoring of learn discards:

```
HP Switch(config)# no instrumentation monitor learn-discards
```

To enable or disable SNMP trap generation:

```
HP Switch(config)# [no] instrumentation monitor trap
```
Viewing the Current Instrumentation Monitor Configuration

The **show instrumentation monitor configuration** command displays the configured thresholds for monitored parameters.

```
HP Switch# show instrumentation monitor configuration

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>LIMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address-count</td>
<td>1000 (med)</td>
</tr>
<tr>
<td>ip-address-count</td>
<td>1000 (med)</td>
</tr>
<tr>
<td>system-resource-usage</td>
<td>50 (med)</td>
</tr>
<tr>
<td>system-delay</td>
<td>5 (high)</td>
</tr>
<tr>
<td>mac-moves/min</td>
<td>100 (med)</td>
</tr>
<tr>
<td>learn-discards/min</td>
<td>100 (med)</td>
</tr>
<tr>
<td>ip-port-scans/min</td>
<td>10 (med)</td>
</tr>
<tr>
<td>arp-requests/min</td>
<td>100 (low)</td>
</tr>
<tr>
<td>login-failures/min</td>
<td>10 (med)</td>
</tr>
<tr>
<td>port-auth-failures/min</td>
<td>10 (med)</td>
</tr>
</tbody>
</table>

SNMP trap generation for alerts: enabled
Instrumentation monitoring log: enabled
```

Figure 10-10. Viewing the Instrumentation Monitor Configuration

An alternate method of determining the current Instrumentation Monitor configuration is to use the **show run** command. However, the show run command output does not display the threshold values for each limit set.
Traffic/Security Filters and Monitors

Overview

**Applicable Switch Models.** As of June, 2010, Traffic/Security filters are available on these current HP switch models:

<table>
<thead>
<tr>
<th>Models</th>
<th>Source-Port Filters</th>
<th>Protocol Filters</th>
<th>Multicast Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>8200zl Switches</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6600 Switches</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6400cl Switches</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5400zl Switches</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4200vl Switches</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>3500/3500yl Switches</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3400cl Switches</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2910al Switches</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2800 Switches</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2510 Switches</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2500 Switches</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4000m and 8000m Switches</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

This chapter describes Traffic/Security filters on the switches covered in this guide. For information on filters for other HP switches in the above table or switches not listed here, refer to the documentation provided for those switches.
Traffic/Security Filters and Monitors

Introduction

You can enhance in-band security and improve control over access to network resources by configuring static filters to forward (the default action) or drop unwanted traffic. That is, you can configure a traffic filter to either forward or drop all network traffic moving to outbound (destination) ports and trunks (if any) on the switch.

Filter Limits

The switch accepts up to 101 static filters. These limitations apply:

- Source-port filters: up to 78
- Multicast filters: up to 16 with 1024 or fewer VLANs configured. Up to 8 with more than 1024 VLANs configured.
- Protocol filters: up to 7

Using Port Trunks with Filters

The switch manages a port trunk as a single source or destination for source-port filtering. If you configure a port for filtering before adding it to a port trunk, the port retains the filter configuration, but suspends the filtering action while a member of the trunk. If you want a trunk to perform filtering, first configure the trunk, then configure the trunk for filtering. Refer to “Configuring a Filter on a Port Trunk” on page 11-18.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>WebAgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure source-port filters</td>
<td>none</td>
<td>n/a</td>
<td>page 11-20</td>
<td>n/a</td>
</tr>
<tr>
<td>configure protocol filters</td>
<td>none</td>
<td>n/a</td>
<td>page 11-20</td>
<td>n/a</td>
</tr>
<tr>
<td>configure multicast filters</td>
<td>none</td>
<td>n/a</td>
<td>page 11-20</td>
<td>n/a</td>
</tr>
<tr>
<td>display filter data</td>
<td>n/a</td>
<td>n/a</td>
<td>page 11-22</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Filter Types and Operation

Table 11-1. Filter Types and Criteria

<table>
<thead>
<tr>
<th>Static Filter Type</th>
<th>Selection Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-Port</td>
<td>Inbound traffic from a designated, physical source-port will be forwarded or dropped on a per-port (destination) basis.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Inbound traffic having a specified multicast MAC address will be forwarded to outbound ports (the default) or dropped on a per-port (destination) basis.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Inbound traffic having the selected frame (protocol) type will be forwarded or dropped on a per-port (destination) basis.</td>
</tr>
</tbody>
</table>

Source-Port Filters

This filter type enables the switch to forward or drop traffic from all end nodes on the indicated source-port to specific destination ports.

![Figure 11-1. Example of a Source-Port Filter Application](image_url)

Operating Rules for Source-Port Filters

- You can configure one source-port filter for each physical port and port trunk on the switch. (Refer to the `filter` command on page 11-17.)
You can include all destination ports and trunks in the switch on a single source-port filter.

Each source-port filter includes:
- One source port or port trunk (trk1, trk2, ... trkn)
- A set of destination ports and/or port trunks that includes all untrunked LAN ports and port trunks on the switch
- An action (forward or drop) for each destination port or port trunk

When you create a source-port filter, the switch automatically sets the filter to forward traffic from the designated source to all destinations for which you do not specifically configure a “drop” action. Thus, it is not necessary to configure a source-port filter for traffic you want the switch to forward unless the filter was previously configured to drop the desired traffic.

When you create a source port filter, all ports and port trunks (if any) on the switch appear as destinations on the list for that filter, even if routing is disabled and separate VLANs and/or subnets exist. Where traffic would normally be allowed between ports and/or trunks, the switch automatically forwards traffic to the outbound ports and/or trunks you do not specifically configure to drop traffic. (Destination ports that comprise a trunk are listed collectively by the trunk name—such as Trk1—instead of by individual port name.)

Packets allowed for forwarding by a source-port filter are subject to the same operation as inbound packets on a port that is not configured for source-port filtering.

With multiple IP addresses configured on a VLAN, and routing enabled on the switch, a single port or trunk can be both the source and destination of packets moving between subnets in that same VLAN. In this case, you can prevent the traffic of one subnet from being routed to another subnet of the same port by configuring the port or trunk as both the source and destination for traffic to drop.

Example

If you wanted to prevent server “A” from receiving traffic sent by workstation “X”, but do not want to prevent any other servers or end nodes from receiving traffic from workstation “X”, you would configure a filter to drop traffic from port 5 to port 7. The resulting filter would drop traffic from port 5 to port 7, but would forward all other traffic from any source port to any destination port. (Refer to figures 11-2 and 11-3.)
Traffic/Security Filters and Monitors
Filter Types and Operation

Figure 11-2. Example of a Filter Blocking Traffic only from Port 5 to Server "A"

Figure 11-3. The Filter for the Actions Shown in Figure 11-2

Named Source-Port Filters

You can specify named source-port filters that may be used on multiple ports and port trunks. A port or port trunk can only have one source-port filter, but by using this capability you can define a source-port filter once and apply it to multiple ports and port trunks. This can make it easier to configure and manage source-port filters on your switch. The commands to define, configure, apply, and display the status of named source-port filters are described below.
Operating Rules for Named Source-Port Filters

- A port or port trunk may only have one source-port filter, named or not named.
- A named source-port filter can be applied to multiple ports or port trunks.
- Once a named source-port filter is defined, subsequent changes only modify its action, they don’t replace it.
- To change the named source-port filter used on a port or port trunk, the current filter must first be removed, using the `no filter source-port named-filter <filter-name>` command.
- A named source-port filter can only be deleted when it is not applied to any ports.

Defining and Configuring Named Source-Port Filters

The named source-port filter command operates from the global configuration level.

**Syntax:** `[no] filter source-port named-filter <filter-name>

Defines or deletes a named source-port filter. The `<filter-name>` may contain a maximum of 20 alpha-numeric characters (longer names may be specified, but they are not displayed.) A filter-name cannot be a valid port or port trunk name.

The maximum number of named source-port filters that can be used is equal to the number of ports on a switch.

A named source-port filter can only be removed if it is not in use (use the `show filter source-port` command to check the status). Named source-port filters are not automatically deleted when they are no longer used.

Use the `no` option to delete an unused named source-port filter.
Traffic/Security Filters and Monitors
Filter Types and Operation

Syntax: filter source-port named-filter <filter-name> drop <destination-port-list>

Configures the named source-port filter to drop traffic having a destination on the ports and/or port trunks in the <destination-port-list>. Can be followed by the forward option if you have other destination ports or port trunks previously set to drop that you want to change to forward. For example:

filter source-port named-filter <filter-name> drop <destination-port-list> forward <destination-port-list>

The destination-port-list may contain ports, port trunks, and ranges (for example 3-7 or trk4-trk9) separated by commas.

Syntax: filter source-port named-filter <filter-name> forward <destination-port-list>

Configures the named source-port filter to forward traffic having a destination on the ports and/or port trunks in the <destination-port-list>. Since “forward” is the default state for destinations in a filter, this command is useful when destinations in an existing filter are configured for “drop” and you want to change them to “forward”. Can be followed by the drop option if you have other destination ports set to forward that you want to change to drop. For example:

filter source-port named-filter <filter-name> forward <destination-port-list> drop <destination-port-list>

A named source-port filter must first be defined and configured before it can be applied. In the following example two named source-port filters are defined, web-only and accounting.

HP Switch(config)# filter source-port named-filter web-only

HP Switch(config)# filter source-port named-filter accounting

By default, these two named source-port filters forward traffic to all ports and port trunks.

To configure a named source-port filter to prevent inbound traffic from being forwarded to specific destination switch ports or port trunks, the drop option is used. For example, on a 26-port switch, to configure the named source-port filter web-only to drop any traffic except that for destination ports 1 and 2, the following command would be used:

HP Switch(config)# filter source-port named-filter web-only drop 3-26

A named source-port filter can be defined and configured in a single command by adding the drop option, followed by the required destination-port-list.
Viewing a Named Source-Port Filter

You can list all source-port filters configured in the switch, both named and unnamed, and their action using the `show` command below.

**Syntax:** `show filter source-port`

Displays a listing of configured source-port filters, where each filter entry includes a Filter Name, Port List, and Action:

- **Filter Name:** The filter-name used when a named source-port filter is defined. Non-named source-port filters are automatically assigned the port or port trunk number of the source port.
- **Port List:** Lists the port and port trunk destinations using the filter. Named source-port filters that are not in use display `NOT USED`.
- **Action:** Lists the ports and port trunks dropped by the filter. If a named source-port filter has been defined but not configured, this field is blank.

For the supplied index (IDX) displays the action taken (Drop or Forward) for each destination port on the switch.

Using Named Source-Port Filters

A company wants to manage traffic to the Internet and its accounting server on a 26-port switch. Their network is pictured in Figure 11-4. Switch port 1 connects to a router that provides connectivity to a WAN and the Internet. Switch port 7 connects to the accounting server. Two workstations in accounting are connected to switch ports 10 and 11.

<table>
<thead>
<tr>
<th>Network Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Accounting Workstations may only send traffic to the Accounting Server.</td>
</tr>
<tr>
<td>2. No Internet traffic may be sent to the Accounting Server or Workstations.</td>
</tr>
<tr>
<td>3. All other switch ports may only send traffic to Port 1.</td>
</tr>
</tbody>
</table>

![Figure 11-4. Network Configuration for Named Source-Port Filters Example](image-url)
Defining and Configuring Example Named Source-Port Filters. While named source-port filters may be defined and configured in two steps, this is not necessary. Here we define and configure each of the named source-port filters for our example network in a single step.

```
HP Switch(config)# filter source-port named-filter web-only drop 2-26
HP Switch(config)# filter source-port named-filter accounting drop 1-6,8,9,12-26
HP Switch(config)# filter source-port named-filter no-incoming-web drop 7,10,11
```

Once the named source-port filters have been defined and configured we now apply them to the switch ports.

```
HP Switch(config)# show filter source-port
Traffic/Security Filters

| Filter Name    | Port List   | Action    |
|----------------+-------------+-----------|
| web-only       | NOT USED    | drop 2-26 |
| accounting     | NOT USED    | drop 1-6,8-9,12-26 |
| no-incoming-web| NOT USED    | drop 7,10-11 |

HP Switch(config)#
```

The `show filter` command shows what ports have filters applied.
Traffic/Security Filters and Monitors
Filter Types and Operation

HP Switch(config)# show filter

Traffic/Security Filters

<table>
<thead>
<tr>
<th>IDX</th>
<th>Filter Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Source Port</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Source Port</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Source Port</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>Source Port</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>Source Port</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>Source Port</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>Source Port</td>
<td>9</td>
</tr>
<tr>
<td>8</td>
<td>Source Port</td>
<td>12</td>
</tr>
<tr>
<td>20</td>
<td>Source Port</td>
<td>24</td>
</tr>
<tr>
<td>21</td>
<td>Source Port</td>
<td>25</td>
</tr>
<tr>
<td>22</td>
<td>Source Port</td>
<td>26</td>
</tr>
<tr>
<td>23</td>
<td>Source Port</td>
<td>7</td>
</tr>
<tr>
<td>24</td>
<td>Source Port</td>
<td>10</td>
</tr>
<tr>
<td>25</td>
<td>Source Port</td>
<td>11</td>
</tr>
<tr>
<td>26</td>
<td>Source Port</td>
<td>1</td>
</tr>
</tbody>
</table>

Indicates the port number or port-trunk name of the source port or trunk assigned to the filter.

An automatically assigned index number used to identify the filter for a detailed information listing. A filter retains its assigned IDX number for as long as the filter exists in the switch. The switch assigns the lowest available IDX number to a new filter. This can result in a newer filter having a lower IDX number than an older filter if a previous (source-port or named source-port) filter deletion created a gap in the filter listing.

Figure 11-7. Example of the show filter Command

Using the IDX value in the show filter command, we can see how traffic is filtered on a specific port (Value). The two outputs below show a non-accounting and an accounting switch port.
Traffic/Security Filters and Monitors
Filter Types and Operation

Figure 11-8. Example Showing Traffic Filtered on Specific Ports

The same command, using IDX 26, shows how traffic from the Internet is handled.

<table>
<thead>
<tr>
<th>Dest</th>
<th>Port Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10/100TX</td>
<td>Forward</td>
</tr>
<tr>
<td>2</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>3</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>4</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>5</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>6</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>7</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>8</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>9</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>10</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>11</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>12</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dest</th>
<th>Port Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>2</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>3</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>4</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>5</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>6</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>7</td>
<td>10/100TX</td>
<td>Forward</td>
</tr>
<tr>
<td>8</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>9</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>10</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>11</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
<tr>
<td>12</td>
<td>10/100TX</td>
<td>Drop</td>
</tr>
</tbody>
</table>

HP Switch(config)# show filter 4
Traffic/Security Filters
Filter Type : Source Port
Source Port : 5

HP Switch(config)# show filter 24
Traffic/Security Filters
Filter Type : Source Port
Source Port : 10
As the company grows, more resources are required in accounting. Two additional accounting workstations are added and attached to ports 12 and 13. A second server is added attached to port 8.

Network Design
1. Accounting Workstations may only send traffic to the Accounting Server.
2. No Internet traffic may be sent to the Accounting Server or Workstations.
3. All other switch ports may only send traffic to Port 1.

Figure 11-9. Example of Source Port Filtering with Internet Traffic

Figure 11-10. Expanded Network Configuration for Named Source-Port Filters Example
The following revisions to the named source-port filter definitions maintain the desired network traffic management, as shown in the Action column of the show command.

| HP Switch(config)# filter source-port named-filter accounting forward 8,12,13 |
| HP Switch(config)# filter source-port named-filter no-incoming-web drop 8,12,13 |
| HP Switch(config)# show filter source-port |

| Traffic/Security Filters |
|--------------------------|--------------------------|--------------------------|
| Filter Name               | Port List                | Action                   |
| web-only                  | 2-6,8-9,12-26            | drop 2-26                |
| accounting                | 7,10-11                  | drop 1-6,9,14-26         |
| no-incoming-web           | 1                        | drop 7-8,10-13           |

HP Switch(config)#

Figure 11-11. Example Showing Network Traffic Management with Source Port Filters

We next apply the updated named source-port filters to the appropriate switch ports. As a port can only have one source-port filter (named or not named), before applying the new named source-port filters we first remove the existing source-port filters on the port.

| HP Switch(config)# no filter source-port 8,12,13 |
| HP Switch(config)# filter source-port 8,12,13 named-filter accounting |
| HP Switch(config)#

The named source-port filters now manage traffic on the switch ports as shown below, using the show filter source-port command.
Traffic/Security Filters and Monitors
Filter Types and Operation

Static Multicast Filters

This filter type enables the switch to forward or drop multicast traffic to a specific set of destination ports. This helps to preserve bandwidth by reducing multicast traffic on ports where it is unnecessary, and to isolate multicast traffic to enhance security.

You can configure up to 16 static multicast filters (defined by the `filter` command—page 11-20). However, if an IGMP-controlled filter for a joined multicast group has the same multicast address as a static multicast filter configured on a given port, the IGMP-controlled filter overrides the static multicast filter configured on that port. Note that in the default configuration, IGMP is disabled on VLANs configured in the switch. To enable IGMP on a specific VLAN, use the `vlan < vid > ip igmp` command. (For more on this command, refer to the chapter titled “Multimedia Traffic Control with IP Multicast (IGMP)” in the Multicast and Routing Guide for your switch.)

The total of static multicast filters and IGMP multicast filters together can range from 389 to 420, depending on the current `max-vlans` setting in the switch. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Port List</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>web-only</td>
<td>2-6,9,14-26</td>
<td>drop 2-26</td>
</tr>
<tr>
<td>accounting</td>
<td>7-8,10-13</td>
<td>drop 1-6,9,14-26</td>
</tr>
<tr>
<td>no-incoming-web</td>
<td>1</td>
<td>drop 7-8,10-13</td>
</tr>
</tbody>
</table>

Figure 11-12. Named Source-Port Filters Managing Traffic
**Table 11-2. Multicast Filter Limits**

<table>
<thead>
<tr>
<th>Max-VLANs Setting</th>
<th>Maximum # of Multicast Filters (Static and IGMP Combined)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (the minimum)</td>
<td>420</td>
</tr>
<tr>
<td>8 (the default)</td>
<td>413</td>
</tr>
<tr>
<td>32 or higher</td>
<td>389</td>
</tr>
</tbody>
</table>

**Notes**

**Per-Port IP Multicast Filters.** The static multicast filters described in this section filter traffic having a multicast address you specify. To filter all multicast traffic on a per-VLAN basis, refer to the section titled “Configuring and Displaying IGMP” in the chapter titled “Multimedia Traffic Control with IP Multicast (IGMP)” in the *Multicast and Routing Guide* for your switch.

**IP Multicast Filters.** Multicast filters are configured using the Ethernet format for the multicast address. IP multicast addresses occur in the range of 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7fffff). Any static Traffic/Security filters configured with a *multicast* filter type and a multicast address in this range will continue to be in effect unless IGMP learns of a multicast group destination in this range. In this case, IGMP takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the static filter resumes control over traffic to the multicast address.

**Caution**

If Spanning Tree is enabled, then the MSTP multicast MAC address (0180c2-000000) should not be filtered. (STP will not operate properly if the MSTP multicast MAC address is filtered.)

**Protocol Filters**

This filter type enables the switch to forward or drop, on the basis of protocol type, traffic to a specific set of destination ports on the switch. Filtered protocol types include:

- AppleTalk
- ARP
- IPX
- NetBEUI
- SNA
- IPX
Only one filter for a particular protocol type can be configured at any one time. For example, a separate protocol filter can be configured for each of the protocol types listed above, but only one of those can be an IP filter. Also, the destination ports for a protocol filter can be on different VLANs.

You can configure up to seven protocol filters.

---

### Configuring Traffic/Security Filters

Use this procedure to specify the type of filters to use on the switch and whether to forward or drop filtered packets for each filter you specify.

1. Select the static filter type(s).
2. For inbound traffic matching the filter type, determine the filter action you want for each outbound (destination) port on the switch (forward or drop). The default action for a new filter is to forward traffic of the specified type to all outbound ports.
3. Configure the filter.
4. Use `show filter` (page 11-22) to check the filter listing to verify that you have configured correct action for the desired outbound ports.
Configuring a Source-Port Traffic Filter

**Syntax:** [no] filter

[source-port < port-number | trunk-name>]

Specifies one inbound port or trunk. Traffic received inbound on this interface from other devices will be filtered. The no form of the command deletes the source-port filter for <port-number> and returns the destination ports for that filter to the Forward action. (Default: Forward on all ports.)

**Note:** If multiple VLANs are configured, the source-port and the destination port(s) must be in the same VLAN unless routing is enabled. Similarly, if a VLAN containing both the source and destination is multi-netted, the source and destination ports and/or trunks must be in the same subnet unless routing is enabled.

[ drop ] < destination-port-list > [ forward < port-list>]

Configures the filter to drop traffic for the ports and/or trunks in the designated <destination-port-list>. Can be followed by forward <destination-port-list> if you have other destination ports set to drop that you want to change to forward. If no drop or forward action is specified, the switch automatically creates a filter with a forward action from the designated source port (or trunk) to all destination ports (or trunks) on the switch.

[ forward ] < port-list>

Configures the filter to forward traffic for the ports and/or trunks in the designated <destination-port-list>. Because forward is the default state for destinations in a filter, this command is useful when destinations in an existing filter are configured for drop and you want to change them to forward. Can be followed by drop <destination-port-list> if you have other destination ports set to forward that you want to change to drop. If no drop or forward action is specified, the switch automatically creates a filter with a forward action from the designated source port (or trunk) to all destination ports (or trunks) on the switch.
Example of Creating a Source-Port Filter

For example, assume that you want to create a source-port filter that drops all traffic received on port 5 with a destination of port trunk 1 (Trk1) and any port in the range of port 10 to port 15. To create this filter you would execute this command:

```
HP Switch(config)# filter source-port 5 drop trk1,10-15
```

Later, suppose you wanted to shift the destination port range for this filter up by two ports; that is, to have the filter drop all traffic received on port 5 with a destination of any port in the range of port 12 to port 17. (The Trk1 destination is already configured in the filter and can remain as-is.) With one command you can restore forwarding to ports 10 and 11 while adding ports 16 and 17 to the "drop" list:

```
HP Switch(config)# filter source-port 5 forward 10-11 drop 16-17
```

Configuring a Filter on a Port Trunk

This operation uses the same command as is used for configuring a filter on an individual port. However, the configuration process requires two steps:

1. Configure the port trunk.
2. Configure a filter on the port trunk by using the trunk name (trk1, trk2, ...trk6) instead of a port name.

For example, to create a filter on port trunk 1 to drop traffic received inbound for trunk 2 and ports 10-15:

```
HP Switch(config)# filter source-port trk1 drop trk2,10-15
```

Note that if you first configure a filter on a port and then later add the port to a trunk, the port remains configured for filtering but the filtering action will be suspended while the port is a member of the trunk. That is, the trunk does not adopt filtering from the port configuration. You must still explicitly configure the filter on the port trunk. If you use the `show filter < index>` command for a filter created before the related source port was added to a trunk, the port number appears between asterisks (*), indicating that the filter action has been suspended for that filter. For example, if you create a filter on port 5, then create a trunk with ports 5 and 6, and display the results, you would see the following:
Traffic/Security Filters and Monitors  
Configuring Traffic/Security Filters

Figure 11-13. Example of Switch Response to Adding a Filtered Source Port to a Trunk

Editing a Source-Port Filter

The switch includes in one filter the action(s) for all destination ports and/or trunks configured for a given source port or trunk. Thus, if a source-port filter already exists and you want to change the currently configured action for some destination ports or trunks, use the `filter source-port` command to update the existing filter. For example, suppose you configure a filter to drop traffic received on port 8 and destined for ports 1 and 2. The resulting filter is shown on the left in figure 11-14. Later, you update the filter to drop traffic received on port 8 and destined for ports 3 through 5. Since only one filter exists for a given source port, the filter on traffic from port 8 appears as shown on the right in figure 11-14:

```
HP Switch(config)# filter source-port 5 drop 2
HP Switch(config)# trunk 5-6 trk1
HP Switch(config)# show filter
```

<table>
<thead>
<tr>
<th>IDX</th>
<th>Filter Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Source Port</td>
<td><em>5</em></td>
</tr>
</tbody>
</table>

```
HP Switch(config)# show filter 1
```

| Filter Type : Source Port |
| Source Port : *5* |

<table>
<thead>
<tr>
<th>Dest Port Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 100/1000T</td>
<td>Forward</td>
</tr>
<tr>
<td>2 100/1000T</td>
<td>Forward</td>
</tr>
<tr>
<td>3 100/1000T</td>
<td>Forward</td>
</tr>
<tr>
<td>4 100/1000T</td>
<td>Forward</td>
</tr>
</tbody>
</table>

The *5* shows that port 5 is configured for filtering, but the filtering action has been suspended while the port is a member of a trunk. If you want the trunk to which port 5 belongs to filter traffic, then you must explicitly configure filtering on the trunk. 

**Note:** If you configure an existing trunk for filtering and later add another port to the trunk, the switch will apply the filter to all traffic moving on any link in the trunk. If you remove a port from the trunk it returns to the configuration it had before it was added to the trunk.
### Traffic/Security Filters and Monitors

#### Configuring Traffic/Security Filters

<table>
<thead>
<tr>
<th>Dest Port Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100/1000T</td>
</tr>
<tr>
<td>2</td>
<td>100/1000T</td>
</tr>
<tr>
<td>3</td>
<td>100/1000T</td>
</tr>
<tr>
<td>4</td>
<td>100/1000T</td>
</tr>
<tr>
<td>5</td>
<td>100/1000T</td>
</tr>
<tr>
<td>6</td>
<td>100/1000T</td>
</tr>
<tr>
<td>7</td>
<td>100/1000T</td>
</tr>
</tbody>
</table>

#### Syntax:

```
[no] filter

[multicast < mac-address>]

Specifies a multicast address. Inbound traffic received (on any port) with this multicast address will be filtered. (Default: Forward on all ports.)

The no form of the command deletes the multicast filter for the <mac-address> multicast address and returns the destination ports for that filter to the Forward action.

[< forward | drop > < port-list>]

Specifies whether the designated destination port(s) should forward or drop the filtered traffic.

[protocol < ip | ipx | arp | appletalk | sna | netbeui>]

Specifies a protocol type. Traffic received (on any port) with this protocol type will be filtered. (Default: Forward on all ports.)

The no form of the command deletes the protocol filter for the specified protocol and returns the destination ports for that filter to the Forward action.

[< forward | drop > < port-list>]

Specifies whether the designated destination port(s) should forward or drop the filtered traffic.
```
For example, suppose you wanted to configure the filters in table 11-3 on a switch. (For more on source-port filters, refer to “Configuring a Source-Port Traffic Filter” on page 11-17.)

**Table 11-3. Filter Example**

<table>
<thead>
<tr>
<th>Filter Type</th>
<th>Filter Value</th>
<th>Action</th>
<th>Destination Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-Port</td>
<td>Inbound ports: A1, A2*</td>
<td>Drop</td>
<td>D1-D4</td>
</tr>
<tr>
<td>Multicast</td>
<td>010000-123456</td>
<td>Drop</td>
<td>C1-C24, D5-D10</td>
</tr>
<tr>
<td>Multicast</td>
<td>010000-224466</td>
<td>Drop</td>
<td>B1-B4</td>
</tr>
<tr>
<td>Protocol</td>
<td>Appletalk</td>
<td>Drop</td>
<td>C12-C18, D1</td>
</tr>
<tr>
<td>Protocol</td>
<td>ARP</td>
<td>Drop</td>
<td>D17, D21-D24</td>
</tr>
</tbody>
</table>

*Because the switch allows one inbound port in a source-port filter, the requirement to filter ports A1 and A2 means you will configure two separate source-port filters.

The following commands configure the filters listed above:

```plaintext
HP Switch(config)# filter source-port a1 drop e d1-d4
HP Switch(config)# filter source-port a2 drop d1-d4
HP Switch(config)# filter multicast 010000-123456 drop e c1-c24,d5-d10
HP Switch(config)# filter multicast 010000-224466 drop e b1-b4
HP Switch(config)# filter protocol appletalk drop e c12-c18,d1
HP Switch(config)# filter protocol arp drop e d17,d21-d24
```

**Figure 11-15. Configuring Various Traffic/Security Filters**

**Filter Indexing**

The switch automatically assigns each new filter to the lowest-available index (IDX) number. The index numbers are included in the `show filter` command described in the next section and are used with the `show filter < index>` command to display detailed information about a specific filter.

If there are no filters currently configured, and you create three filters in succession, they will have index numbers 1 - 3. However, if you then delete the filter using index number “2” and then configure two new filters, the first new filter will receive the index number “2” and the second new filter will receive the index number "4". This is because the index number “2” was made vacant by the earlier deletion, and was therefore the lowest index number available for the next new filter.
Displaying Traffic/Security Filters

This command displays a listing of all filters by index number and also enables you to use the index number to display the details of individual filters.

Syntax:  
```plaintext
show filter
```

- **Lists the filters configured in the switch, with corresponding filter index (IDX) numbers.**
- **IDX:** An automatically assigned index number used to identify the filter for a detailed information listing. A filter retains its assigned IDX number for as long as the filter exists in the switch. The switch assigns the lowest available IDX number to a new filter. This can result in a newer filter having a lower IDX number than an older filter if a previous filter deletion created a gap in the filter listing.
- **Filter Type:** Indicates the type of filter assigned to the IDX number (source-port, multicast, or protocol).
- **Value:** Indicates the port number or port-trunk name of the source port or trunk assigned to the filter

```plaintext
[ index ]
```

Lists the filter type and other data for the filter corresponding to the index number in the show filter output. Also lists, for each outbound destination port in the switch, the port number, port type, and filter action (forward or drop). The switch assigns the lowest available index number to a new filter. If you delete a filter, the index number for that filter becomes available for the next filter you create.

For example, to display the filters created in figure 11-15 on page 11-21 and then list the details of the multicast filter for multicast address 010000-224466:
Figure 11-16. Example of Displaying Filter Data
Configuring Port-Based and User-Based Access Control (802.1X)

Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>WebAgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Switch Ports as 802.1X Authenticators</td>
<td>Disabled</td>
<td>n/a</td>
<td>page 12-17</td>
<td>n/a</td>
</tr>
<tr>
<td>Configuring 802.1X Open VLAN Mode</td>
<td>Disabled</td>
<td>n/a</td>
<td>page 12-32</td>
<td>n/a</td>
</tr>
<tr>
<td>Configuring Switch Ports to Operate as 802.1X Supplicants</td>
<td>Disabled</td>
<td>n/a</td>
<td>page 12-50</td>
<td>n/a</td>
</tr>
<tr>
<td>Displaying 802.1X Configuration, Statistics, and Counters</td>
<td>n/a</td>
<td>n/a</td>
<td>page 12-55</td>
<td>n/a</td>
</tr>
<tr>
<td>How 802.1X Affects VLAN Operation</td>
<td>n/a</td>
<td>n/a</td>
<td>page 12-69</td>
<td>n/a</td>
</tr>
<tr>
<td>RADIUS Authentication and Accounting</td>
<td>Refer to chapter 5, “RADIUS Authentication, Authorization, and Accounting”</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Why Use Port-Based or User-Based Access Control?

Local Area Networks are often deployed in a way that allows unauthorized clients to attach to network devices, or allows unauthorized users to get access to unattended clients on a network. Also, the use of DHCP services and zero configuration make access to networking services easily available. This exposes the network to unauthorized use and malicious attacks. While access to the network should be made easy, uncontrolled and unauthorized access is usually not desirable. 802.1X simplifies security management by providing access control along with the ability to control user profiles from up to three RADIUS servers while allowing a given user to use the same entering valid user credentials for access from multiple points within the network.

General Features

802.1X on the switches covered in this guide includes the following:

- Switch operation as both an authenticator (for supplicants having a point-to-point connection to the switch) and as a supplicant for point-to-point connections to other 802.1X-aware switches.
- Authentication of 802.1X access using a RADIUS server and either the EAP or CHAP protocol.
Configuring Port-Based and User-Based Access Control (802.1X)

Overview

- Provision for enabling clients that do not have 802.1 supplicant software to use the switch as a path for downloading the software and initiating the authentication process (802.1X Open VLAN mode).
- User-Based access control option with support for up to 32 authenticated clients per-port.
- Port-Based access control option allowing authentication by a single client to open the port. This option does not force a client limit and, on a port opened by an authenticated client, allows unlimited client access without requiring further authentication.
- Supplicant implementation using CHAP authentication and independent user credentials on each port.

■ The local operator password configured with the password command for management access to the switch is no longer accepted as an 802.1X authenticator credential. The password port-access command configures the local operator username and password used as 802.1X authentication credentials for access to the switch. The values configured can be stored in a configuration file using the include-credentials command. For information about the password port-access command, see “Do These Steps Before You Configure 802.1X Operation” on page 12-13.

■ On-demand change of a port’s configured VLAN membership status to support the current client session.

■ Session accounting with a RADIUS server, including the accounting update interval.

■ Use of Show commands to display session counters.

■ Support for concurrent use of 802.1X and either Web authentication or MAC authentication on the same port.

■ For unauthenticated clients that do not have the necessary 802.1X supplicant software (or for other reasons related to unauthenticated clients), there is the option to configure an Unauthorized-Client VLAN. This mode allows you to assign unauthenticated clients to an isolated VLAN through which you can provide the necessary supplicant software and/or other services you want to extend to these clients.

User Authentication Methods

The switch offers two methods for using 802.1X access control. Generally, the “Port Based” method supports one 802.1X-authenticated client on a port, which opens the port to an unlimited number of clients. The “User-Based” method supports up to 32 802.1X-authenticated clients on a port. In both cases, there are operating details to be aware of that can influence your choice of methods.
802.1X User-Based Access Control

802.1X operation with access control on a per-user basis provides client-level security that allows LAN access to individual 802.1X clients (up to 32 per port), where each client gains access to the LAN by entering valid user credentials. This operation improves security by opening a given port only to individually authenticated clients, while simultaneously blocking access to the same port for clients that cannot be authenticated. All sessions must use the same untagged VLAN (unless MAC-based VLANs are enabled. Please see “MAC-Based VLANs” on page 5-46). Also, an authenticated client can use any tagged VLAN memberships statically configured on the port, provided the client is configured to use the tagged VLAN memberships available on the port. (Note that the session total includes any sessions begun by the Web Authentication or MAC Authentication features covered in chapter 3.) For more information, refer to “Option For Authenticator Ports: Configure Port-Security To Allow Only 802.1X-Authenticated Devices” on page 12-48.

802.1X Port-Based Access Control

802.1X port-based access control provides port-level security that allows LAN access only on ports where a single 802.1X-capable client (supplicant) has entered authorized RADIUS user credentials. For reasons outlined below, this option is recommended for applications where only one client at a time can connect to the port. Using this option, the port processes all IP traffic as if it comes from the same client. Thus, in a topology where multiple clients can connect to the same port at the same time:

- If the first client authenticates and opens the port, and then another client authenticates, the port responds as if the original client has initiated a reauthentication. With multiple clients authenticating on the port, the RADIUS configuration response to the latest client authentication replaces any other configuration from an earlier client authentication. If all clients use the same configuration this should not be a problem. But if the RADIUS server responds with different configurations for different clients, then the last client authenticated will effectively lock out any previously authenticated client. When any client to authenticate closes its session, the port will also close and remain so until another client successfully authenticates.

- The most recent client authentication determines the untagged VLAN membership for the port. Also, any client able to use the port can access any tagged VLAN memberships statically configured on the port, provided the client is configured to use the available, tagged VLAN memberships.
Configuring Port-Based and User-Based Access Control (802.1X)

Overview

- If the first client authenticates and opens the port, and then one or more other clients connect without trying to authenticate, then the port configuration as determined by the original RADIUS response remains unchanged and all such clients will have the same access as the authenticated client. When the authenticated client closes the session, the port will also be closed to any other, unauthenticated clients that may have also been using the port.

This operation unblocks the port while an authenticated client session is in progress. In topologies where simultaneous, multiple client access is possible this can allow unauthorized and unauthenticated access by another client while an authenticated client is using the port. If you want to allow only authenticated clients on the port, then user-based access control (page 12-3) should be used instead of port-based access control. Using the user-based method enables you to specify up to 32 authenticated clients.

Note

Port-Based 802.1X can operate concurrently with Web-Authentication or MAC-Authentication on the same port. However, this is not a commonly used application and is not generally recommended. For more information, refer to the operating note on page 12-12.

Alternative To Using a RADIUS Server

Note that you can also configure 802.1X for authentication through the switch's local username and password instead of a RADIUS server, but doing so increases the administrative burden, decentralizes user credential administration, and reduces security by limiting authentication to one Operator password set for all users.

Accounting

The switches covered in this guide also provide RADIUS Network accounting for 802.1X access. Refer to chapter 5, "RADIUS-Administered CoS and Rate-Limiting".
Terminology

802.1X-Aware: Refers to a device that is running either 802.1X authenticator software or 802.1X client software and is capable of interacting with other devices on the basis of the IEEE 802.1X standard.

Authorized-Client VLAN: Like the Unauthorized-Client VLAN, this is a conventional, static VLAN previously configured on the switch by the System Administrator. The intent in using this VLAN is to provide authenticated clients with network services that are not available on either the port’s statically configured VLAN memberships or any VLAN memberships that may be assigned during the RADIUS authentication process. While an 802.1X port is a member of this VLAN, the port is untagged. When a port loses its authenticated client connection, it drops its membership in this VLAN. Note that with multiple clients on a port, all such clients use the same untagged, port-based VLAN membership (unless MAC-based VLANs are enabled. Please see “MAC-Based VLANs” on page 5-46).

Authentication Server: The entity providing an authentication service to the switch when the switch is configured to operate as an authenticator. In the case of a switch running 802.1X, this is a RADIUS server (unless local authentication is used, in which case the switch performs this function using its own username and password for authenticating a supplicant).

Authenticator: In HP applications, a switch that requires a supplicant to provide the proper credentials before being allowed access to the network.


Client: In this application, an end-node device such as a management station, workstation, or mobile PC linked to the switch through a point-to-point LAN link.

User-Based Authentication: The 802.1X extension in the switches covered in this guide. In this operation, multiple clients on the same port must individually authenticate themselves.

Guest VLAN: See “Unauthorized-Client VLAN”.

EAP (Extensible Authentication Protocol): EAP enables network access that supports multiple authentication methods.
Configuring Port-Based and User-Based Access Control (802.1X)

Terminology

**EAPOL:** Extensible Authentication Protocol Over LAN, as defined in the 802.1X standard.

**Friendly Client:** A client that does not pose a security risk if given access to the switch and your network.

**MD5:** An algorithm for calculating a unique digital signature over a stream of bytes. It is used by CHAP to perform authentication without revealing the shared secret (password).

**PVID (Port VID):** This is the VLAN ID for the untagged VLAN to which an 802.1X port belongs.

**Port-Based Authentication:** In this operation, the first client on a port to authenticate itself unblocks the port for the duration of the client’s 802.1X-authenticated session. The switches covered in this guide use port-based authentication.

**Static VLAN:** A VLAN that has been configured as “permanent” on the switch by using the CLI `vlan < vid >` command or the Menu interface.

**Supplicant:** The entity that must provide the proper credentials to the switch before receiving access to the network. This is usually an end-user workstation, but it can be a switch, router, or another device seeking network services.

**Tagged Membership in a VLAN:** This type of VLAN membership allows a port to be a member of multiple VLANs simultaneously. If a client connected to the port has an operating system that supports 802.1Q VLAN tagging, then the client can access VLANs for which the port is a tagged member. If the client does not support VLAN tagging, then it can access only a VLAN for which the port is an untagged member. (A port can be an untagged member of only one port-based VLAN at a time. Where a port is a tagged member of a VLAN, 802.1X Open VLAN mode does not affect the port’s access to the VLAN unless the port is statically configured as a member of a VLAN that is also configured as the Unauthorized-Client or Authorized-Client VLAN. See also “Untagged Membership in a VLAN”.

**Unauthorized-Client VLAN:** A conventional, static VLAN statically configured on the switch. It is used to provide access to a client prior to authentication, and is sometimes termed a guest VLAN. It should be set up to allow an unauthenticated client to access only the initialization services necessary to establish an authenticated connection, plus any other desirable services whose use by an unauthenticated client poses no security threat to your network. (Note that an unauthenticated client has access to all network resources that have membership in the VLAN you
designate as the Unauthorized-Client VLAN.) A port configured to use a
given Unauthorized-Client VLAN does not have to be statically configured
as a member of that VLAN as long as at least one other port on the switch
is statically configured as a tagged or untagged member of the same
Unauthorized-Client VLAN. An unauthorized-client VLAN is available on
a port only if there is no authenticated client already using the port.

**Untagged Membership in a VLAN**: A port can be an untagged member of
only one VLAN (unless MAC-based VLANs are enabled. Please see “MAC-
Based VLANs” on page 5-46). (In the factory-default configuration, all
ports on the switch are untagged members of the default VLAN.) An
untagged VLAN membership is *required* for a client that does not support
802.1q VLAN tagging. A port can simultaneously have one untagged VLAN
membership and multiple tagged VLAN memberships. Depending on how
you configure 802.1X Open VLAN mode for a port, a statically configured,
untagged VLAN membership may become unavailable while there is a
client session on the port. See also “**Tagged Membership in a VLAN**”. 
General 802.1X Authenticator Operation

This operation provides security on a point-to-point link between a client and the switch, where both devices are 802.1X-aware. (If you expect desirable clients that do not have the necessary 802.1X supplicant software, you can provide a path for downloading such software by using the 802.1X Open VLAN mode—refer to “802.1X Open VLAN Mode” on page 12-32.)

Example of the Authentication Process

Suppose that you have configured a port on the switch for 802.1X authentication operation, which blocks access to the LAN through that port. If you then connect an 802.1X-aware client (supplicant) to the port and attempt to log on:

1. The switch responds with an identity request.
2. The client responds with a user name that uniquely defines this request for the client.
3. The switch responds in one of the following ways:
   - If 802.1X on the switch is configured for RADIUS authentication, the switch then forwards the request to a RADIUS server.
     i. The server responds with an access challenge which the switch forwards to the client.
     ii. The client then provides identifying credentials (such as a user certificate), which the switch forwards to the RADIUS server.
     iii. The RADIUS server then checks the credentials provided by the client.
     iv. If the client is successfully authenticated and authorized to connect to the network, then the server notifies the switch to allow access to the client. Otherwise, access is denied and the port remains blocked.
   - If 802.1X on the switch is configured for local authentication, then:
     i. The switch compares the client’s credentials to the username and password configured in the switch (Operator level).
     ii. If the client is successfully authenticated and authorized to connect to the network, then the switch allows access to the client. Otherwise, access is denied and the port remains blocked for that client.
Configuring Port-Based and User-Based Access Control (802.1X)
General 802.1X Authenticator Operation

Note
The switches covered in this guide can use either 802.1X port-based authentication or 802.1X user-based authentication. For more information, refer to “User Authentication Methods” on page 12-2.

VLAN Membership Priority

Following client authentication, an 802.1X port resumes membership in any tagged VLANs for which it is already assigned in the switch configuration. The port also becomes an untagged member of one VLAN according to the following order of options:

a. **1st Priority:** The port joins a VLAN to which it has been assigned by a RADIUS server during client authentication.

b. **2nd Priority:** If RADIUS authentication does not include assigning the port to a VLAN, then the switch assigns the port to the VLAN entered in the port’s 802.1X configuration as an Authorized-Client VLAN, if configured.

c. **3rd Priority:** If the port does not have an Authorized-Client VLAN configured, but does have a static, untagged VLAN membership in its configuration, then the switch assigns the port to this VLAN.

A port assigned to a VLAN by an Authorized-Client VLAN configuration (or a RADIUS server) will be an untagged member of the VLAN for the duration of the authenticated session. This applies even if the port is also configured in the switch as a tagged member of the same VLAN.

Note
On the switches covered in this guide, using the same port for both RADIUS-assigned clients and clients using a configured, Authorized-Client VLAN is not recommended. This is because doing so can result in authenticated clients with mutually exclusive VLAN priorities, which means that some authenticated clients can be denied access to the port. Refer to figure 12-1 on page 12-10.
Configuring Port-Based and User-Based Access Control (802.1X)
General 802.1X Authenticator Operation

Figure 12-1. Priority of VLAN Assignment for an Authenticated Client
General Operating Rules and Notes

- In the user-based mode, when there is an authenticated client on a port, the following traffic movement is allowed:
  - Multicast and broadcast traffic is allowed on the port.
  - Unicast traffic to authenticated clients on the port is allowed.
  - All traffic from authenticated clients on the port is allowed.

- When a port on the switch is configured as either an authenticator or supplicant and is connected to another device, rebooting the switch causes a re-authentication of the link.

- Using user-based 802.1X authentication, when a port on the switch is configured as an authenticator the port allows only authenticated clients up to the currently configured client limit.

  For clients that do not have the proper 802.1X supplicant software, the optional 802.1X Open VLAN mode can be used to open a path for downloading 802.1X supplicant software to a client or to provide other services for unauthenticated clients. Refer to “802.1X Open VLAN Mode” on page 12-32.

- Using port-based 802.1X authentication, when a port on the switch is configured as an authenticator, one authenticated client opens the port. Other clients that are not running an 802.1X supplicant application can have access to the switch and network through the opened port. If another client uses an 802.1X supplicant application to access the opened port, then a re-authentication occurs using the RADIUS configuration response for the latest client to authenticate. To control access by all clients, use the user-based method.

- Where a switch port is configured with user-based authentication to accept multiple 802.1X (and/or Web- or MAC-Authentication) client sessions, all authenticated clients must use the same port-based, untagged VLAN membership assigned for the earliest, currently active client session. Thus, on a port where one or more authenticated client sessions are already running, all such clients will be on the same untagged VLAN (unless MAC-based VLANs are enabled. Please see “MAC-Based VLANs” on page 5-46). If a RADIUS server subsequently authenticates a new client, but attempts to re-assign the port to a different, untagged VLAN than the one already in use for the previously existing, authenticated client sessions, the connection for the new client will fail. For more on this topic, refer to “802.1X Open VLAN Mode” on page 12-32. (Note that if the port is
Configuring Port-Based and User-Based Access Control (802.1X)
General Operating Rules and Notes

- If a port on switch “A” is configured as an 802.1X supplicant and is connected to a port on another switch, “B”, that is not 802.1X-aware, access to switch “B” will occur without 802.1X security protection.

- On a port configured for 802.1X with RADIUS authentication, if the RADIUS server specifies a VLAN for the supplicant and the port is a trunk member, the port will be blocked. If the port is later removed from the trunk, the port will allow authentication of the supplicant. Similarly, if the supplicant is authenticated and later the port becomes a trunk member, the port will be blocked. If the port is then removed from the trunk, it will allow the supplicant to re-authenticate.

- If a client already has access to a switch port when you configure the port for 802.1X authenticator operation, the port will block the client from further network access until it can be authenticated.

- Meshing is not supported on ports configured for 802.1X port-access security.

- A port can be configured as an authenticator or an 802.1X supplicant, or both. Some configuration instances block traffic flow or allow traffic to flow without authentication. Refer to “Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches” on page 12-50.

- To help maintain security, 802.1X and LACP cannot both be enabled on the same port. If you try to configure 802.1X on a port already configured for LACP (or the reverse) you will see a message similar to the following:

```
Error configuring port X: LACP and 802.1X cannot be run together.
```

Applying Web Authentication or MAC Authentication Concurrently with Port-Based 802.1X Authentication: While 802.1X port-based access control can operate concurrently with Web Authentication or MAC Authentication, port-based access control is subordinate to Web-Auth and MAC-Auth operation. If 802.1X operates in port-based mode and MAC or Web authentication is enabled on the same port, any 802.1X authentication has no effect on the ability of a client to access the controlled port. That is, the client's access will be denied until the client authenticates through Web-Auth or MAC-Auth on the port. Note also that a client authenticating with port-based 802.1X does not open the port in the same way that it would if Web-Auth or MAC-Auth were not enabled. That is, any non-authenticating client attempting to access the port after another client authenticates with port-based 802.1X would still have to authenticate through Web-Auth or MAC-Auth.
General Setup Procedure for 802.1X Access Control

Do These Steps Before You Configure 802.1X Operation

1. Configure a local username and password on the switch for both the Operator (login) and Manager (enable) access levels. (While this may or may not be required for your 802.1X configuration, HP recommends that you use a local username and password pair at least until your other security measures are in place.)

2. Enable include-credentials. The port-access option is available only if include-credentials is enabled. See “Saving Security Credentials in a Config File” on page 2-10 in this guide.

For switches covered in this guide, the local operator password configured with the password command is not accepted as an 802.1X authenticator credential. The port-access command is used to configure the operator username and password that are used as 802.1X credentials for network access to the switch. 802.1X network access is not allowed unless a password has been configured using the `password port-access` command.

**Syntax:**

```plaintext
password port-access [user-name <name>] <password>
```

Configures the operator username and password used to access the network through 802.1X authentication.

- **user-name <name>**
  
  Operator username (text string) used only for local authentication of 802.1X clients. This value is different from the local operator username configured with the `password` command for management access.

- **<password>**
  
  Operator password (text string) used only for local authentication of 802.1X clients. This value is different from the local operator password configured with the `password` command for management access.
Figure 12-2 shows how to configure a local operator password for 802.1X access.

```
HP Switch(config)# password port-access user-name Jim secret3
```

**Figure 12-2. Example of the Password Port-Access Command**

You can save the port-access password for 802.1X authentication in the configuration file by using the `include-credentials` command. For more information, see “Saving Security Credentials in a Config File” on page 2-10. in this guide.

3. Determine the switch ports that you want to configure as authenticators and/or supplicants, and disable LACP on these ports. (For more information on disabling LACP, refer to the “Note” on page 12-18.).

   To display the current configuration of 802.1X, Web-based, and MAC authentication on all switch ports, enter the `show port-access config` command.

```
HP Switch(config)# show port-access config
```

**Figure 12-3. Example of show port-access config Command Output**
4. Determine whether to use user-based access control (page 12-3) or port-based access control (page 12-3).

5. Determine whether to use the optional 802.1X Open VLAN mode for clients that are not 802.1X-aware; that is, for clients that are not running 802.1X supplicant software. (This will require you to provide downloadable software that the client can use to enable an authentication session.) For more on this topic, refer to “802.1X Open VLAN Mode” on page 12-32.

6. For any port you want to operate as a supplicant, determine the user credentials. You can either use the same credentials for each port or use unique credentials for individual ports or subgroups of ports. (This can also be the same local username/password pair that you assign to the switch.)

7. Unless you are using only the switch’s local username and password for 802.1X authentication, configure at least one RADIUS server to authenticate access requests coming through the ports on the switch from external supplicants (including switch ports operating as 802.1X supplicants). You can use up to three RADIUS servers for authentication; one primary and two backups. Refer to the documentation provided with your RADIUS application.
Overview: Configuring 802.1X Authentication on the Switch

This section outlines the steps for configuring 802.1X on the switch. For detailed information on each step, refer to the following:

- “802.1X User-Based Access Control” on page 12-3
- “802.1X Port-Based Access Control” on page 12-3
- “Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches” on page 12-50.

1. Enable 802.1X user-based or port-based authentication on the individual ports you want to serve as authenticators. On the ports you will use as authenticators, either accept the default 802.1X settings or change them, as necessary. Note that, by default, the port-control parameter is set to auto for all ports on the switch. This requires a client to support 802.1X authentication and to provide valid credentials to get network access. Refer to page 12-18.

2. If you want to provide a path for clients without 802.1X supplicant software to download the software so that they can initiate an authentication session, enable the 802.1X Open VLAN mode on the ports you want to support this feature. Refer to page 12-32.

3. Configure the 802.1X authentication type. Options include:
   - Local Operator username and password (using the password port-access command).
   - EAP RADIUS: This option requires your RADIUS server application to support EAP authentication for 802.1X.
   - CHAP (MD5) RADIUS: This option requires your RADIUS server application to support CHAP (MD5) authentication.
   Refer to page 12-24.

4. If you select either eap-radius or chap-radius for step 3, use the radius host command to configure up to three RADIUS server IP address(es) on the switch. See page 12-26.

5. Enable 802.1X authentication on the switch. Refer to “1. Enable 802.1X Authentication on Selected Ports” on page 12-18.

6. Test both the authorized and unauthorized access to your system to ensure that the 802.1X authentication works properly on the ports you have configured for port-access.
If you want to implement the optional port security feature (step 7) on the switch, you should first ensure that the ports you have configured as 802.1X authenticators operate as expected.

7. If you are using Port Security on the switch, configure the switch to allow only 802.1X access on ports configured for 802.1X operation, and (if desired) the action to take if an unauthorized device attempts access through an 802.1X port. Refer to page 12-48.

8. If you want a port on the switch to operate as a supplicant on a port operating as an 802.1X authenticator on another device, then configure the supplicant operation. (Refer to “Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches” on page 12-50.)

Configuring Switch Ports as 802.1X Authenticators

<table>
<thead>
<tr>
<th>802.1X Authentication Commands</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] aaa port-access authenticator &lt; port-list &gt;</td>
<td>12-18</td>
</tr>
<tr>
<td>[auth-vid</td>
<td>clear-statistics</td>
</tr>
<tr>
<td>aaa authentication port-access</td>
<td>12-24</td>
</tr>
<tr>
<td>&lt; local</td>
<td>eap-radius</td>
</tr>
<tr>
<td>[no] aaa port-access authenticator active</td>
<td>12-17</td>
</tr>
<tr>
<td>aaa port-access &lt;port-list&gt; controlled-directions &lt;both</td>
<td>in&gt; [mixed]</td>
</tr>
<tr>
<td>[no] port-security [ethernet] &lt; port-list &gt; learn-mode port-access</td>
<td>12-48</td>
</tr>
</tbody>
</table>

802.1X Open VLAN Mode Commands
802.1X Supplicant Commands
802.1X-Related Show Commands
RADIUS server configuration
1. Enable 802.1X Authentication on Selected Ports

This task configures the individual ports you want to operate as 802.1X authenticators for point-to-point links to 802.1X-aware clients or switches, and consists of two steps:

A. Enable the selected ports as authenticators.
B. Specify either user-based or port-based 802.1X authentication.

(Actual 802.1X operation does not commence until you perform step 5 on page 12-27 to activate 802.1X authentication on the switch.)

**Note**

If you enable 802.1X authentication on a port, the switch automatically disables LACP on that port. However, if the port is already operating in an LACP trunk, you must remove the port from the trunk before you can configure it for 802.1X authentication.

A. Enable the Selected Ports as Authenticators and Enable the (Default) Port-Based Authentication

**Syntax:**  

```
[ no ] aaa port-access authenticator < port-list >
```

Enables specified ports to operate as 802.1X authenticators and enables port-based authentication. (To enable user-based authentication, execute this command first, and then execute the client-limit < port-list > version of this command described in the next section.) The `no` form of the command removes 802.1X authentication from < port-list >. To activate configured 802.1X operation, you must enable 802.1X authentication. Refer to “5. Enable 802.1X Authentication on the switch” on page 12-27.
B. Specify User-Based Authentication or Return to Port-Based Authentication

**User-Based 802.1X Authentication.**

**Syntax:**

```
  aaa port-access authenticator < port-list > client-limit < 1 - 32 >
```

Used after executing `aaa port-access authenticator < port-list >` (above) to convert authentication from port-based to user-based. Specifies user-based 802.1X authentication and the maximum number of 802.1X-authenticated client sessions allowed on each of the ports in `<port-list>`. If a port currently has no authenticated client sessions, the next authenticated client session the port accepts determines the untagged VLAN membership to which the port is assigned during the session. If another client session begins later on the same port while an earlier session is active, the later session will be on the same untagged VLAN membership as the earlier session.

**Note:** The client limit is 256 clients per-port for MAC-auth and Web-auth; the client limit for 802.1X is 32 clients per port. The MAC-auth and Web-auth limit of 256 clients only applies when there are fewer than 16,384 authentication clients on the entire switch. After the limit of 16,384 clients is reached, no additional authentication clients are allowed on any port for any method.
Port-Based 802.1X Authentication.

no aaa port-access authenticator <port-list> client-limit

*Used to convert a port from user-based authentication to port-based authentication, which is the default setting for ports on which authentication is enabled. (Executing `aaa port-access authenticator <port-list>` enables 802.1X authentication on `<port-list>` and enables port-based authentication—page 12-18.)* If a port currently has no authenticated client sessions, the next authenticated client session the port accepts determines the untagged VLAN membership to which the port is assigned during the session. If another authenticated client session begins later on the same port while an earlier session is active, the later session replaces the currently active session and will be on the untagged VLAN membership specified by the RADIUS server for the later session.

Example: Configuring User-Based 802.1X Authentication

This example enables ports A10-A12 to operate as authenticators, and then configures the ports for user-based authentication.

```
HP Switch(config)# aaa port-access authenticator a10-A12
HP Switch(config)# aaa port-access authenticator a10-A12 client-limit 4
```

*Figure 12-4. Example of Configuring User-Based 802.1X Authentication*

Example: Configuring Port-Based 802.1X Authentication

This example enables ports A13-A15 to operate as authenticators, and then configures the ports for port-based authentication.

```
HP Switch(config)# aaa port-access authenticator a13-a15
HP Switch(config)# no aaa port-access authenticator a13-a15 client-limit
```

*Figure 12-5. Example of Configuring Port-Based 802.1X Authentication*
2. Reconfigure Settings for Port-Access

The commands in this section are initially set by default and can be reconfigured as needed.

**Syntax:**  
`aaa port-access authenticator < port-list >`  
`[control < authorized | auto | unauthorized >]`

*Controls authentication mode on the specified port:*

- **authorized:** Also termed "Force Authorized". Gives access to a device connected to the port. In this case, the device does not have to provide 802.1X credentials or support 802.1X authentication. (You can still configure console, Telnet, or SSH security on the port.)

- **auto (the default):** The device connected to the port must support 802.1X authentication and provide valid credentials to get network access. (Optional: You can use the Open VLAN mode to provide a path for clients without 802.1X supplicant software to down-load this software and begin the authentication process. Refer to “802.1X Open VLAN Mode” on page 12-32.)

- **unauthorized:** Also termed "Force Unauthorized". Do not grant access to the network, regardless of whether the device provides the correct credentials and has 802.1X support. In this state, the port blocks access to any connected device.

— Continued on Next Page —
[quiet-period < 0 - 65535 >]

Sets the period during which the port does not try to acquire a supplicant. The period begins after the last attempt authorized by the max-requests parameter fails (next page). (Default: 60 seconds)

[tx-period < 0 - 65535 >]

Sets the period the port waits to retransmit the next EAPOL PDU during an authentication session. (Default: 30 seconds)

[supplicant-timeout < 1 - 300 >]

Sets the period of time the switch waits for a supplicant response to an EAP request. If the supplicant does not respond within the configured time frame, the session times out. (Default: 30 seconds)

[server-timeout < 1 - 300 >]

Sets the period of time the switch waits for a server response to an authentication request. If there is no response within the configured time frame, the switch assumes that the authentication attempt has timed out. Depending on the current max-requests setting, the switch will either send a new request to the server or end the authentication session. (Default: 30 seconds)

[max-requests < 1 - 10 >]

Sets the number of authentication attempts that must time-out before authentication fails and the authentication session ends. If you are using the Local authentication option, or are using RADIUS authentication with only one host server, the switch will not start another session until a client tries a new access attempt. If you are using RADIUS authentication with two or three host servers, the switch will open a session with each server, in turn, until authentication occurs or there are no more servers to try. During the quiet-period (previous page), if any, you cannot reconfigure this parameter. (Default: 2)

— Continued on Next Page —
Configuring Port-Based and User-Based Access Control (802.1X)

Configuring Switch Ports as 802.1X Authenticators

[reauth-period < 0 - 9999999 >]
Sets the period of time after which clients connected
must be re-authenticated. When the timeout is set to 0
the reauthentication is disabled (Default: 0 second)

[unauth-vid < vlan-id >]
Configures an existing static VLAN to be the Unauthorized-Client VLAN. This enables you to provide a path
for clients without supplicant software to download the
software and begin an authentication session. Refer to
“802.1X Open VLAN Mode” on page 12-32.

aaa port-access authenticator < port-list >

[logoff-period]< 1 - 999999999 >
Configures the period of time the switch waits for
client activity before removing an inactive client from
the port. (Default: 300 seconds)

[unauth-period < 0-255 >]
Specifies a delay in seconds for placing a port on the
Unauthorized-Client VLAN. This delay allows more
time for a client with 802.1X supplicant capability to
initiate an authentication session. If a connected cli-
ent does not initiate a session before the timer expires,
the port is assigned to the Unauthenticated-Client
VLAN. (Default: 0 seconds)

[auth-vid < vid >]
Configures an existing, static VLAN to be the Autho-
rized-Client VLAN. Refer to “802.1X Open VLAN Mode”
on page 12-32.
3. Configure the 802.1X Authentication Method

This task specifies how the switch authenticates the credentials provided by a supplicant connected to a switch port configured as an 802.1X authenticator.

You can configure `local`, `chap-radius` or `eap-radius` as the primary password authentication method for the port-access method. You also need to select `none` or `authorized` as a secondary, or backup, method.

**Syntax:**  
```
aaa authentication port-access <chap-radius | eap-radius | local>
```

Configures `local`, `chap-radius` (MD5), or `eap-radius` as the primary password authentication method for port-access. The default primary authentication is `local`. (Refer to the documentation for your RADIUS server application.)

For switches covered in this guide, you must use the `password port-access` command to configure the operator username and password for 802.1X access. See “General Setup Procedure for 802.1X Access Control” on page 12-13 for more information.

[<none | authorized>]

Provides options for secondary authentication. The `none` option specifies that a backup authentication method is not used. The `authorized` option allows access without authentication. (default: `none`).
Configuring Port-Based and User-Based Access Control (802.1X)
Configuring Switch Ports as 802.1X Authenticators

For example, to enable the switch to perform 802.1X authentication using one or more EAP-capable RADIUS servers:

```
HP Switch(config)# aaa authentication port-access eap-radius
HP Switch(config)# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled

<table>
<thead>
<tr>
<th>Access Task</th>
<th>Primary</th>
<th>Server Group</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Port-Access</td>
<td>EapRadius</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Webui</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Web-Auth</td>
<td>ChapRadius</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>MAC-Auto</td>
<td>ChapRadius</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Task</th>
<th>Primary</th>
<th>Server Group</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Webui</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Local</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

802.1X (Port-Access) configured for EAP-RADIUS authentication.

Figure 12-6. Example of 802.1X (Port-Access) Authentication
4. Enter the RADIUS Host IP Address(es)

If you select either `eap-radius` or `chap-radius` for the authentication method, configure the switch to use 1, 2, or 3 RADIUS servers for authentication. The following syntax shows the basic commands. For coverage of all commands related to RADIUS server configuration, refer to chapter 5, “RADIUS Authentication, Authorization, and Accounting”.

**Syntax:** `radius host <ip-address>`

*Adds a server to the RADIUS configuration.*

[key <server-specific key-string>]

Optional. Specifies an encryption key for use during authentication (or accounting) sessions with the specified server. This key must match the key used on the RADIUS server. Use this option only if the specified server requires a different key than configured for the global encryption key. The tilde (~) character is allowed in the string. It is not backward compatible; the “~” character is lost if you use a software version that does not support the “~” character.

**Syntax:** `radius-server key <global key-string>`

Specifies the global encryption key the switch uses for sessions with servers for which the switch does not have a server-specific key. This key is optional if all RADIUS server addresses configured in the switch include a server-specific encryption key. The tilde (~) character is allowed in the string, for example, `radius-server key hp-switch`. It is not backward compatible; the “~” character is lost if you use a software version that does not support the “~” character.

Default: Null

The no form of the command removes the global encryption key.
5. Enable 802.1X Authentication on the Switch

After configuring 802.1X authentication as described in the preceding four sections, activate it with this command:

**Syntax:**  
```
aaa port-access authenticator active
```

*Activates 802.1X port-access on ports you have configured as authenticators.*

6. Optional: Reset Authenticator Operation

While 802.1X authentication is operating, you can use the following `aaa port-access authenticator` commands to reset 802.1X authentication and statistics on specified ports.

**Syntax:**  
```
aaa port-access authenticator <port-list>  
[initialize]  
```

*On the specified ports, blocks inbound and outbound traffic and restarts the 802.1X authentication process. This happens only on ports configured with `control auto` and actively operating as 802.1X authenticators.*

```
[reauthenticate]  
```

*On the specified ports, forces reauthentication (unless the authenticator is in “HELD” state).*

```
[clear-statistics]  
```

*On the specified ports, clears authenticator statistics counters.*

7. Optional: Configure 802.1X Controlled Directions

After you enable 802.1X authentication on specified ports, you can use the `aaa port-access controlled-directions` command to configure how a port transmits traffic before it successfully authenticates a client and enters the authenticated state.

As documented in the IEEE 802.1X standard, an 802.1X-aware port that is unauthenticated can control traffic in either of the following ways:

- In both ingress and egress directions by disabling both the reception of incoming frames and transmission of outgoing frames
- Only in the ingress direction by disabling only the reception of incoming frames.
Prerequisite. As documented in the IEEE 802.1X standard, the disabling of incoming traffic and transmission of outgoing traffic on an 802.1X-aware egress port in an unauthenticated state (using the `aaa port-access controlled-directions` command) is supported only if:

- The port is configured as an edge port in the network using the `spanning-tree edge-port` command.
- The 802.1s Multiple Spanning Tree Protocol (MSTP) or 802.1w Rapid Spanning Tree Protocol (RSTP) is enabled on the switch. MSTP and RSTP improve resource utilization while maintaining a loop-free network.

For information on how to configure the prerequisites for using the `aaa port-access controlled-directions` command, see Chapter 4, “Multiple Instance Spanning-Tree Operation” in the Advanced Traffic Management Guide.

**Syntax:**
```
aaa port-access <port-list> controlled-directions <both | in>
```
*both* (default): Incoming and outgoing traffic is blocked on an 802.1X-aware port before authentication occurs.

*in:* Incoming traffic is blocked on an 802.1X-aware port before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on unauthenticated 802.1X-aware ports.

Wake-on-LAN Traffic

The Wake-on-LAN feature is used by network administrators to remotely power on a sleeping workstation (for example, during early morning hours to perform routine maintenance operations, such as patch management and software updates).

The `aaa port-access controlled-direction in` command allows Wake-on-LAN traffic to be transmitted on an 802.1X-aware egress port that has not yet transitioned to the 802.1X authenticated state; the `controlled-direction both` setting prevents Wake-on-LAN traffic to be transmitted on an 802.1X-aware egress port until authentication occurs.

**Note**

Although the `controlled-direction in` setting allows Wake-on-LAN traffic to traverse the switch through unauthenticated 802.1X-aware egress ports, it does not guarantee that the Wake-on-LAN packets will arrive at their destination. For example, firewall rules on other network devices and VLAN rules may prevent these packets from traversing the network.
Operating Notes

- Using the `aaa port-access controlled-directions in` command, you can enable the transmission of Wake-on-LAN traffic on unauthenticated egress ports that are configured for any of the following port-based security features:
  - 802.1X authentication
  - MAC authentication
  - Web authentication

Because a port can be configured for more than one type of authentication to protect the switch from unauthorized access, the last setting you configure with the `aaa port-access controlled-directions` command is applied to all authentication methods configured on the switch.

For information about how to configure and use MAC and Web authentication, refer to chapter 3, “Web and MAC Authentication”.

- To display the currently configured 802.1X Controlled Directions value, enter the `show port-access authenticator config` command as shown in Figure 12-12.

- When an 802.1X-authenticated port is configured with the `controlled-directions in` setting, eavesdrop prevention is not supported on the port.

Example: Configuring 802.1X Controlled Directions

The following example shows how to enable the transmission of Wake-on-LAN traffic in the egress direction on an 802.1X-aware port before it transitions to the 802.1X authenticated state and successfully authenticates a client device.

```
HP Switch(config)# aaa port-access authenticator a10
HP Switch(config)# aaa authentication port-access eap-radius
HP Switch(config)# aaa port-access authenticator active
HP Switch(config)# aaa port-access a10 controlled-directions in
```

Figure 12-7. Example of Configuring 802.1X Controlled Directions

Unauthenticated VLAN Access (Guest VLAN Access)

When a PC is connected through an IP phone to a switch port that has been authorized using 802.1X or Web/MAC authentication, the IP phone is authenticated using client-based 802.1X or Web/MAC authentication and has access to secure, tagged VLANs on the port. If the PC is unauthenticated, it needs to
have access to the insecure guest VLAN (unauthenticated VLAN) that has been configured for 802.1X or Web/MAC authentication. 802.1X and Web/MAC authentication normally do not allow authenticated clients (the phone) and unauthenticated clients (the PC) on the same port (unless MAC-based VLANs are enabled. Please see “MAC-Based VLANs” on page 5-46).

Mixed port access mode allows 802.1X and Web/MAC authenticated and unauthenticated clients on the same port when the guest VLAN is the same as the port’s current untagged authenticated VLAN for authenticated clients, or when none of the authenticated clients are authorized on the untagged authenticated VLAN. Instead of having just one client per port, multiple clients can use the guest VLAN.

Authenticated clients always have precedence over guests (unauthenticated clients) if access to a client’s untagged VLAN requires removal of a guest VLAN from the port. If an authenticated client becomes authorized on its untagged VLAN as the result of initial authentication or because of an untagged packet from the client, then all 802.1X or Web/MAC authenticated guests are removed from the port and the port becomes an untagged member of the client’s untagged VLAN.

Characteristics of Mixed Port Access Mode

- The port keeps tagged VLAN assignments continuously.
- The port sends broadcast traffic from the VLANs even when there are only guests authorized on the port.
- Guests cannot be authorized on any tagged VLANs.
- Guests can use the same bandwidth, rate limits and QoS settings that may be assigned for authenticated clients on the port (via RADIUS attributes).
- When no authenticated clients are authorized on the untagged authenticated VLAN, the port becomes an untagged member of the guest VLAN for as long as no untagged packets are received from any authenticated clients on the port.
- New guest authorizations are not allowed on the port if at least one authenticated client is authorized on its untagged VLAN and the guest VLAN is not the same as the authenticated client’s untagged VLAN.

**Note**

If you disable mixed port access mode, this does not automatically remove guests that have already been authorized on a port where an authenticated client exists. New guests are not allowed after the change, but the existing
authorized guests will still be authorized on the port until they are removed by a new authentication, an untagged authorization, a port state change, and so on.

Configuring Mixed Port Access Mode

**Syntax:**  
[no] aaa port-access <port-list> mixed

*Enables or disables guests on ports with authenticated clients.*

*Default: Disabled; guests do not have access*

```bash
HP Switch(config)# aaa port-access 6 mixed
```

*Figure 12-8. Example of Configuring Mixed Port Access Mode*
802.1X Open VLAN Mode

Introduction

This section describes how to use the 802.1X Open VLAN mode to provide a path for clients that need to acquire 802.1X supplicant software before proceeding with the authentication process. The Open VLAN mode involves options for configuring unauthorized-client and authorized-client VLANs on ports configured as 802.1X authenticators.

Configuring the 802.1X Open VLAN mode on a port changes how the port responds when it detects a new client. In earlier releases, a “friendly” client computer not running 802.1X supplicant software could not be authenticated on a port protected by 802.1X access security. As a result, the port would become blocked and the client could not access the network. This prevented the client from:

- Acquiring IP addressing from a DHCP server
- Downloading the 802.1X supplicant software necessary for an authentication session

The 802.1X Open VLAN mode solves this problem by temporarily suspending the port’s static VLAN memberships and placing the port in a designated Unauthorized-Client VLAN (sometimes termed a guest VLAN). In this state the client can proceed with initialization services, such as acquiring IP addressing and 802.1X client software, and starting the authentication process.
On ports configured to allow multiple sessions using 802.1X user-based access control, all clients must use the same untagged VLAN (unless MAC-based VLANs are enabled. Please see “MAC-Based VLANs” on page 5-46). On a given port where there are no currently active, authenticated clients, the first authenticated client determines the untagged VLAN in which the port will operate for all subsequent, overlapping client sessions.

If the switch operates in an environment where some valid clients will not be running 802.1X supplicant software and need to download it from your network. Then, because such clients would need to use the Unauthorized-Client VLAN and authenticated clients would be using a different VLAN (for security reasons), allowing multiple clients on an 802.1X port can result in blocking some or all clients needing to use the Unauthorized-Client VLAN.

On ports configured for port-based 802.1X access control, if multiple clients try to authenticate on the same port, the most recently authenticated client determines the untagged VLAN membership for that port. Clients that connect without trying to authenticate will have access to the untagged VLAN membership that is currently assigned to the port.

VLAN Membership Priorities

Following client authentication, an 802.1X port resumes membership in any tagged VLANs for which it is already assigned in the switch configuration. The port also becomes an untagged member of one VLAN according to the following order of options:

a. **1st Priority:** The port joins a VLAN to which it has been assigned by a RADIUS server during client authentication.

b. **2nd Priority:** If RADIUS authentication does not include assigning the port to a VLAN, then the switch assigns the port to the VLAN entered in the port’s 802.1X configuration as an Authorized-Client VLAN, if configured.

c. **3rd Priority:** If the port does not have an Authorized-Client VLAN configured, but does have a static, untagged VLAN membership in its configuration, then the switch assigns the port to this VLAN.

A port assigned to a VLAN by an Authorized-Client VLAN configuration (or a RADIUS server) will be an untagged member of the VLAN for the duration of the authenticated session. This applies even if the port is also configured in the switch as a tagged member of the same VLAN.
Configuring Port-Based and User-Based Access Control (802.1X)

802.1X Open VLAN Mode

**Note**
After client authentication, the port resumes membership in any tagged VLANs for which it is configured. If the port is a tagged member of a VLAN used for 1 or 2 listed above, then it also operates as an untagged member of that VLAN while the client is connected. When the client disconnects, the port reverts to tagged membership in the VLAN.

Use Models for 802.1X Open VLAN Modes

You can apply the 802.1X Open VLAN mode in more than one way. Depending on your use, you will need to create one or two static VLANs on the switch for exclusive use by per-port 802.1X Open VLAN mode authentication:

- **Unauthorized-Client VLAN**: Configure this VLAN when unauthenticated, friendly clients will need access to some services before being authenticated or instead of being authenticated.

- **Authorized-Client VLAN**: Configure this VLAN for authenticated clients when the port is not statically configured as an untagged member of a VLAN you want clients to use, or when the port is statically configured as an untagged member of a VLAN you do not want clients to use. (A port can be configured as untagged on only one port-based VLAN. When an Authorized-Client VLAN is configured, it will always be untagged and will block the port from using a statically configured, untagged membership in another VLAN.) Note that after client authentication, the port returns to membership in any tagged VLANs for which it is configured. See the "Note", above.
### Table 12-1. 802.1X Open VLAN Mode Options

<table>
<thead>
<tr>
<th>802.1X Per-Port Configuration</th>
<th>Port Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Open VLAN mode:</td>
<td>The port automatically blocks a client that cannot initiate an authentication session.</td>
</tr>
<tr>
<td>Open VLAN mode with both of the following configured:</td>
<td></td>
</tr>
<tr>
<td>Unauthorized-Client VLAN</td>
<td>• When the port detects a client without 802.1X supplicant capability, it automatically becomes an untagged member of this VLAN. If you previously configured the port as a static, tagged member of the VLAN, membership temporarily changes to untagged while the client remains unauthenticated.</td>
</tr>
<tr>
<td></td>
<td>• If the port already has a statically configured, untagged membership in another VLAN, then the port temporarily closes access to this other VLAN while in the Unauthorized-Client VLAN.</td>
</tr>
<tr>
<td></td>
<td>• To limit security risks, the network services and access available on the Unauthorized-Client VLAN should include only what a client needs to enable an authentication session. If the port is statically configured as a tagged member of any other VLANs, access to these VLANs is blocked while the port is a member of the Unauthorized-Client VLAN.</td>
</tr>
<tr>
<td>Note for a Port Configured To Allow Multiple Client Sessions:</td>
<td>If any previously authenticated clients are using a port assigned to a VLAN other than the Unauthorized-Client VLAN, then a later client that is not running 802.1X supplicant software is blocked on the port until all other, authenticated clients on the port have disconnected.</td>
</tr>
</tbody>
</table>
Authorized-Client VLAN

- After client authentication, the port drops membership in the Unauthorized-Client VLAN and becomes an untagged member of this VLAN.

**Notes:** If the client is running an 802.1X supplicant application when the authentication session begins, and is able to authenticate itself before the switch assigns the port to the Unauthorized-Client VLAN, then the port does not become a member of the Unauthorized-Client VLAN. On the switches covered in this guide, you can use the `unauth-period` command—page 12-23—to delay moving the port into the Unauthorized-Client VLAN.

If RADIUS authentication assigns a VLAN and there are no other authenticated clients on the port, then the port becomes a member of the RADIUS-assigned VLAN —instead of the Authorized-Client VLAN—while the client is connected.

- If the port is statically configured as a tagged member of a VLAN, and this VLAN is used as the Authorized-Client VLAN, then the port temporarily becomes an untagged member of this VLAN when the client becomes authenticated.

- If the port is statically configured as a tagged member of a VLAN, the port returns to tagged membership in this VLAN upon successful authentication. This happens even if the RADIUS server assigns the port to another, authorized VLAN. If the port is already configured as a tagged member of a VLAN that RADIUS assigns as an authorized VLAN, then the port becomes an untagged member of that VLAN for the duration of the client connection.
### 802.1X Per-Port Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Open VLAN Mode with Only an Unauthorized-Client VLAN Configured:</strong></td>
<td></td>
</tr>
<tr>
<td>- When the port detects a client, it automatically becomes an untagged member of this VLAN. To limit security risks, the network services and access available on this VLAN should include only what a client needs to enable an authentication session. If the port is statically configured as an untagged member of another VLAN, the switch temporarily removes the port from membership in this other VLAN while membership in the Unauthorized-Client VLAN exists.</td>
<td></td>
</tr>
<tr>
<td>- After the client is authenticated, and if the port is statically configured as an untagged member of another VLAN, the port’s access to this other VLAN is restored.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If RADIUS authentication assigns the port to a VLAN, this assignment overrides any statically configured, untagged VLAN membership on the port (while the client is connected).</td>
<td></td>
</tr>
<tr>
<td>- If the port is statically configured as a tagged member of a VLAN, the port returns to tagged membership in this VLAN upon successful client authentication. This happens even if the RADIUS server assigns the port to another, authorized VLAN. Note that if the port is already configured as a tagged member of a VLAN that RADIUS assigns as an authorized VLAN, then the port becomes an untagged member of that VLAN for the duration of the client connection.</td>
<td></td>
</tr>
<tr>
<td><strong>Note for a Port Configured To Allow Multiple Client Sessions:</strong> If any previously authenticated clients are using a port assigned to a VLAN other than the Unauthorized-Client VLAN (such as a RADIUS-assigned VLAN), then a later client that is not running 802.1X supplicant software is blocked on the port until all other, authenticated clients on the port have disconnected. Refer to figure 12-1 on page 12-10.</td>
<td></td>
</tr>
</tbody>
</table>
802.1X Open VLAN Mode

<table>
<thead>
<tr>
<th>802.1X Per-Port Configuration</th>
<th>Port Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open VLAN Mode with Only an Authorized-Client VLAN Configured:</td>
<td></td>
</tr>
<tr>
<td>• Port automatically blocks a client that cannot initiate an authentication session.</td>
<td></td>
</tr>
<tr>
<td>• If the client successfully completes an authentication session, the port becomes an untagged member of this VLAN.</td>
<td></td>
</tr>
<tr>
<td>• If the port is statically configured as a tagged member of any other VLAN, the port returns to tagged membership in this VLAN upon successful client authentication. This happens even if the RADIUS server assigns the port to another, authorized VLAN. If the port is already configured as a tagged member of a VLAN that RADIUS assigns as an authorized VLAN, then the port becomes an untagged member of that VLAN for the duration of the client connection.</td>
<td></td>
</tr>
</tbody>
</table>

Note: An authorized-client VLAN configuration can be overridden by a RADIUS authentication that assigns a VLAN. (Refer to figure 12-1 on page 12-10.)
Operating Rules for Authorized-Client and Unauthorized-Client VLANs

<table>
<thead>
<tr>
<th>Condition</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static VLANs used as Authorized-Client or Unauthorized-Client VLANs</td>
<td>These must be configured on the switch before you configure an 802.1X authenticator port to use them. (Use the <code>vlan &lt;vlan-id&gt;</code> command or the VLAN Menu screen in the Menu interface.)</td>
</tr>
<tr>
<td>VLAN Assignment Received from a RADIUS Server</td>
<td>If the RADIUS server specifies a VLAN for an authenticated supplicant connected to an 802.1X authenticator port, this VLAN assignment overrides any Authorized-Client VLAN assignment configured on the authenticator port. This is because membership in both VLANs is untagged, and the switch allows only one untagged, port-based VLAN membership per-port. For example, suppose you configured port A4 to place authenticated supplicants in VLAN 20. If a RADIUS server authenticates supplicant “A” and assigns this supplicant to VLAN 50, then the port can access VLAN 50 as an untagged member while the client session is running. When the client disconnects from the port, then the port drops these assignments and uses the untagged VLAN memberships for which it is statically configured. (After client authentication, the port resumes any tagged VLAN memberships for which it is already configured. For details, refer to the Note on page 12-34.)</td>
</tr>
</tbody>
</table>
| Temporary VLAN Membership During a Client Session                           | • Port membership in a VLAN assigned to operate as the Unauthorized-Client VLAN is temporary, and ends when the client receives authentication or the client disconnects from the port, whichever is first. In the case of the multiple clients allowed on switches covered in this guide, the first client to authenticate determines the untagged VLAN membership for the port until all clients have disconnected. Any other clients that cannot operate in that VLAN are blocked at that point.  
• Port membership in a VLAN assigned to operate as the Authorized-Client VLAN ends when the client disconnects from the port. If a VLAN assignment from a RADIUS server is used instead, the same rule applies. In the case of the multiple clients allowed on switches, the port maintains the same VLAN as long as there is any authenticated client using the VLAN. When the last client disconnects, then the port reverts to only the VLAN(s) for which it is statically configured as a member. |
### Configuring Port-Based and User-Based Access Control (802.1X)

#### 802.1X Open VLAN Mode

<table>
<thead>
<tr>
<th>Condition</th>
<th>Rule</th>
</tr>
</thead>
</table>
| **Effect of Unauthorized-Client VLAN session on untagged port VLAN membership** | - When an unauthenticated client connects to a port that is already configured with a static, untagged VLAN, the switch temporarily moves the port to the Unauthorized-Client VLAN (also untagged). (While the Unauthorized-Client VLAN is in use, the port does not access any other VLANs.)  
  - If the client disconnects, the port leaves the Unauthorized-Client VLAN and re-acquires membership in all the statically configured VLANs to which it belongs.  
  - If the client becomes authenticated, the port leaves the Unauthenticated-Client VLAN and joins the appropriate VLAN. (Refer to “VLAN Membership Priorities” on page 12-33.)  
  - In the case of the multiple clients allowed on switches, if an authenticated client is already using the port for a different VLAN, then any other unauthenticated clients needing to use the Unauthorized-Client VLAN are blocked. |

| Effect of Authorized-Client VLAN session on untagged port VLAN membership. | - When a client becomes authenticated on a port that is already configured with a static, untagged VLAN, the switch temporarily moves the port to the Authorized-Client VLAN (also untagged). While the Authorized-Client VLAN is in use, the port does not have access to the statically configured, untagged VLAN.  
  - When the authenticated client disconnects, the switch removes the port from the Authorized-Client VLAN and moves it back to the untagged membership in the statically configured VLAN. (After client authentication, the port resumes any tagged VLAN memberships for which it is already configured. For details, refer to the Note on page 12-34.) |

**Note:** This rule assumes:  
- No alternate VLAN has been assigned by a RADIUS server.  
- No other authenticated clients are already using the port.

| Multiple Authenticator Ports Using the Same Unauthorized-Client and Authorized-Client VLANs | You can use the same static VLAN as the Unauthorized-Client VLAN for all 802.1X authenticator ports configured on the switch. Similarly, you can use the same static VLAN as the Authorized-Client VLAN for all 802.1X authenticator ports configured on the switch.  
**Caution:** Do not use the same static VLAN for both the unauthorized-client VLAN and the authorized-client VLAN. Using one VLAN for both creates a security risk by defeating the isolation of unauthenticated clients. |

| Effect of Failed Client Authentication Attempt | When there is an Unauthorized-Client VLAN configured on an 802.1X authenticator port, an unauthorized client connected to the port has access only to the network resources belonging to the Unauthorized-Client VLAN. This access continues until the client disconnects from the port. (If there is no Unauthorized-Client VLAN configured on the authenticator port, the port simply blocks access for any unauthorized client.) |

---

12-40
### Configuring Port-Based and User-Based Access Control (802.1X)

#### 802.1X Open VLAN Mode

<table>
<thead>
<tr>
<th>Condition</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effect of RADIUS-assigned VLAN</td>
<td>This rule assumes no other authenticated clients are already using the port on a different VLAN. The port joins the RADIUS-assigned VLAN as an untagged member.</td>
</tr>
<tr>
<td>IP Addressing for a Client Connected to a Port Configured for 802.x Open VLAN Mode</td>
<td>A client can either acquire an IP address from a DHCP server or use a manually configured IP address before connecting to the switch.</td>
</tr>
<tr>
<td>802.1X Supplicant Software for a Client Connected to a Port Configured for 802.1X Open VLAN Mode</td>
<td>A friendly client, without 802.1X supplicant software, connecting to an authenticator port must be able to download this software from the Unauthorized-Client VLAN before authentication can begin.</td>
</tr>
</tbody>
</table>
| Switch with a Port Configured To Allow Multiple Authorized-Client Sessions | When a new client is authenticated on a given port:  
  - If no other clients are authenticated on that port, then the port joins one VLAN in the following order of precedence:  
    a. A RADIUS-assigned VLAN, if configured.  
    b. An Authenticated-Client VLAN, if configured.  
    c. A static, port-based VLAN to which the port belongs as an untagged member.  
    d. Any VLAN(s) to which the port is configured as a tagged member (provided that the client can operate in that VLAN).  
  - If another client is already authenticated on the port, then the port is already assigned to a VLAN for the previously-existing client session, and the new client must operate in this same VLAN, regardless of other factors. (This means that a client without 802.1X client authentication software cannot access a configured, Unauthenticated-Client VLAN if another, authenticated client is already using the port.) |
Configuring Port-Based and User-Based Access Control (802.1X)

802.1X Open VLAN Mode

<table>
<thead>
<tr>
<th>Condition</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> Limitation on Using an Unauthorized-Client VLAN on an 802.1X Port Configured to Allow Multiple-Client Access</td>
<td>You can optionally enable switches to allow up to 32 clients per-port. The Unauthorized-Client VLAN feature can operate on an 802.1X-configured port regardless of how many clients the port is configured to support. However, all clients on the same port must operate through the same untagged VLAN membership (unless MAC-based VLANs are enabled. Please see “MAC-Based VLANs” on page 6-52). This means that any client accessing a given port must be able to authenticate and operate on the same VLAN as any other previously authenticated clients that are currently using the port. Thus, an Unauthorized-Client VLAN configured on a switch port that allows multiple 802.1X clients cannot be used if there is already an authenticated client using the port on another VLAN. Also, a client using the Unauthorized-Client VLAN will be blocked when another client becomes authenticated on the port. For this reason, the best utilization of the Unauthorized-Client VLAN feature is in instances where only one client is allowed per-port. Otherwise, unauthenticated clients are subject to being blocked at any time by authenticated clients using a different VLAN. (Using the same VLAN for authenticated and unauthenticated clients can create a security risk and is not recommended.)</td>
</tr>
</tbody>
</table>

**Note**

If you use the same VLAN as the Unauthorized-Client VLAN for all authenticator ports, unauthenticated clients on different ports can communicate with each other.

Setting Up and Configuring 802.1X Open VLAN Mode

**Preparation.** This section assumes use of both the Unauthorized-Client and Authorized-Client VLANs. Refer to Table 12-1 on page 12-35 for other options.

Before you configure the 802.1X Open VLAN mode on a port:

- Statically configure an “Unauthorized-Client VLAN” in the switch. The only ports that should belong to this VLAN are ports offering services and access you want available to unauthenticated clients. (802.1X authenticator ports do not have to be members of this VLAN.)

**Caution**

Do not allow any port memberships or network services on this VLAN that would pose a security risk if exposed to an unauthorized client.
Configuring Port-Based and User-Based Access Control (802.1X)
802.1X Open VLAN Mode

- Statically configure an Authorized-Client VLAN in the switch. The only ports that should belong to this VLAN are ports offering services and access you want available to authenticated clients. 802.1X authenticator ports do not have to be members of this VLAN.

Note that if an 802.1X authenticator port is an untagged member of another VLAN, the port’s access to that other VLAN will be temporarily removed while an authenticated client is connected to the port. For example, if:
  i. Port A5 is an untagged member of VLAN 1 (the default VLAN).
  ii. You configure port A5 as an 802.1X authenticator port.
  iii. You configure port A5 to use an Authorized-Client VLAN.

Then, if a client connects to port A5 and is authenticated, port A5 becomes an untagged member of the Authorized-Client VLAN and is temporarily suspended from membership in the default VLAN.

- If you expect friendly clients to connect without having 802.1X supplicant software running, provide a server on the Unauthorized-Client VLAN for downloading 802.1X supplicant software to the client, and a procedure by which the client initiates the download.

- A client must either have a valid IP address configured before connecting to the switch, or download one through the Unauthorized-Client VLAN from a DHCP server. In the latter case, you will need to provide DHCP services on the Unauthorized-Client VLAN.

- Ensure that the switch is connected to a RADIUS server configured to support authentication requests from clients using ports configured as 802.1X authenticators. (The RADIUS server should not be on the Unauthorized-Client VLAN.)

Note that as an alternative, you can configure the switch to use local password authentication instead of RADIUS authentication. However, this is less desirable because it means that all clients use the same passwords and have the same access privileges. Also, you must use 802.1X supplicant software that supports the use of local switch passwords.

**Caution**

Ensure that you do not introduce a security risk by allowing Unauthorized-Client VLAN access to network services or resources that could be compromised by an unauthorized client.

**Configuring General 802.1X Operation:** These steps enable 802.1X authentication, and must be done before configuring 802.1X VLAN operation.
1. Enable 802.1X authentication on the individual ports you want to serve as authenticators. (The switch automatically disables LACP on the ports on which you enable 802.1X.) On the ports you will use as authenticators with VLAN operation, ensure that the port-control parameter is set to **auto** (the default). (Refer to “1. Enable 802.1X Authentication on Selected Ports” on page 12-18.) This setting requires a client to support 802.1X authentication (with 802.1X supplicant operation) and to provide valid credentials to get network access.

**Syntax:**  
```
aaa port-access authenticator < port-list > control auto
```
Activates 802.1X port-access on ports you have configured as authenticators.

2. Configure the 802.1X authentication type. Options include:

**Syntax:**  
```
aaa authentication port-access < local | eap-radius | chap-radius >
```
Determines the type of RADIUS authentication to use.

- **local:** Use the switch’s local username and password for supplicant authentication (the default).
- **eap-radius:** Use EAP-RADIUS authentication. (Refer to the documentation for your RADIUS server.)
- **chap-radius:** Use CHAP-RADIUS (MD5) authentication. (Refer to the documentation for your RADIUS server software.)
3. If you selected either `eap-radius` or `chap-radius` for step 2, use the `radius host` command to configure up to three RADIUS server IP address(es) on the switch.

**Syntax:** `radius host < ip-address >`

- Adds a server to the RADIUS configuration.
- `[key < server-specific key-string>]`
  - Optional. Specifies an encryption key for use with the specified server. This key must match the key used on the RADIUS server. Use this option only if the specified server requires a different key than configured for the global encryption key. The tilde (~) character is allowed in the string. It is not backward compatible; the “~” character is lost if you use a software version that does not support the “~” character.

**Syntax:** `radius-server key < global key-string >`

- Specifies the global encryption key the switch uses for sessions with servers for which the switch does not have a server-specific key. This key is optional if all RADIUS server addresses configured in the switch include a server-specific encryption key. The tilde (~) character is allowed in the string, for example, `radius-server key hp~switch`. It is not backward compatible; the “~” character is lost if you use a software version that does not support the “~” character.

  Default: Null

  The `no` form of the command removes the global encryption key.

4. Activate authentication on the switch.

**Syntax:** `aaa port-access authenticator active`

- Activates 802.1X port-access on ports you have configured as authenticators.

5. Test both the authorized and unauthorized access to your system to ensure that the 802.1X authentication works properly on the ports you have configured for port-access.
Configuring Port-Based and User-Based Access Control (802.1X)

802.1X Open VLAN Mode

**Note**

If you want to implement the optional port-security feature on the switch, you should first ensure that the ports you have configured as 802.1X authenticators operate as expected. Then refer to “Option For Authenticator Ports: Configure Port-Security To Allow Only 802.1X-Authenticated Devices” on page 12-48.

After you complete steps 1 and 2, the configured ports are enabled for 802.1X authentication (without VLAN operation), and you are ready to configure VLAN Operation.

**Configuring 802.1X Open VLAN Mode.** Use these commands to actually configure Open VLAN mode. For a listing of the steps needed to prepare the switch for using Open VLAN mode, refer to “Preparation” on page 12-42.

**Syntax:**

```
aaa port-access authenticator < port-list >
[auth-vid < vlan-id >]
  Configures an existing, static VLAN to be the Authorized-Client VLAN.
[< unauth-vid < vlan-id >]
  Configures an existing, static VLAN to be the Unauthorized-Client VLAN.
```

For example, suppose you want to configure 802.1X port-access with Open VLAN mode on ports A10 - A20 and:

- These two static VLANs already exist on the switch:
  - Unauthorized, VID = 80
  - Authorized, VID = 81
- Your RADIUS server has an IP address of 10.28.127.101. The server uses `rad4all` as a server-specific key string. The server is connected to a port on the Default VLAN.
- The switch's default VLAN is already configured with an IP address of 10.28.127.100 and a network mask of 255.255.255.0

```
HP Switch(config)# aaa authentication port-access eap-radius
  Configures the switch for 802.1X authentication using an EAP-RADIUS server.
HP Switch(config)# aaa port-access authenticator a10-a20
  Configures ports A10 - A20 as 802.1 authenticator ports.
HP Switch(config)# radius host 10.28.127.101 key rad4all
  Configures the switch to look for a RADIUS server with an IP address of 10.28.127.101 and an encryption key of rad4all.
```
Configuring Port-Based and User-Based Access Control (802.1X)

802.1X Open VLAN Mode

Inspecting 802.1X Open VLAN Mode Operation. For information and an example on viewing current Open VLAN mode operation, refer to “Viewing 802.1X Open VLAN Mode Status” on page 12-64.

802.1X Open VLAN Operating Notes

- Although you can configure Open VLAN mode to use the same VLAN for both the Unauthorized-Client VLAN and the Authorized-Client VLAN, this is not recommended. Using the same VLAN for both purposes allows unauthenticated clients access to a VLAN intended only for authenticated clients, which poses a security breach.

- While an Unauthorized-Client VLAN is in use on a port, the switch temporarily removes the port from any other statically configured VLAN for which that port is configured as a member. Note that the Menu interface will still display the port’s statically configured VLAN(s).

- A VLAN used as the Unauthorized-Client VLAN should not allow access to resources that must be protected from unauthenticated clients.

- If a port is configured as a tagged member of VLAN “X”, then the port returns to tagged membership in VLAN “X” upon successful client authentication. This happens even if the RADIUS server assigns the port to another, authorized VLAN “Y”. Note that if RADIUS assigns VLAN “X” as an authorized VLAN, then the port becomes an untagged member of VLAN “X” for the duration of the client connection. (If there is no Authorized-Client or RADIUS-assigned VLAN, then an authenticated client without tagged VLAN capability can access only a statically configured, untagged VLAN on that port.)

- When a client’s authentication attempt on an Unauthorized-Client VLAN fails, the port remains a member of the Unauthorized-Client VLAN until the client disconnects from the port.

HP Switch(config)# aaa port-access authenticator e a10-a20 unauth-vid 80
                   
Configures ports A10 - A20 to use VLAN 80 as the Unauthorized-Client VLAN.

HP Switch(config)# aaa port-access authenticator e a10-a20 auth-vid 81
                   
Configures ports A10 - A20 to use VLAN 81 as the Authorized-Client VLAN.

HP Switch(config)# aaa port-access authenticator active
                   
Activates 802.1X port-access on ports you have configured as authenticators.
During an authentication session on a port in 802.1X Open VLAN mode, if RADIUS specifies membership in an untagged VLAN, this assignment overrides port membership in the Authorized-Client VLAN. If there is no Authorized-Client VLAN configured, then the RADIUS assignment overrides any untagged VLAN for which the port is statically configured.

- If the only authenticated client on a port loses authentication during a session in 802.1X Open VLAN mode, the port VLAN membership reverts back to the Unauthorized-Client VLAN. If there is no Unauthorized-Client VLAN configured, then the client loses access to the port until it can reauthenticate itself. If there are multiple clients authenticated on the port, if one client loses access and attempts to re-authenticate, that client will be handled as a new client on the port.

- The first client to authenticate on a port configured to support multiple clients will determine the port’s VLAN membership for any subsequent clients that authenticate while an active session is already in effect.

**Option For Authenticator Ports:**

Configure Port-Security To Allow Only 802.1X-Authenticated Devices

If 802.1X authentication is disabled on a port or set to authorized (Force Authorize), the port can allow access to a non-authenticated client. Port-Security operates with 802.1X authentication only if the selected ports are configured as 802.1X with the control mode in the port-access authenticator command set to auto (the default setting). For example, if port A10 was at a non-default 802.1X setting and you wanted to configure it to support the port-security option, you would use the following `aaa port-access` command:
Configuring Port-Based and User-Based Access Control (802.1X)

Option For Authenticator Ports: Configure Port-Security To Allow Only 802.1X-Authenticated Devices

Figure 12-9. Port-Acc ess Support for Port-Security Operation

**Note**

If 802.1X port-access is configured on a given port, then port-security **learn-mode** for that port must be set to either **continuous** (the default) or **port-access**.

In addition to the above, to use port-security on an authenticator port (chapter 13), use the per-port **client-limit** option to control how many MAC addresses of 802.1X-authenticated devices the port is allowed to learn. (Using **client-limit** sets 802.1X to user-based operation on the specified ports.) When this limit is reached, no further devices can be authenticated until a currently authenticated device disconnects and the current delay period or logoff period has expired.

**Configure the port access type.**

**Syntax:**

```
aaa port-access authenticator < port-list > client-limit < 1 - 32 >
```

Configures user-based 802.1X authentication on the specified ports and sets the number of authenticated devices the port is allowed to learn. For more on this command, refer to “Configuring Switch Ports as 802.1X Authenticators” on page 12-17.)

--- Or ---

```
no aaa port-access authenticator < port-list > client-limit
```

Configures port-based 802.1X authentication on the specified ports, which opens the port. (Refer to “User Authentication Methods” on page 12-2.)
Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches

802.1X Authentication Commands

802.1X Supplicant Commands

[no] aaa port-access < supplicant < [ethernet] < port-list> page 12-52

[auth-timeout | held-period | start-period | max-start | initialize | identity | secret | clear-statistics] page 12-52

802.1X-Related Show Commands page 12-55

RADIUS server configuration pages 12-26

A switch port can operate as a supplicant in a connection to a port on another 802.1X-aware switch to provide security on links between 802.1X-aware switches. (A port can operate as both an authenticator and a supplicant.)

Example

Suppose that you want to connect two switches, where:

- Switch “A” has port A1 configured for 802.1X supplicant operation.
- You want to connect port A1 on switch “A” to port B5 on switch “B”.

Figure 12-10. Example of Supplicant Operation

1. When port A1 on switch “A” is first connected to a port on switch “B”, or if the ports are already connected and either switch reboots, port A1 begins sending start packets to port B5 on switch “B”.

12-50
Configuring Port-Based and User-Based Access Control (802.1X)
Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches

- If, after the supplicant port sends the configured number of start packets, it does not receive a response, it assumes that switch “B” is not 802.1X-aware, and transitions to the authenticated state. If switch “B” is operating properly and is not 802.1X-aware, then the link should begin functioning normally, but without 802.1X security.
- If, after sending one or more start request packets, port A1 receives a request packet from port B5, then switch “B” is operating as an 802.1X authenticator. The supplicant port then sends a response/ID packet. If switch “B” is configured for RADIUS authentication, it forwards this request to a RADIUS server. If switch “B” is configured for Local 802.1X authentication, the authenticator compares the switch “A” response to its local username and password.

2. The RADIUS server then responds with an MD5 access challenge that switch “B” forwards to port A1 on switch “A”.
3. Port A1 replies with an MD5 hash response based on its username and password or other unique credentials. Switch “B” forwards this response to the RADIUS server.
4. The RADIUS server then analyzes the response and sends either a “success” or “failure” packet back through switch “B” to port A1.
   - A “success” response unblocks port B5 to normal traffic from port A1.
   - A “failure” response continues the block on port B5 and causes port A1 to wait for the “held-time” period before trying again to achieve authentication through port B5.
Supplicant Port Configuration

Enabling a Switch Port as a Supplicant. You can configure a switch port as a supplicant for a point-to-point link to an 802.1X-aware port on another switch. Configure the port as a supplicant before configuring any supplicant-related parameters.

**Syntax:** [no] aaa port-access supplicant [ethernet] <port-list>

Configures a port as a supplicant with either the default supplicant settings or any previously configured supplicant settings, whichever is most recent. The "no" form of the command disables supplicant operation on the specified ports.

Configuring a Supplicant Switch Port. You must enable supplicant operation on a port before changing the supplicant configuration. This means you must execute the supplicant command once without any other parameters, then execute it again with a supplicant parameter you want to configure. If the intended authenticator port uses RADIUS authentication, then use the identity and secret options to configure the RADIUS-expected credentials on the supplicant port. If the intended authenticator port uses Local 802.1X authentication, then use the identity and secret options to configure the authenticator switch’s local username and password on the supplicant port.

**Syntax:** aaa port-access supplicant [ethernet] <port-list>

To enable supplicant operation on the designated ports, execute this command without any other parameters. After doing this, you can use the command again with the following parameters to configure supplicant operation. (Use one instance of the command for each parameter you want to configure. The no form disables supplicant operation on the designated port(s)).

[identity <username>]

Sets the username and password to pass to the authenticator port when a challenge-request packet is received from the authenticator port due to an authentication request. If the intended authenticator port is configured for RADIUS authentication, then <username> and <password> must be the username and password expected by the RADIUS server. If the intended authenticator port is configured for Local authentication, then <username> and <password> must be the username and password configured on the Authenticator switch. (Default: Null.)
Configuring Port-Based and User-Based Access Control (802.1X)
Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches

aaa port-access supplicant [ethernet] < port-list > *(Syntax Continued)*

[secret]

**Enter secret:** < password >
**Repeat secret:** < password >

Sets the secret password to be used by the port supplicant when an MD5 authentication request is received from an authenticator. The switch prompts you to enter the secret password after the command is invoked.

[encrypted-secret]

Specify secret as a base64-encoded aes-256 encrypted string.

[auth-timeout < 1 - 300 >]

Sets the delay period the port waits to receive a challenge from the authenticator. If the request times out, the port sends another request, up to the number of attempts specified by the **max-start** parameter. (Default: 30 seconds).

[max-start < 1 - 10 >]

Defines the maximum number of times the supplicant port requests authentication. See step 1 on page 12-50 for a description of how the port reacts to the authenticator response. (Default: 3).

[held-period < 0 - 65535 >]

Sets the time period the supplicant port waits after an active 802.1X session fails before trying to re-acquire the authenticator port. (Default: 60 seconds)

[start-period < 1 - 300 >]

Sets the delay between Start packet retransmissions. That is, after a supplicant sends a start packet, it waits during the **start-period** for a response. If no response comes during the **start-period**, the supplicant sends a new start packet. The **max-start** setting (above) specifies how many start attempts are allowed in the session. (Default: 30 seconds)
Configuring Port-Based and User-Based Access Control (802.1X)
Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches

```
aaa port-access supplicant [ethernet] < port-list >
  [initialize]
      On the specified ports, blocks inbound and outbound traffic and restarts the 802.1X authentication process. Affects only ports configured as 802.1X supplicants.
  [clear-statistics]
      Clears and restarts the 802.1X supplicant statistics counters.
```
Displaying 802.1X Configuration, Statistics, and Counters

### 802.1X Authentication Commands
- page 12-17

### 802.1X Supplicant Commands
- page 12-50

### 802.1X Open VLAN Mode Commands
- page 12-32

### 802.1X-Related Show Commands
- show port-access authenticator
- page 12-57
- show port-access authenticator config
- page 12-58
- show port-access authenticator statistics
- page 12-59
- show port-access authenticator session-counters
- page 12-60
- show port-access authenticator vlan
- page 12-61
- show port-access authenticator clients
- page 12-62
- show port-access authenticator clients <port-list> detailed
- page 12-63
- show port-access supplicant
- page 12-68
- Details of 802.1X Mode Status Listings
- page 12-64

### RADIUS server configuration
- pages 12-26

---

**Show Commands for Port-Access Authenticator**

**Syntax:** show port-access authenticator [port-list]

[config | statistics | session-counters | vlan | clients [detailed]]

*If you enter the `show port-access authenticator` command without an optional value, the following configuration information is displayed for all switch ports, or specified ports, that are enabled for 802.1X port-access authentication:

- **Port-access authenticator activated:** Are any switch ports configured to operate as 802.1X authenticators using the `aaa port-access authenticator` command? Yes or No
- **Allow RADIUS-assigned dynamic (GVRP) VLANs:** Are RADIUS-assigned dynamic (GVRP-learned) VLANs supported for authenticated and unauthenticated client sessions on the switch? Yes or No
- **Auth Clients:** Number of authorized clients
- **Unauth Clients:** Number of unauthorized clients*
Syntax: show port-access authenticator [port-list]
           [config | statistics | session-counters | vlan | clients | clients detailed]
—Continued—

- **Untagged VLAN**: VLAN ID number of the untagged VLAN used in client sessions. If the switch supports MAC-based (untagged) VLANs, **MACbased** is displayed to show that multiple untagged VLANs are configured for authentication sessions.

- **Tagged VLANs**: Are tagged VLANs (statically configured or RADIUS-assigned) used for authenticated clients? Yes or No

- **Port COS**: 
  **Yes** - Client-specific CoS (Class of Service) values are applied to more than one authenticated client on the port.  
  **No** - No client-specific CoS values are applied to any authenticated client on the port.  
  `<cos-value>`- Numerical value of the CoS (802.1p priority) applied to inbound traffic from one authenticated client. For client-specific per-port CoS values, enter the `show port-access web-based clients detailed` command.

- **% In Limit**: Inbound rate limit applied.

- **RADIUS ACL**: Are RADIUS-assigned ACLs used for authenticated clients? Yes or No

- **Cntrl Dir**: Directions in which flow of incoming and outgoing traffic is blocked on 802.1X-aware port that has not yet entered the authenticated state:  
  **Both**: Incoming and outgoing traffic is blocked on port until authentication occurs.  
  **In**: Only incoming traffic is blocked on port before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on the unauthenticated 802.1X-aware port.
HP Switch(config)# show port-access authenticator

Port Access Authenticator Status

Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : Yes

<table>
<thead>
<tr>
<th>Port</th>
<th>Auth Clients</th>
<th>Unauth Clients</th>
<th>VLAN</th>
<th>Untagged VLANs</th>
<th>Tagged VLANs</th>
<th>% In</th>
<th>Port COS Limit</th>
<th>RADIUS Cntrl</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4006</td>
<td>Yes</td>
<td>77777777</td>
<td>No</td>
<td>Yes</td>
<td>both</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>MACbased</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>both</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>both</td>
</tr>
</tbody>
</table>

Figure 12-11. Example of show port-access authenticator Command

The information displayed with the show port-access authenticator command for individual (config | statistics | session-counters | vlan | clients) options is described below.

**Syntax:** show port-access authenticator config [port-list]

Displays 802.1X port-access authenticator configuration settings, including:

- Whether port-access authentication is enabled
- Whether RADIUS-assigned dynamic VLANs are supported
- 802.1X configuration of ports that are enabled as 802.1X authenticators (For a description of each setting, refer to the syntax descriptions in “2. Reconfigure Settings for Port-Access” on page 12-21. Use the show running command to view the current client-limit configuration available for switches.)

You can display 802.1X port-access authenticator configuration for all switch ports or specified ports. 802.1X configuration information for ports that are not enabled as 802.1X authenticators is not displayed.
Configuring Port-Based and User-Based Access Control (802.1X)
Displaying 802.1X Configuration, Statistics, and Counters

Figure 12-12. Example of show port-access authenticator config Command

<table>
<thead>
<tr>
<th>Port</th>
<th>Re-auth Access</th>
<th>Max Reqs</th>
<th>Quiet Period</th>
<th>TX Timeout</th>
<th>Supplicant Timeout</th>
<th>Server Timeout</th>
<th>Cntrl Dir</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>Auto</td>
<td>2</td>
<td>60</td>
<td>30</td>
<td>30</td>
<td>both</td>
</tr>
<tr>
<td>2</td>
<td>No</td>
<td>Auto</td>
<td>2</td>
<td>60</td>
<td>30</td>
<td>30</td>
<td>in</td>
</tr>
</tbody>
</table>

Table 12-2. Field Descriptions of show port-access authenticator config Command Output (Figure 12-12)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-access authenticator activated</td>
<td>Whether 802.1X authentication is enabled or disabled on specified port(s).</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on switch.</td>
</tr>
<tr>
<td>Re-auth Period</td>
<td>Period of time (in seconds) after which clients connected to the port need to be re-authenticated.</td>
</tr>
</tbody>
</table>
| Access Control | Port’s authentication mode:  
  **Auto**: Network access is allowed to any connected device that supports 802.1X authentication and provides valid 802.1X credentials.  
  **Authorized**: Network access is allowed to any device connected to the port, regardless of whether it meets 802.1X criteria.  
  **Unauthorized**: Network access is blocked to any device connected to the port, regardless of whether the device meets 802.1X criteria. |
| Max reqs | Number of authentication attempts that must time-out before authentication fails and the authentication session ends. |
| Quiet Period | Period of time (in seconds) during which the port does not try to acquire a supplicant. |
| TX Timeout | Period of time (in seconds) that the port waits to retransmit the next EAPOL PDU during an authentication session. |
| Supplicant Timeout | Period of time (in seconds) that the switch waits for a supplicant response to an EAP request. |
| Server Timeout | Period of time (in seconds) that the switch waits for a server response to an authentication request. |
| Cntrl Dir | Directions in which flow of incoming and outgoing traffic is blocked on 802.1X-aware port that has not yet entered the authenticated state:  
  **Both**: Incoming and outgoing traffic is blocked on port until authentication occurs.  
  **In**: Only incoming traffic is blocked on port before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on the unauthenticated 802.1X-aware port. |
Configuring Port-Based and User-Based Access Control (802.1X)
Displaying 802.1X Configuration, Statistics, and Counters

**Syntax:** `show port-access authenticator statistics [port-list]`

Displays statistical information for all switch ports or specified ports that are enabled as 802.1X authenticators, including:

- Whether port-access authentication is enabled
- Whether RADIUS-assigned dynamic VLANs are supported
- 802.1X supplicant's MAC address as determined by the content of the last EAPOL frame received on the port
- 802.1X traffic statistics from received and transmitted packets

802.1X configuration information for ports that are not enabled as an 802.1X authenticators is not displayed.

```bash
HP Switch(config)# show port-access authenticator statistics

Port Access Authenticator Statistics

Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

<table>
<thead>
<tr>
<th>Source</th>
<th>TX</th>
<th>TX</th>
<th>RX</th>
<th>RX</th>
<th>RX</th>
<th>RX</th>
<th>RX</th>
<th>RX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port MAC address</td>
<td>ReqId</td>
<td>Req</td>
<td>Start</td>
<td>Logoff</td>
<td>RespId</td>
<td>Resp</td>
<td>Errors</td>
<td></td>
</tr>
<tr>
<td>2  001560-b3ea48</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

*Figure 12-13. Example of show port-access authenticator statistics Command*
Syntax: show port-access authenticator session-counters [port-list]

Displays information for active 802.1X authentication sessions on all switch ports or specified ports that are enabled as 802.1X authenticators, including:

- 802.1X frames received and transmitted on each port
- Duration and status of active 802.1X authentication sessions (in-progress or terminated)
- User name of 802.1X supplicant included in 802.1X response packets, configured with the `aaa port-access supplicant-identity <username>` command (see page 13-49).

802.1X configuration information for ports that are not enabled as an 802.1X authenticators is not displayed.

```
HP Switch(config)# show port-access authenticator session-counters

Port Access Authenticator Session Counters

Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

<table>
<thead>
<tr>
<th>Session</th>
<th>Port Frames In</th>
<th>Frames Out</th>
<th>Time(sec.)</th>
<th>Status</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>45623</td>
<td>45623</td>
<td>20</td>
<td>in-progress</td>
<td>bert</td>
</tr>
</tbody>
</table>
```

Figure 12-14. Example of show port-access authenticator session-counters Command
Syntax: show port-access authenticator vlan [port-list]

Displays the following information on the VLANs configured for use in 802.1X port-access authentication on all switch ports, or specified ports, that are enabled as 802.1X authenticator:

- Authentication mode used on each port, configured with the `aaa port-access authenticator control` command (see page 12-21)
- VLAN ID (if any) to be used for traffic from 802.1X-authenticated clients
- VLAN ID (if any) to be used for traffic from unauthenticated clients

802.1X configuration information for ports that are not enabled as an 802.1X authenticators is not displayed.

```
HP Switch(config)# show port-access authenticator vlan

Port Access Authenticator VLAN Configuration

Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

<table>
<thead>
<tr>
<th>Access Port Control</th>
<th>Unauth VLAN ID</th>
<th>Auth VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Auto</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Syntax: show port-access authenticator clients [port-list]

Displays the session status, name, and address for each 802.1X port-access-authenticated client on the switch. Multiple authenticated clients may be displayed for the same port. The IP address displayed is taken from the DHCP binding table (learned through the DHCP Snooping feature).

- If DHCP snooping is not enabled on the switch, n/a (not available) is displayed for a client’s IP address.
- If an 802.1X-authenticated client uses an IPv6 address, n/a - IPv6 is displayed.
- If DHCP snooping is enabled but no MAC-to-IP address binding for a client is found in the DHCP binding table, n/a - no info is displayed.

<table>
<thead>
<tr>
<th>Port</th>
<th>Client Name</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Session Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>webuser1</td>
<td>001321-eb8063</td>
<td>192.192.192.192</td>
<td>Authenticated</td>
</tr>
<tr>
<td>1</td>
<td>webuser2</td>
<td>001560-b3ea48</td>
<td>n/a - no info</td>
<td>Authenticating</td>
</tr>
<tr>
<td>1</td>
<td>webuser3</td>
<td>000000-111111</td>
<td>n/a - IPv6</td>
<td>Authenticating</td>
</tr>
<tr>
<td>3</td>
<td>webuser4</td>
<td>000000-111112</td>
<td>n/a</td>
<td>Authenticating</td>
</tr>
</tbody>
</table>

Figure 12-16. Example of show port-access authenticator clients Command Output
Configuring Port-Based and User-Based Access Control (802.1X)
Displaying 802.1X Configuration, Statistics, and Counters

Syntax: show port-access authenticator clients <port-list> detailed

Displays detailed information on the status of 802.1X-authenticated client sessions on specified ports, including the matches the switch detects for individual ACEs configured with the cnt (counter) option in an ACL assigned to the port by a RADIUS server.

<table>
<thead>
<tr>
<th>Client Base Details:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port: 5</td>
</tr>
<tr>
<td>Session Status: Open</td>
</tr>
<tr>
<td>Session Time (sec): 999999999</td>
</tr>
<tr>
<td>Frames In: 999999999</td>
</tr>
<tr>
<td>Frames Out: 99999999</td>
</tr>
<tr>
<td>Username: webuser1</td>
</tr>
<tr>
<td>MAC Address: 001321-eb8063</td>
</tr>
</tbody>
</table>

Access Policy Details:
- COS Map: 70000000
- In Limit %: 87
- Untagged VLAN: 3096
- Out Limit %: 100
- Tagged VLANs: 1, 3, 5, 6, 334, 2066
- RADIUS-ACL List:
  - deny in udp from any to 10.2.8.233 CNT
    - Hit Count: 10
  - permit in udp from any to 10.2.8.233 CNT
    - Hit Count: 17
  - deny in tcp from any to 10.2.8.233 CNT
    - Hit Count: 1
  - permit in tcp from any to 10.2.8.233 CNT
    - Hit Count: 11
  - permit in ip from any to any cnt
    - Hit Count: 42

Figure 12-17. Example of show port-access authenticator clients detailed Command Output
Viewing 802.1X Open VLAN Mode Status

You can examine the switch's current VLAN status by using the **show port-access authenticator vlan** and **show port-access authenticator < port-list >** commands as illustrated in figure 12-18. Table 12-1 describes the data that these two commands display. Figure 12-19 shows related VLAN data that can help you to see how the switch is using statically configured VLANs to support 802.1X operation.

---

**Table 12-1**

<table>
<thead>
<tr>
<th>Port</th>
<th>Control</th>
<th>VLAN ID</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Auto</td>
<td>100</td>
<td>101</td>
</tr>
<tr>
<td>2</td>
<td>Auto</td>
<td>100</td>
<td>101</td>
</tr>
<tr>
<td>3</td>
<td>Auto</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Auto</td>
<td>100</td>
<td>101</td>
</tr>
</tbody>
</table>

---

**Figure 12-18. Example Showing Ports Configured for Open VLAN Mode**

---

Items 1 through 3 indicate that an authenticated client is connected to port 2:

1. **Open** in the Status column
2. **Authorized** in the Authenticator State column
3. The Auth VLAN ID (101) is also in the Current VLAN ID column. (This assumes that the port is not a statically configured member of VLAN 101.)
4. A "0" in the row for port 3 indicates there is no Authorized VLAN configured for port 3.
5. No PVID means there is currently no untagged VLAN membership on port 4.

---

**Note:** Series 5400zl switches do not include the Authenticator State and Authenticator Backend State fields shown in this figure.
Configuring Port-Based and User-Based Access Control (802.1X)  
Displaying 802.1X Configuration, Statistics, and Counters

Thus, in the output shown in figure 12-18:

- When the **Auth VLAN ID** is configured and matches the **Current VLAN ID**, an authenticated client is connected to the port. (This assumes the port is not a statically configured member of the VLAN you are using for Auth VLAN.)

- When the **Unauth VLAN ID** is configured and matches the **Current VLAN ID**, an unauthenticated client is connected to the port. (This assumes the port is not a statically configured member of the VLAN you are using for Unauth VLAN.)

Note that because a temporary Open VLAN port assignment to either an authorized or unauthorized VLAN is an untagged VLAN membership, these assignments temporarily replace any other untagged VLAN membership that is statically configured on the port. For example, if port 12 is statically configured as an untagged member of VLAN 1, but is configured to use VLAN 25 as an authorized VLAN, then the port's membership in VLAN 1 will be temporarily suspended whenever an authenticated 802.1X client is attached to the port.

<table>
<thead>
<tr>
<th>Table 12-1. Output for Determining Open VLAN Mode Status (Figure 12-18, Upper)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status Indicator</strong></td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Unauthorized VLAN ID</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Authorized VLAN ID</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Table 12-2. Output for Determining Open VLAN Mode Status (Figure 12-18, Lower)

<table>
<thead>
<tr>
<th>Status Indicator</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| Status           | Closed: Either no client is connected or the connected client has not received authorization through 802.1X authentication.  
|                   | Open: An authorized 802.1X supplicant is connected to the port. |

| Current VLAN ID   | < vlan-id >: Lists the VID of the static, untagged VLAN to which the port currently belongs.  
|                   | No PVID: The port is not an untagged member of any VLAN. |


| % Curr. Rate Limit Inbound |

Syntax:    show vlan < vlan-id >

Displays the port status for the selected VLAN, including an indication of which port memberships have been temporarily overridden by Open VLAN mode.
Configuring Port-Based and User-Based Access Control (802.1X)
Displaying 802.1X Configuration, Statistics, and Counters

```
HP Switch(config)# show vlan 1

Status and Counters - VLAN Information - VLAN 1

VLAN ID : 1
Name : DEFAULT_VLAN
Status : Static
Voice : No
Jumbo : No

<table>
<thead>
<tr>
<th>Port Information Mode</th>
<th>Unknown VLAN Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>A2</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>A3</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>A4</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B1</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B2</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B3</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B4</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B5</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B6</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B7</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B8</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B9</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B10</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B11</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B12</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B13</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B14</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B15</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B16</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B17</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B18</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B19</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B20</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B21</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B22</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B23</td>
<td>Untagged Learn</td>
</tr>
<tr>
<td>B24</td>
<td>Untagged Learn</td>
</tr>
</tbody>
</table>

Overridden Port VLAN configuration

<table>
<thead>
<tr>
<th>Port Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
</tr>
<tr>
<td>B3</td>
</tr>
</tbody>
</table>
```

Note that ports B1 and B3 are not in the upper listing, but are included under “Overridden Port VLAN configuration”. This shows that static, untagged VLAN memberships on ports B1 and B3 have been overridden by temporary assignment to the authorized or unauthorized VLAN. Using the `show port-access authenticator <port-list>` command shown in figure 12-18 provides details.

Figure 12-19. Example of Showing a VLAN with Ports Configured for Open VLAN Mode
Show Commands for Port-Access Supplicant

**Syntax:**

```plaintext
show port-access supplicant [<port-list>] [statistics]
show port-access supplicant [<port-list>]
```

*Shows the port-access supplicant configuration (excluding the secret parameter) for all ports or <port-list> ports configured on the switch as supplicants. The Supplicant State can include the following:

- **Connecting** - Starting authentication.
- **Authenticated** - Authentication completed (regardless of whether the attempt was successful).
- **Acquired** - The port received a request for identification from an authenticator.
- **Authenticating** - Authentication is in progress.
- **Held** - Authenticator sent notice of failure. The supplicant port is waiting for the authenticator's held-period (page 12-52).

For descriptions of the supplicant parameters, refer to “Configuring a Supplicant Switch Port” on page 12-52.

```plaintext
show port-access supplicant [<port-list>] statistics
```

*Shows the port-access statistics and source MAC address(es) for all ports or <port-list> ports configured on the switch as supplicants. See the “Note on Supplicant Statistics”, below.*

**Note on Supplicant Statistics.** For each port configured as a supplicant, `show port-access supplicant statistics <port-list>` displays the source MAC address and statistics for transactions with the authenticator device most recently detected on the port. If the link between the supplicant port and the authenticator device fails, the supplicant port continues to show data received from the connection to the most recent authenticator device until one of the following occurs:

- The supplicant port detects a different authenticator device.
- You use the `aaa port-access supplicant <port-list> clear-statistics` command to clear the statistics for the supplicant port.
- The switch reboots.

Thus, if the supplicant’s link to the authenticator fails, the supplicant retains the transaction statistics it most recently received until one of the above events occurs. Also, if you move a link with an authenticator from one
supplicant port to another without clearing the statistics data from the first port, the authenticator’s MAC address will appear in the supplicant statistics for both ports.

---

**How RADIUS/802.1X Authentication Affects VLAN Operation**

**Static VLAN Requirement.** RADIUS authentication for an 802.1X client on a given port can include a (static) VLAN requirement. (Refer to the documentation provided with your RADIUS application.) The static VLAN to which a RADIUS server assigns a client must already exist on the switch. If it does not exist or is a dynamic VLAN (created by GVRP), authentication fails. Also, for the session to proceed, the port must be an untagged member of the required VLAN. If it is not, the switch temporarily reassigns the port as described below.

**If the Port Used by the Client Is Not Configured as an Untagged Member of the Required Static VLAN:** When a client is authenticated on port “N”, if port “N” is not already configured as an untagged member of the static VLAN specified by the RADIUS server, then the switch temporarily assigns port “N” as an untagged member of the required VLAN (for the duration of the 802.1X session). At the same time, if port “N” is already configured as an untagged member of another VLAN, port “N” loses access to that other VLAN for the duration of the session. (This is because a port can be an untagged member of only one VLAN at a time.)

Using a RADIUS server to authenticate clients, you can provide port-level security protection from unauthorized network access for the following authentication methods:

- **802.1X:** Port-based or client-based access control to open a port for client access after authenticating valid user credentials.
- **MAC address:** Authenticates a device’s MAC address to grant access to the network.
- **WebAgent:** Authenticates clients for network access using a web page for user login.
You can use 802.1X (port-based or client-based) authentication and either Web or MAC authentication at the same time on a port, with a maximum of 32 clients allowed on the port. (The default is one client.) Web authentication and MAC authentication are mutually exclusive on the same port. Also, you must disable LACP on ports configured for any of these authentication methods. For more information, see “Web and MAC Authentication” on page 3-1 in this guide.

VLAN Assignment on a Port

Following client authentication, VLAN configurations on a port are managed as follows when you use 802.1X, MAC, or Web authentication:

- The port resumes membership in any tagged VLANs for which it is already assigned in the switch configuration. Tagged VLAN membership allows a port to be a member of multiple VLANs simultaneously.
- The port is temporarily assigned as a member of an untagged (static or dynamic) VLAN for use during the client session according to the following order of options.
  a. The port joins the VLAN to which it has been assigned by a RADIUS server during client authentication.
  b. If RADIUS authentication does not include assigning the port to a VLAN, then the switch assigns the port to the authorized-client VLAN configured for the authentication method.
  c. If the port does not have an authorized-client VLAN configured, but is configured for membership in an untagged VLAN, the switch assigns the port to this untagged VLAN.

Operating Notes

- During client authentication, a port assigned to a VLAN by a RADIUS server or an authorized-client VLAN configuration is an untagged member of the VLAN for the duration of the authenticated session. This applies even if the port is also configured in the switch as a tagged member of the same VLAN. The following restrictions apply:
  - If the port is assigned as a member of an untagged static VLAN, the VLAN must already be configured on the switch. If the static VLAN configuration does not exist, the authentication fails.
Configuring Port-Based and User-Based Access Control (802.1X)
How RADIUS/802.1X Authentication Affects VLAN Operation

- If the port is assigned as a member of an untagged dynamic VLAN that was learned through GVRP, the dynamic VLAN configuration must exist on the switch at the time of authentication and GVRP-learned dynamic VLANs for port-access authentication must be enabled.

If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.

- To enable the use of a GVRP-learned (dynamic) VLAN as the untagged VLAN used in an authentication session, enter the `aaa port-access gvrp-vlans` command, as described in “Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions” on page 12-76.

- Enabling the use of dynamic VLANs in an authentication session offers the following benefits:
  - You avoid the need of having static VLANs pre-configured on the switch.
  - You can centralize the administration of user accounts (including user VLAN IDs) on a RADIUS server.

  For information on how to enable the switch to dynamically create 802.1Q-compliant VLANs on links to other devices using the GARP VLAN Registration Protocol (GVRP), see the chapter on “GVRP” in the Advanced Traffic Management Guide.

- For an authentication session to proceed, a port must be an untagged member of the (static or dynamic) VLAN assigned by the RADIUS server (or an authorized-client VLAN configuration). The port temporarily drops any current untagged VLAN membership.

  If the port is not already a member of the RADIUS-assigned (static or dynamic) untagged VLAN, the switch temporarily reassigns the port as an untagged member of the required VLAN (for the duration of the session). At the same time, if the port is already configured as an untagged member of a different VLAN, the port loses access to the other VLAN for the duration of the session. (A port can be an untagged member of only one VLAN at a time.)

  When the authentication session ends, the switch removes the temporary untagged VLAN assignment and re-activates the temporarily disabled, untagged VLAN assignment.

- If GVRP is already enabled on the switch, the temporary untagged (static or dynamic) VLAN created on the port for the authentication session is advertised as an existing VLAN.
If this temporary VLAN assignment causes the switch to disable a different untagged static or dynamic VLAN configured on the port (as described in the preceding bullet and in “Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session” on page 12-72), the disabled VLAN assignment is not advertised. When the authentication session ends, the switch:

- Removes the temporary untagged VLAN assignment and stops advertising it.
- Re-activates and resumes advertising the temporarily disabled, untagged VLAN assignment.

If you modify a VLAN ID configuration on a port during an 802.1X, MAC, or Web authentication session, the changes do not take effect until the session ends.

When a switch port is configured with RADIUS-based authentication to accept multiple 802.1X and/or MAC or Web authentication client sessions, all authenticated clients must use the same port-based, untagged VLAN membership assigned for the earliest, currently active client session.

Therefore, on a port where one or more authenticated client sessions are already running, all such clients are on the same untagged VLAN (unless MAC-based VLANs are enabled. Please see “MAC-Based VLANs” on page 5-46). If a RADIUS server subsequently authenticates a new client, but attempts to re-assign the port to a different, untagged VLAN than the one already in use for the previously existing, authenticated client sessions, the connection for the new client will fail.

Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session

The following example shows how an untagged static VLAN is temporarily assigned to a port for use during an 802.1X authentication session. In the example, an 802.1X-aware client on port A2 has been authenticated by a RADIUS server for access to VLAN 22. However, port A2 is not configured as a member of VLAN 22 but as a member of untagged VLAN 33 as shown in Figure 12-20.
For example, suppose that a RADIUS-authenticated, 802.1X-aware client on port A2 requires access to VLAN 22, but VLAN 22 is configured for no access on port A2, and VLAN 33 is configured as untagged on port A2:

```
Port  default_vlan vlan_22 vlan_33 vlan_44
--- + --------- + + + +
A1 | Untagged  Tagged No No
A2 | No        No  Untagged No
A3 | Untagged  No  Forbid Forbid
A4 | Untagged  Tagged Tagged
```

Figure 12-20.Example of an Active VLAN Configuration

In Figure 12-20, if RADIUS authorizes an 802.1X client on port A2 with the requirement that the client use VLAN 22, then:

■ VLAN 22 becomes available as Untagged on port A2 for the duration of the session.
■ VLAN 33 becomes unavailable to port A2 for the duration of the session (because there can be only one untagged VLAN on any port).

To view the temporary VLAN assignment as a change in the active configuration, use the `show vlan <vlan-id>` command as shown in Figure 12-21 where `<vlan-id>` is the (static or dynamic) VLAN used in the authenticated client session.
However, as shown in Figure 12-20, because VLAN 33 is configured as untagged on port A2 and because a port can be untagged on only one VLAN, port A2 loses access to VLAN 33 for the duration of the 802.1X session on VLAN 22.

You can verify the temporary loss of access to VLAN 33 by entering the `show vlan 33` command as shown in Figure 12-22.
Port Information Mode Unknown VLAN Status
---------------- -------- ------------ 
A4 Tagged Learn Up

Figure 12-22. The Active Configuration for VLAN 33 Temporarily Drops Port 22 for the 802.1X Session

When the 802.1X client’s session on port A2 ends, the port removes the temporary untagged VLAN membership. The static VLAN (VLAN 33) that is “permanently” configured as untagged on the port becomes available again. Therefore, when the RADIUS-authenticated 802.1X session on port A2 ends, VLAN 22 access on port A2 also ends, and the untagged VLAN 33 access on port A2 is restored as shown in Figure 12-23.

After the 802.1X session on VLAN 22 ends, the active configuration again includes VLAN 33 on port A2.
Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions

**Syntax:**  
`aaa port-access gvrp-vlans`

Enables the use of GVRP VLANs (learned through GVRP) in the temporary untagged VLAN assigned by a RADIUS server on an authenticated port in an 802.1X, MAC, or Web authentication session.

Enter the `no` form of this command to disable the use of GVRP-learned VLANs in an authentication session.

For information on how to enable a switch to dynamically create 802.1Q-compliant VLANs, see the chapter on “GVRP” in the Advanced Traffic Management Guide.

**Notes:**

1. If a port is assigned as a member of an untagged dynamic VLAN, the dynamic VLAN configuration must exist at the time of authentication and GVRP for port-access authentication must be enabled on the switch.

   If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.

2. After you enable dynamic VLAN assignment in an authentication session, it is recommended that you use the `interface unknown-vlans` command on a per-port basis to prevent denial-of-service attacks. The `interface unknown-vlans` command allows you to:
   - Disable the port from sending advertisements of existing GVRP-created VLANs on the switch.
   - Drop all GVRP advertisements received on the port.

For more information, refer to the chapter on “GVRP” in the Advanced Traffic Management Guide.
3. If you disable the use of dynamic VLANs in an authentication session using the `no aaa port-access gvrp-vlans` command, client sessions that were authenticated with a dynamic VLAN continue and are not deauthenticated. (This behavior differs from how static VLAN assignment is handled in an authentication session. If you remove the configuration of the static VLAN used to create a temporary client session, the 802.1X, MAC, or Web authenticated client is deauthenticated.) However, if a RADIUS-configured dynamic VLAN used for an authentication session is deleted from the switch through normal GVRP operation (for example, if no GVRP advertisements for the VLAN are received on any switch port), authenticated clients using this VLAN are deauthenticated.

**Note**

Any port VLAN-ID changes you make on 802.1X-aware ports during an 802.1X-authenticated session do not take effect until the session ends.

With GVRP enabled, a temporary, untagged static VLAN assignment created on a port by 802.1X authentication is advertised as an existing VLAN. If this temporary VLAN assignment causes the switch to disable a configured (untagged) static VLAN assignment on the port, then the disabled VLAN assignment is not advertised. When the 802.1X session ends, the switch:

- Eliminates and ceases to advertise the temporary VLAN assignment.
- Re-activates and resumes advertising the temporarily disabled VLAN assignment.
### Messages Related to 802.1X Operation

#### Table 12-3. 802.1X Operating Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port <code>&lt;port-list&gt;</code> is not an authenticator.</td>
<td>The ports in the port list have not been enabled as 802.1X authenticators. Use this command to enable the ports as authenticators: <code>HP Switch(config)# aaa port-access authenticator e 10</code></td>
</tr>
<tr>
<td>Port <code>&lt;port-list&gt;</code> is not a supplicant.</td>
<td>Occurs when there is an attempt to change the supplicant configuration on a port that is not currently enabled as a supplicant. Enable the port as a supplicant and then make the desired supplicant configuration changes. Refer to “Enabling a Switch Port as a Supplicant” on page 12-52.</td>
</tr>
<tr>
<td>No server(s) responding.</td>
<td>This message can appear if you configured the switch for EAP-RADIUS or CHAP-RADIUS authentication, but the switch does not receive a response from a RADIUS server. Ensure that the switch is configured to access at least one RADIUS server. (Use <code>show radius</code>.) If you also see the message Can’t reach RADIUS server <code>&lt;x.x.x.x&gt;</code>, try the suggestions listed for that message (page 5-79).</td>
</tr>
<tr>
<td>LACP has been disabled on 802.1X port(s).</td>
<td>To maintain security, LACP is not allowed on ports configured for 802.1X authenticator operation. If you configure port security on a port on which LACP (active or passive) is configured, the switch removes the LACP configuration, displays a notice that LACP is disabled on the port(s), and enables 802.1X on that port.</td>
</tr>
<tr>
<td>Error configuring port <code>&lt;port-number&gt;</code>: LACP and 802.1X cannot be run together.</td>
<td>Also, the switch will not allow you to configure LACP on a port on which port access (802.1X) is enabled.</td>
</tr>
</tbody>
</table>
Configuring and Monitoring Port Security

Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>WebAgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying Current Port Security</td>
<td>n/a</td>
<td>—</td>
<td>page 13-8</td>
<td></td>
</tr>
<tr>
<td>Configuring Port Security</td>
<td>disabled</td>
<td>—</td>
<td>page 13-12</td>
<td></td>
</tr>
<tr>
<td>Retention of Static Addresses</td>
<td>n/a</td>
<td>—</td>
<td>page 13-17</td>
<td>n/a</td>
</tr>
<tr>
<td>MAC Lockdown</td>
<td>disabled</td>
<td>—</td>
<td>page 13-24</td>
<td></td>
</tr>
<tr>
<td>MAC Lockout</td>
<td>disabled</td>
<td>—</td>
<td>page 13-32</td>
<td></td>
</tr>
<tr>
<td>Intrusion Alerts and Alert Flags</td>
<td>n/a</td>
<td>page 13-41</td>
<td>page 13-39</td>
<td>page 13-41</td>
</tr>
</tbody>
</table>

**Port Security (Page 13-2).** This feature enables you to configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch.

**Note**

This feature does not prevent intruders from receiving broadcast and multicast traffic. Also, Port Security and MAC Lockdown are mutually exclusive on a switch. If one is enabled, then the other cannot be used.

**MAC Lockdown (Page 13-24).** This feature, also known as “Static Addressing”, is used to prevent station movement and MAC address “hijacking” by allowing a given MAC address to use only an assigned port on the switch. MAC Lockdown also restricts the client device to a specific VLAN. (See also the **Note**, above.)

**MAC Lockout (Page 13-32).** This feature enables you to block a specific MAC address so that the switch drops all traffic to or from the specified address.
Port Security

Basic Operation

**Default Port Security Operation.** The default port security setting for each port is off, or “continuous”. That is, any device can access a port without causing a security reaction.

**Intruder Protection.** A port that detects an “intruder” blocks the intruding device from transmitting to the network through that port.

**Eavesdrop Protection.** Using either the port-security command or the switch's WebAgent to enable port security on a given port automatically enables eavesdrop prevention on that port.

**General Operation for Port Security.** On a per-port basis, you can configure security measures to block unauthorized devices, and to send notice of security violations. Once port security is configured, you can then monitor the network for security violations through one or more of the following:

- Alert flags that are captured by network management tools such as PCM+
- Alert Log entries in the WebAgent
- Event Log entries in the console interface
- Intrusion Log entries in the menu interface, CLI, or WebAgent

For any port, you can configure the following:

- **Action:** Used when a port detects an intruder. Specifies whether to send an SNMP trap to a network management station and whether to disable the port.
- **Address Limit:** Sets the number of authorized MAC addresses allowed on the port.
- **Learn-Mode:** Specify how the port acquires authorized addresses.
  - **Continuous:** Allows the port to learn addresses from inbound traffic from any connected device. This is the default setting.
  - **Limited-Continuous:** Sets a finite limit (1 - 32) to the number of learned addresses allowed per port.
Configuring and Monitoring Port Security
Port Security

- **Static**: Enables you to set a fixed limit on the number of MAC addresses authorized for the port and to specify some or all of the authorized addresses. (If you specify only some of the authorized addresses, the port learns the remaining authorized addresses from the traffic it receives from connected devices.)
- **Configured**: Requires that you specify all MAC addresses authorized for the port. The port is not allowed to learn addresses from inbound traffic.

- **Authorized (MAC) Addresses**: Specify up to eight devices (MAC addresses) that are allowed to send inbound traffic through the port. This feature:
  - Closes the port to inbound traffic from any unauthorized devices that are connected to the port.
  - Provides the option for sending an SNMP trap notifying of an attempted security violation to a network management station and, optionally, disables the port. (For more on configuring the switch for SNMP management, see “Trap Receivers and Authentication Traps” in the Management and Configuration Guide for your switch.)
- **Port Access**: Allows only the MAC address of a device authenticated through the switch’s 802.1X Port-Based access control. Refer to chapter 12, Configuring Port-Based and User-Based Access Control (802.1X).

For configuration details, refer to “Configuring Port Security” on page 13-12.

Eavesdrop Prevention

Configuring port security on a given switch port automatically enables Eavesdrop Prevention for that port. This prevents use of the port to flood unicast packets addressed to MAC addresses unknown to the switch and blocks unauthorized users from eavesdropping on traffic intended for addresses that have aged-out of the switch’s address table. (Eavesdrop Prevention does not affect multicast and broadcast traffic; the switch floods these two traffic types out a given port regardless of whether port security is enabled on that port.)

Disabling Eavesdrop Prevention

Traffic with an unknown destination address is blocked when port security is configured and Eavesdrop Prevention is enabled. You can disable Eavesdrop Prevention on ports where it may cause problems, such as on ports that are configured to use limited-continuous learning mode. See “Configuring Port Security” on page 13-12 for more information on learning modes.
Feature Interactions When Eavesdrop Prevention is Disabled

The following table explains the various interactions between learning modes and Eavesdrop Prevention when Eavesdrop Prevention is disabled.

**Note**
When the learning mode is “port-access”, Eavesdrop Prevention will not be applied to the port. However, it can still be configured or disabled for the port.

<table>
<thead>
<tr>
<th>Learn Mode</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured and only a limited number of static MAC addresses are learned. A device must generate traffic before the MAC address is learned and traffic is forwarded to it.</td>
</tr>
<tr>
<td>Continuous</td>
<td>The default. The Eavesdrop Prevention option does not apply because port security is disabled. Ports forward traffic with unknown destination addresses normally.</td>
</tr>
<tr>
<td>Port-access</td>
<td>Disabling Eavesdrop Prevention is not applied to the port. There is no change.</td>
</tr>
<tr>
<td>Limited-continuous</td>
<td>When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured; MAC addresses age normally. Eavesdrop Prevention may cause difficulties in learning MAC addresses (as with static MAC addresses) and cause serious traffic issues when a MAC ages out.</td>
</tr>
<tr>
<td>Configured</td>
<td>When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured by a static MAC address. Eavesdrop Prevention should not cause any issues because all valid MAC addresses have been configured.</td>
</tr>
</tbody>
</table>

**Syntax**

```
[no] port-security <port-list> eavesdrop-prevention
```

When this option is enabled, the port is prevented from transmitting packets that have unknown destination addresses. Only devices attached to the port receive packets intended for them. This option does not apply to a learning mode of port-access or continuous.

Default: Enabled
Configuring and Monitoring Port Security

Port Security

Figure 13-1. Example of show port-security Command Displaying Eavesdrop Prevention

<table>
<thead>
<tr>
<th>Port</th>
<th>Learn Mode</th>
<th>Action</th>
<th>Eavesdrop Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Continuous</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>2</td>
<td>Continuous</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>3</td>
<td>Continuous</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>4</td>
<td>Continuous</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>5</td>
<td>Continuous</td>
<td>None</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

MIB Support

The following MIB support is provided for Eavesdrop Prevention.

```
hpSecPtPreventEavesdrop OBJECT-TYPE
    SYNTAX INTEGER {
        enable (1),
        disable (2)
    }
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        “If enabled on a switch, outbound unknown unicast packets will not be forwarded out this port. If enabled on a repeater, outbound unknown unicast packets for this port will be scrambled.
    ::= { hpSecurePortEntry 5 }
```

Blocking Unauthorized Traffic

Unless you configure the switch to disable a port on which a security violation is detected, the switch security measures block unauthorized traffic without disabling the port. This implementation enables you to apply the security configuration to ports on which hubs, switches, or other devices are connected, and to maintain security while also maintaining network access to authorized users. For example:

```
HP Switch(config)# show port-security
```
Configuring and Monitoring Port Security

Port Security

Figure 13-2. Example of How Port Security Controls Access

Note

Broadcast and Multicast traffic is always allowed, and can be read by intruders connected to a port on which you have configured port security.

Trunk Group Exclusion

Port security does not operate on either a static or dynamic trunk group. If you configure port security on one or more ports that are later added to a trunk group, the switch will reset the port security parameters for those ports to the factory-default configuration. (Ports configured for either Active or Passive LACP, and which are not members of a trunk, can be configured for port security.)
Planning Port Security

1. Plan your port security configuration and monitoring according to the following:
   a. On which ports do you want port security?
   b. Which devices (MAC addresses) are authorized on each port?
   c. For each port, what security actions do you want? (The switch automatically blocks intruders detected on that port from transmitting to the network.) You can configure the switch to (1) send intrusion alarms to an SNMP management station and to (2) optionally disable the port on which the intrusion was detected.
   d. How do you want to learn of the security violation attempts the switch detects? You can use one or more of these methods:
      – Through network management (That is, do you want an SNMP trap sent to a net management station when a port detects a security violation attempt?)
      – Through the switch’s Intrusion Log, available through the CLI, menu, and WebAgent
      – Through the Event Log (in the menu interface or through the CLI show log command)

2. Use the CLI or WebAgent to configure port security operating and address controls. The following table describes the parameters.
Port Security Command Options and Operation

**Port Security Commands Used in This Section**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show port-security</td>
<td>13-9</td>
</tr>
<tr>
<td>show mac-address</td>
<td>13-10</td>
</tr>
<tr>
<td>port-security</td>
<td>13-12</td>
</tr>
<tr>
<td>&lt; port-list&gt;</td>
<td>13-12</td>
</tr>
<tr>
<td>learn-mode</td>
<td>13-12</td>
</tr>
<tr>
<td>address-limit</td>
<td>13-15</td>
</tr>
<tr>
<td>mac-address</td>
<td>13-16</td>
</tr>
<tr>
<td>action</td>
<td>13-16</td>
</tr>
<tr>
<td>clear-intrusion-flag</td>
<td>13-17</td>
</tr>
<tr>
<td>no port-security</td>
<td>13-17</td>
</tr>
</tbody>
</table>

This section describes the CLI port security command and how the switch acquires and maintains authorized addresses.

**Note**

Use the global configuration level to execute port-security configuration commands.

**Port Security Display Options**

You can use the CLI to display the current port-security settings and to list the currently authorized MAC addresses the switch detects on one or more ports.
Configuring and Monitoring Port Security
Port Security

Displaying Port Security Settings.

**Syntax:**

```
show port-security
show port-security <port number>
show port-security [<port number>-<port number>]...
```

The CLI uses the same command to provide two types of port security listings:

- All ports on the switch with their Learn Mode and (alarm) Action
- Only the specified ports with their Learn Mode, Address Limit, (alarm) Action, and Authorized Addresses

Without port parameters, `show port-security` displays Operating Control settings for all ports on a switch.

```
HP Switch(config)# show port-security
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Learn Mode</th>
<th>Action</th>
<th>Eavesdrop Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Continuous</td>
<td>Send Alarm, Disable Port</td>
<td>Enabled</td>
</tr>
<tr>
<td>2</td>
<td>Continuous</td>
<td>Send Alarm, Disable Port</td>
<td>Enabled</td>
</tr>
<tr>
<td>3</td>
<td>Static</td>
<td>Send Alarm</td>
<td>Enabled</td>
</tr>
<tr>
<td>4</td>
<td>Continuous</td>
<td>Send Alarm, Disable Port</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Figure 13-3. Example Port Security Listing (Ports A7 and A8 Show the Default Setting)

With port numbers included in the command, `show port-security` displays Learn Mode, Address Limit, (alarm) Action, and Authorized Addresses for the specified ports on a switch. The following example lists the full port security configuration for a single port:
Configuring and Monitoring Port Security

Port Security

Figure 13-4. Example of the Port Security Configuration Display for a Single Port

The next example shows the option for entering a range of ports, including a series of non-contiguous ports. Note that no spaces are allowed in the port number portion of the command string:

HP Switch(config)# show port-security A1-A3,A6,A8

Listing Authorized and Detected MAC Addresses.

Syntax: show mac-address [ port-list | mac-address | vlan < vid > ]

Without an optional parameter, show mac-address lists the authorized MAC addresses that the switch detects on all ports.

mac-address: Lists the specified MAC address with the port on which it is detected as an authorized address.

port list: Lists the authorized MAC addresses detected on the specified port(s).

vlan < vid >: Lists the authorized MAC addresses detected on ports belonging to the specified VLAN.
Switch(config)# show mac-address
Status and Counters - Port Address Table

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Port</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000c-07ac00</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>0000aa-9c09cb</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>000102-f215c7</td>
<td>5</td>
<td>100</td>
</tr>
<tr>
<td>0018fe-a5e504</td>
<td>1</td>
<td>222</td>
</tr>
</tbody>
</table>

Switch(config)# show mac-address 7
Status and Counters - Port Address Table - 7

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000c-07ac00</td>
<td></td>
</tr>
<tr>
<td>0000aa-9c09cb</td>
<td></td>
</tr>
</tbody>
</table>

Switch(config)# show mac-address 00000c-07ac00
Status and Counters - Address Table - 00000c-07ac00

<table>
<thead>
<tr>
<th>Port</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>100</td>
</tr>
</tbody>
</table>

Switch(config)# show mac-address vlan 1
Status and Counters - Address Table - VLAN 1

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000c-07ac00</td>
<td></td>
</tr>
<tr>
<td>000050-53c774</td>
<td></td>
</tr>
</tbody>
</table>

Figure 13-5. Examples of Show Mac-Address Outputs
Configuring Port Security

Using the CLI, you can:

- Configure port security and edit security settings.
- Add or delete devices from the list of authorized addresses for one or more ports.
- Clear the Intrusion flag on specific ports

Syntax: port-security

\[ \text{[e]} \text{<port-list>} \text{<learn-mode | address-limit | mac-address | action | clear-intrusion-flag >} \]

\(<\text{port-list}>\): Specifies a list of one or more ports to which the port-security command applies.

\(\text{learn-mode < continuous | static | port-access | configured | limited-continuous >} \)

For the specified port:

- Identifies the method for acquiring authorized addresses.
- On switches covered in this guide, automatically invokes eavesdrop protection. (Refer to “Eavesdrop Prevention” on page 13-3.)

\(\text{continuous (Default): Appears in the factory-default setting or when you execute no port-security. Allows the port to learn addresses from the device(s) to which it is connected. In this state, the port accepts traffic from any device(s) to which it is connected. Addresses learned in the learn continuous mode will “age out” and be automatically deleted if they are not used regularly. The default age time is five minutes.}

Addresses learned this way appear in the switch and port address tables and age out according to the MAC Age Interval in the System Information configuration screen of the Menu interface or the show system information listing. You can set the MAC age out time using the CLI, SNMP, Web, or menu interfaces. For more information on the mac-age-time command refer to the chapter titled “Interface Access and System Information” in the Basic Operation Guide for your switch.

— Continued —
Syntax:  port-security (Continued)

    learn-mode < continuous | static | port-access | configured | limited-continuous > (Continued)

    static: Enables you to use the **mac-address** parameter to specify the MAC addresses of the devices authorized for a port, and the **address-limit** parameter (explained below) to specify the number of MAC addresses authorized for the port. You can authorize specific devices for the port, while still allowing the port to accept other, non-specified devices until the device limit has been reached. That is, if you enter fewer MAC addresses than you authorized, the port authorizes the remaining addresses in the order in which it automatically learns them.

    For example, if you use address-limit to specify three authorized devices, but use **mac-address** to specify only one authorized MAC address, the port adds the one specifically authorized MAC address to its authorized-devices list and the first two additional MAC addresses it detects.

    If, for example:
    You use **mac-address** to authorize MAC address 0060b0-880a80 for port A4.
    You use **address-limit** to allow three devices on port A4 and the port detects these MAC addresses:

    1. 080090-1362f2
    2. 00f031-423fc1
    3. 080071-0c45a1
    4. 0060b0-880a80 (the address you authorized with the **mac-address** parameter)

    In this example port A4 would assume the following list of authorized addresses:

    080090-1362f2 (the first address the port detected)
    00f031-423fc1 (the second address the port detected)
    0060b0-880a80 (the address you authorized with the **mac-address** parameter)

    The remaining MAC address detected by the port, 080071-0c45a1, is not allowed and is handled as an intruder. Learned addresses that become authorized do not age-out. See also “Retention of Static Addresses” on page 13-17.

    — Continued —
Syntax: port-security (Continued)

learn-mode < continuous | static | port-access | configured | limited-continuous > (Continued)

**Caution:** Using the **static** parameter with a device limit greater than the number of MAC addresses specified with **mac-address** can allow an unwanted device to become “authorized”. This is because the port, to fulfill the number of devices allowed by the **address-limit** parameter (see below), automatically adds devices it detects until it reaches the specified limit.

**Note:** If 802.1X port-access is configured on a given port, then port-security learn-mode must be set to either **continuous** (the default) or **port-access**.

**port-access:** Enables you to use Port Security with (802.1X) Port-Based Access Control. Refer to chapter 12, Configuring Port-Based and User-Based Access Control (802.1X).

**configured:** Must specify which MAC addresses are allowed for this port. Range is 1 (default) to 8 and addresses are not ageable. Addresses are saved across reboots.

**limited-continuous:** Also known as MAC Secure, or “limited” mode. The limited parameter sets a finite limit to the number of learned addresses allowed per port. (You can set the range from 1, the default, to a maximum of 64 MAC addresses which may be learned by each port.) All addresses are ageable, meaning they are automatically removed from the authorized address list for that port after a certain amount of time. Limited mode and the address limit are saved across reboots, but addresses which had been learned are lost during the reboot process. Addresses learned in the limited mode are normal addresses learned from the network until the limit is reached, but they are not configurable. (You cannot enter or remove these addresses manually if you are using learn-mode with the limited-continuous option.)

—Continued—
Syntax: port-security (Continued)

Addresses learned this way appear in the switch and port address tables and age out according to the MAC Age Interval in the System Information configuration screen of the Menu interface or the show system information listing. You can set the MAC age out time using the CLI, SNMP, Web, or menu interfaces. For more on the mac-age-time command, refer to the chapter titled “Interface Access and System Information” in the Basic Operation Guide for your switch. To set the learn-mode to limited use this command syntax:

```
port-security <port-list> learn-mode limited address-limit < 1..64> action < none | send-alarm | send-disable >
```

The default address-limit is 1 but may be set for each port to learn up to 64 addresses. The default action is none. To see the list of learned addresses for a port use the command:

```
show mac < port-list >
```

When learn-mode is set to static, configured, or limited-continuous, the address-limit parameter specifies how many authorized devices (MAC addresses) to allow. Range: 1 (the default) to 8 for static and configured modes. For learn-mode with the limited-continuous option, the range is 1-64 addresses.

—Continued—
Configuring and Monitoring Port Security
Port Security

Syntax: port-security (Continued)

mac-address [<mac-addr>] [<mac-addr>] ... [<mac-addr>]

Available for learn-mode with the, static, configured, or limited-continuous option. Allows up to eight authorized devices (MAC addresses) per port, depending on the value specified in the address-limit parameter. The mac-address limited-continuous mode allows up to 64 authorized MAC addresses per port.

If you use mac-address with static, but enter fewer devices than you specified in the address-limit field, the port accepts not only your specified devices, but also as many other devices as it takes to reach the device limit. For example, if you specify four devices, but enter only two MAC addresses, the port will accept the first two non-specified devices it detects, along with the two specifically authorized devices. Learned addresses that become authorized do not age-out. See also “Retention of Static Addresses” on page 13-17.

action < none | send-alarm | send-disable >

Specifies whether an SNMP trap is sent to a network management station when Learn Mode is set to static and the port detects an unauthorized device, or when Learn Mode is set to continuous and there is an address change on a port.

none: Prevents an SNMP trap from being sent. none is the default value.

send-alarm: Sends an intrusion alarm. Causes the switch to send an SNMP trap to a network management station.

send-disable: Sends alarm and disables the port. Available only in the static, port-access, configured, or limited learn modes. Causes the switch to send an SNMP trap to a network management station and disable the port. If you subsequently re-enable the port without clearing the port's intrusion flag, the port blocks further intruders, but the switch will not disable the port again until you reset the intrusion flag. See the Note on 13-37.

For information on configuring the switch for SNMP management, refer to the Management and Configuration Guide for your switch.

—Continued—
Configuring and Monitoring Port Security
Port Security

Syntax:  port-security (Continued)

    clear-intrusion-flag

    Clears the intrusion flag for a specific port. (See “Reading Intrusion Alerts and Resetting Alert Flags” on page 13-35.)

    no port-security <port-list> mac-address <mac-addr> [<mac-addr>]

    Removes the specified learned MAC address(es) from the specified port.

Retention of Static Addresses

Static MAC addresses do not age-out. MAC addresses learned by using learn-mode continuous or learn-mode limited-continuous age out according to the currently configured MAC age time. (For information on the mac-age-time command, refer to the chapter titled “Interface Access and System Information” in the Basic Operation Guide for your switch.

Learned Addresses. In the following two cases, a port in Static learn mode retains a learned MAC address even if you later reboot the switch or disable port security for that port:

- The port learns a MAC address after you configure the port for Static learn mode in both the startup-config file and the running-config file (by executing the write memory command).
- The port learns a MAC address after you configure the port for Static learn mode in only the running-config file and, after the address is learned, you execute write memory to configure the startup-config file to match the running-config file.

To remove an address learned using either of the preceding methods, do one of the following:

- Delete the address by using no port-security < port-number > mac-address < mac-addr >.
- Download a configuration file that does not include the unwanted MAC address assignment.
- Reset the switch to its factory-default configuration.
Assigned/Authorized Addresses. If you manually assign a MAC address (using `port-security <port-number> address-list <mac-addr>`) and then execute `write memory`, the assigned MAC address remains in memory until you do one of the following:

- Delete it by using `no port-security <port-number> mac-address <mac-addr>`.
- Download a configuration file that does not include the unwanted MAC address assignment.
- Reset the switch to its factory-default configuration.

Specifying Authorized Devices and Intrusion Responses. This example configures port A1 to automatically accept the first device (MAC address) it detects as the only authorized device for that port. (The default device limit is 1.) It also configures the port to send an alarm to a network management station and disable itself if an intruder is detected on the port.

```
HP Switch(config)# port-security a1 learn-mode static action send-disable
```

The next example does the same as the preceding example, except that it specifies a MAC address of 0c0090-123456 as the authorized device instead of allowing the port to automatically assign the first device it detects as an authorized device.

```
HP Switch(config)# port-security a1 learn-mode static mac-address 0c0090-123456 action send-disable
```

This example configures port A5 to:

- Allow two MAC addresses, 00c100-7fec00 and 0060b0-889e00, as the authorized devices.
- Send an alarm to a management station if an intruder is detected on the port, but allow the intruder access to the network.

```
HP Switch(config)# port-security a5 learn-mode static address-limit 2 mac-address 00c100-7fec00 0060b0-889e00 action send-alarm
```

If you manually configure authorized devices (MAC addresses) and/or an alarm action on a port, those settings remain unless you either manually change them or the switch is reset to its factory-default configuration. You can “turn off” authorized devices on a port by configuring the port to continuous Learn Mode, but subsequently reconfiguring the port to static Learn Mode restores those authorized devices.
Adding an Authorized Device to a Port. To simply add a device (MAC address) to a port’s existing Authorized Addresses list, enter the port number with the `mac-address` parameter and the device’s MAC address. This assumes that Learn Mode is set to static and the Authorized Addresses list is not full (as determined by the current Address Limit value). For example, suppose port A1 allows two authorized devices, but has only one device in its Authorized Address list:

```
HP Switch(config)# port-security a1 mac-address 0c0090-456456
```

After executing the above command, the security configuration for port A1 would be:

```
Port Security
Port : 1
Action [None] : None
Eavesdrop Prevention [Enabled] : Enabled
Authorized Addresses
----------------------
0c0090-123456
```

With the above configuration for port A1, the following command adds the 0c0090-456456 MAC address as the second authorized address.

```
HP Switch(config)# port-security a1 mac-address 0c0090-456456
```

After executing the above command, the security configuration for port A1 would be:

```
Port Security
Port : 1
Action [None] : None
Eavesdrop Prevention [Enabled] : Enabled
Authorized Addresses
----------------------
0c0090-123456
0c0090-456456
```

Although the Address Limit is set to 2, only one device has been authorized for this port. In this case you can add another without having to also increase the Address Limit.
(The message **Inconsistent value** appears if the new MAC address exceeds the current Address Limit or specifies a device that is already on the list. Note that if you change a port from static to continuous learn mode, the port retains in memory any authorized addresses it had while in static mode. If you subsequently attempt to convert the port back to static mode with the same authorized address(es), the **Inconsistent value** message appears because the port already has the address(es) in its “Authorized” list.)

If you are adding a device (MAC address) to a port on which the Authorized Addresses list is already full (as controlled by the port’s current Address Limit setting), then you must increase the Address Limit in order to add the device, even if you want to replace one device with another. Using the CLI, you can simultaneously increase the limit and add the MAC address with a single command. For example, suppose port A1 allows one authorized device and already has a device listed:

![Figure 13-8. Example of Port Security on Port A1 with an Address Limit of “1”](image)

To add a second authorized device to port A1, execute a **port-security** command for port A1 that raises the address limit to 2 and specifies the additional device’s MAC address. For example:

```
HP Switch(config)# port-security a1 mac-address 0c0090-456456 address-limit 2
```
Removing a Device From the “Authorized” List for a Port. This command option removes unwanted devices (MAC addresses) from the Authorized Addresses list. (An Authorized Address list is available for each port for which Learn Mode is currently set to “Static”. Refer to the command syntax listing under “Configuring Port Security” on page 13-12.)

**Caution**

When learn mode is set to static, the Address Limit (address-limit) parameter controls how many devices are allowed in the Authorized Addresses (mac-address) for a given port. If you remove a MAC address from the Authorized Addresses list without also reducing the Address Limit by 1, the port may subsequently detect and accept as authorized a MAC address that you do not intend to include in your Authorized Address list. Thus, if you use the CLI to remove a device that is no longer authorized, it is recommended that you first reduce the Address Limit (address-limit) integer by 1, as shown below. This prevents the possibility of the same device or another unauthorized device on the network from automatically being accepted as “authorized” for that port.

To remove a device (MAC address) from the “Authorized” list and when the current number of devices equals the Address Limit value, you should first reduce the Address Limit value by 1, then remove the unwanted device.

**Note**

You can reduce the address limit below the number of currently authorized addresses on a port. This enables you to subsequently remove a device from the “Authorized” list without opening the possibility for an unwanted device to automatically become authorized.

For example, suppose port A1 is configured as shown below and you want to remove 0c0090-123456 from the Authorized Address list:

```
HP Switch(config)# show port-security 1
Port Security
Port : 1
Action [None] : None
Eavesdrop Prevention [Enabled] : Enabled
Authorized Addresses
------------------------
0c0090-123456
0c0090-456456
```

**Figure 13-9. Example of Two Authorized Addresses on Port A1**
Configuring and Monitoring Port Security
Clear MAC Address Table

The following command serves this purpose by removing 0c0090-123456 and reducing the Address Limit to 1:

HP Switch(config)# port-security a1 address-limit 1
HP Switch(config)# no port-security a1 mac-address 0c0090-123456

The above command sequence results in the following configuration for port A1:

```
HP Switch(config)# show port-security 1
Port Security
  Port : 1
  Learn Mode [Continuous] : Static
  Address Limit [1] : 1
  Action [None] : None
  Eavesdrop Prevention [Enabled] : Enabled

  Authorized Addresses
  ---------------------
  0c0090-456456
```

Figure 13-10. Example of Port A1 After Removing One MAC Address

---

Clear MAC Address Table

The following options allow learned MAC addresses to be removed from the MAC address table as follows:

- Remove all MAC addresses.
- Remove all MAC address on a specified VLAN
- Remove all MAC addresses on a port
- Remove a specific MAC address on a specific VLAN

This functionality is also supported by SNMP.
Configuring Clearing of Learned MAC Addresses

Use the following commands to clear learned MAC addresses from a port or list of ports, a specific VLAN, or to clear a specific MAC address from a VLAN.

**Syntax:** clear mac-address port <port-list>

*Removes MAC addresses that were learned on the specified port or ports in* `<port-list>`. *Use all to remove all MAC addresses in the MAC address table.*

```
HP Switch(config)# clear mac-address port 4-7
```

Figure 13-11. Example of clearing a learned MAC Addresses from multiple ports.

**Syntax:** clear mac-address vlan <vid>

*Removes all MAC addresses that were learned on the specified VLAN.*

```
HP Switch(config)# clear mac-address vlan 2
```

Figure 13-12. Example of clearing a learned MAC Address from a VLAN

**Syntax:** clear mac-address vlan <vid> mac <mac-addr>

*Removes the specified MAC address from the specified VLAN*

```
HP Switch(config)# clear mac-address vlan 2 mac 0001e6-b197a8
```

Figure 13-13. Example of clearing a specific MAC Address from a specific VLAN

To view the results from clearing a MAC address, use the `show mac-address` command with the appropriate option.
MAC Lockdown

MAC Lockdown, also known as “static addressing,” is the permanent assignment of a given MAC address (and VLAN, or Virtual Local Area Network) to a specific port on the switch. MAC Lockdown is used to prevent station movement and MAC address hijacking. It also controls address learning on the switch.

Locking down a MAC address on a port and a specific VLAN only restricts the MAC address on that VLAN. The client device with that MAC address is allowed to access other VLANs on the same port or through other ports.

Note

Port security and MAC Lockdown are mutually exclusive on a given port. You can either use port security or MAC Lockdown, but never both at the same time on the same port.

Syntax: [no] static-mac <mac-addr> vlan <vid> interface <port-number>

Figure 13-14. Example showing a MAC Address cleared from the MAC Address Table.
You will need to enter a separate command for each MAC/VLAN pair you wish to lock down. If you do not specify a VLAN ID (VID) the switch inserts a VID of “1”.

**How It Works.** When a device’s MAC address is locked down to a port (typically in a pair with a VLAN) all information sent to that MAC address must go through the locked-down port. If the device is moved to another port it cannot receive data. Traffic to the designated MAC address goes only to the allowed port, whether the device is connected to it or not.

MAC Lockdown is useful for preventing an intruder from “hijacking” a MAC address from a known user in order to steal data. Without MAC Lockdown, this will cause the switch to learn the address on the malicious user’s port, allowing the intruder to steal the traffic meant for the legitimate user.

MAC Lockdown ensures that traffic intended for a specific MAC address can only go through the one port which is supposed to be connected to that MAC address. It does not prevent intruders from transmitting packets with the locked MAC address, but it does prevent responses to those packets from going anywhere other than the locked-down port. Thus TCP connections cannot be established. Traffic sent to the locked address cannot be hijacked and directed out the port of the intruder.

If the device (computer, PDA, wireless device) is moved to a different port on the switch (by reconnecting the Ethernet cable or by moving the device to an area using a wireless access point connected to a different port on that same switch), the port will detect that the MAC Address is not on the appropriate port and will continue to send traffic out the port to which the address was locked.

Once a MAC address is configured for one port, you cannot perform port security using the same MAC address on any other port on that same switch.

You cannot lock down a single MAC Address/VLAN pair to more than one port; however you can lock down multiple different MAC Addresses to a single port on the same switch.

Stations can move from the port to which their MAC address is locked to other parts of the network. They can send, but will not receive data if that data must go through the locked down switch. Please note that if the device moves to a distant part of the network where data sent to its MAC address never goes through the locked down switch, it may be possible for the device to have full two-way communication. For full and complete lockdown network-wide all switches must be configured appropriately.
Other Useful Information. Once you lock down a MAC address/VLAN pair on one port that pair cannot be locked down on a different port.

You cannot perform MAC Lockdown and 802.1X authentication on the same port or on the same MAC address. MAC Lockdown and 802.1X authentication are mutually exclusive.

Lockdown is permitted on static trunks (manually configured link aggregations).

Differences Between MAC Lockdown and Port Security

Because port-security relies upon MAC addresses, it is often confused with the MAC Lockdown feature. However, MAC Lockdown is a completely different feature and is implemented on a different architecture level.

Port security maintains a list of allowed MAC addresses on a per-port basis. An address can exist on multiple ports of a switch. Port security deals with MAC addresses only while MAC Lockdown specifies both a MAC address and a VLAN for lockdown.

MAC Lockdown, on the other hand, is not a “list.” It is a global parameter on the switch that takes precedence over any other security mechanism. The MAC Address will only be allowed to communicate using one specific port on the switch.

MAC Lockdown is a good replacement for port security to create tighter control over MAC addresses and which ports they are allowed to use (only one port per MAC Address on the same switch in the case of MAC Lockdown). (You can still use the port for other MAC addresses, but you cannot use the locked down MAC address on other ports.)

Using only port security the MAC Address could still be used on another port on the same switch. MAC Lockdown, on the other hand, is a clear one-to-one relationship between the MAC Address and the port. Once a MAC address has been locked down to a port it cannot be used on another port on the same switch.

The switch does not allow MAC Lockdown and port security on the same port.
MAC Lockdown Operating Notes

**Limits.** There is a limit of 500 MAC Lockdowns that you can safely code per switch. To truly lock down a MAC address it would be necessary to use the MAC Lockdown command for every MAC Address and VLAN ID on every switch. In reality few network administrators will go to this length, but it is important to note that just because you have locked down the MAC address and VID for a single switch, the device (or a hacker “spoofing” the MAC address for the device) may still be able to use another switch which hasn’t been locked down.

**Event Log Messages.** If someone using a locked down MAC address is attempting to communicate using the wrong port the “move attempt” generates messages in the log file like this:

Move attempt (lockdown) logging:

W 10/30/03 21:33:43 maclock: module A: Move 0001e6-1f96c0 to A15 denied
W 10/30/03 21:33:48 maclock: module A: Move 0001e6-1f96c0 to A15 denied
W 10/30/03 21:33:48 maclock: module A: Ceasing move-denied logs for 5m

These messages in the log file can be useful for troubleshooting problems. If you are trying to connect a device which has been locked down to the wrong port, it will not work but it will generate error messages like this to help you determine the problem.

**Limiting the Frequency of Log Messages.** The first move attempt (or intrusion) is logged as you see in the example above. Subsequent move attempts send a message to the log file also, but message throttling is imposed on the logging on a per-module basis. What this means is that the logging system checks again after the first 5 minutes to see if another attempt has been made to move to the wrong port. If this is the case the log file registers the most recent attempt and then checks again after one hour. If there are no further attempts in that period then it will continue to check every 5 minutes. If another attempt was made during the one hour period then the log resets itself to check once a day. The purpose of rate-limiting the log messaging is to prevent the log file from becoming too full. You can also configure the switch to send the same messages to a Syslog server. Refer to “Debug and Syslog Messaging Operation” in appendix C of the *Management and Configuration Guide* for your switch.
Deploying MAC Lockdown

When you deploy MAC Lockdown you need to consider how you use it within your network topology to ensure security. In some cases where you are using techniques such as “meshing” or Spanning Tree Protocol (STP) to speed up network performance by providing multiple paths for devices, using MAC Lockdown either will not work or else it defeats the purpose of having multiple data paths.

The purpose of using MAC Lockdown is to prevent a malicious user from “hijacking” an approved MAC address so they can steal data traffic being sent to that address.

As we have seen, MAC Lockdown can help prevent this type of hijacking by making sure that all traffic to a specific MAC address goes only to the proper port on a switch which is supposed to be connected to the real device bearing that MAC address.

However, you can run into trouble if you incorrectly try to deploy MAC Lockdown in a network that uses multiple path technology, like Spanning Tree or “mesh networks.”

Let’s examine a good use of MAC Lockdown within a network to ensure security first.
Basic MAC Lockdown Deployment. In the Model Network Topology shown above, the switches that are connected to the edge of the network each have one and only one connection to the core network. This means each switch has only one path by which data can travel to Server A. You can use MAC Lockdown to specify that all traffic intended for Server A's MAC Address must go through the one port on the edge switches. That way, users on the edge can still use other network resources, but they cannot “spoof” Server A and hijack data traffic which is intended for that server alone.
The key points for this Model Topology are:

- The Core Network is separated from the edge by the use of switches which have been “locked down” for security.
- All switches connected to the edge (outside users) each have only one port they can use to connect to the Core Network and then to Server A.
- Each switch has been configured with MAC Lockdown so that the MAC Address for Server A has been locked down to one port per switch that can connect to the Core and Server A.

Using this setup Server A can be moved around within the core network, and yet MAC Lockdown will still prevent a user at the edge from hijacking its address and stealing data.

Please note that in this scenario a user with bad intentions at the edge can still “spoof” the address for Server A and send out data packets that look as though they came from Server A. The good news is that because MAC Lockdown has been used on the switches on the edge, any traffic that is sent back to Server A will be sent to the proper MAC Address because MAC Lockdown has been used. The switches at the edge will not send Server A’s data packets anywhere but the port connected to Server A. (Data would not be allowed to go beyond the edge switches.)

**Caution**

Using MAC Lockdown still does not protect against a hijacker within the core! In order to protect against someone spoofing the MAC Address for Server A inside the Core Network, you would have to lock down each and every switch inside the Core Network as well, not just on the edge.

**Problems Using MAC Lockdown in Networks With Multiple Paths.** Now let’s take a look at a network topology in which the use of MAC Lockdown presents a problem. In the next figure, Switch 1 (on the bottom-left) is located at the edge of the network where there is a mixed audience that might contain hackers or other malicious users. Switch 1 has two paths it could use to connect to Server A. If you try to use MAC Lockdown here to make sure that all data to Server A is “locked down” to one path, connectivity problems would be the result since both paths need to be usable in case one of them fails.
The resultant connectivity issues would prevent you from locking down Server A to Switch 1. And when you remove the MAC Lockdown from Switch 1 (to prevent broadcast storms or other connectivity issues), you then open the network to security problems. The use of MAC Lockdown as shown in the above figure would defeat the purpose of using MSTP or having an alternate path.

Technologies such as MSTP or “meshing” are primarily intended for an internal campus network environment in which all users are trusted. MSTP and “meshing” do not work well with MAC Lockdown.

If you deploy MAC Lockdown as shown in the Model Topology in figure 13-15 (page 13-29), you should have no problems with either security or connectivity.
MAC Lockout

MAC Lockout involves configuring a MAC address on all ports and VLANs for a switch so that any traffic to or from the “locked-out” MAC address will be dropped. This means that all data packets addressed to or from the given address are stopped by the switch. MAC Lockout is implemented on a per switch assignment.

You can think of MAC Lockout as a simple blacklist. The MAC address is locked out on the switch and on all VLANs. No data goes out or in from the blacklisted MAC address to a switch using MAC Lockout.

To fully lock out a MAC address from the network it would be necessary to use the MAC Lockout command on all switches.

To use MAC Lockout you must first know the MAC Address you wish to block.

Syntax: [no] lockout-mac < mac-address >

How It Works. Let’s say a customer knows there are unauthorized wireless clients who should not have access to the network. The network administrator “locks out” the MAC addresses for the wireless clients by using the MAC Lockout command (lockout-mac <mac-address>). When the wireless clients then attempt to use the network, the switch recognizes the intruding MAC addresses and prevents them from sending or receiving data on that network.

If a particular MAC address can be identified as unwanted on the switch then that MAC Address can be disallowed on all ports on that switch with a single command. You don’t have to configure every single port—just perform the command on the switch and it is effective for all ports.
MAC Lockout overrides MAC Lockdown, port security, and 802.1X authentication.

You cannot use MAC Lockout to lock:

- Broadcast or Multicast Addresses (Switches do not learn these)
- Switch Agents (The switch’s own MAC Address)

A MAC address can exist on many different VLANs, so a lockout MAC address must be added to the MAC table as a drop. As this can quickly fill the MAC table, restrictions are placed on the number of lockout MAC addresses based on the number of VLANs configured.

<table>
<thead>
<tr>
<th>VLANs Configured</th>
<th>Number of MAC Lockout Addresses</th>
<th>Total Number of MAC Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-8</td>
<td>200</td>
<td>1,600</td>
</tr>
<tr>
<td>9-16</td>
<td>100</td>
<td>1,600</td>
</tr>
<tr>
<td>17-256</td>
<td>64</td>
<td>16,384</td>
</tr>
<tr>
<td>257-1024</td>
<td>16</td>
<td>16,384</td>
</tr>
<tr>
<td>1025-2048</td>
<td>8</td>
<td>16,384</td>
</tr>
</tbody>
</table>

There are limits for the number of VLANs, Multicast Filters, and Lockout MACs that can be configured concurrently as all use MAC table entries. The limits are shown below:

<table>
<thead>
<tr>
<th># VLANs</th>
<th># Multicast Filters</th>
<th># Lockout MACs</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= 1024</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>1025-2048</td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>
If someone using a locked out MAC address tries to send data through the switch a message is generated in the log file:

Lockout logging format:

W 10/30/03 21:35:15 maclock: module A: 0001e6-1f96c0
   detected on port A15
W 10/30/03 21:35:18 maclock: module A: 0001e6-1f96c0
   detected on port A15
W 10/30/03 21:35:18 maclock: module A: Ceasing lock-out
   logs for 5m

As with MAC Lockdown a rate limiting algorithm is used on the log file so that it does not become overclogged with error messages. (Refer to “Limiting the Frequency of Log Messages” on page 13-27.)

---

**Port Security and MAC Lockout**

MAC Lockout is independent of port-security and in fact will override it. MAC Lockout is preferable to port-security to stop access from known devices because it can be configured for all ports on the switch with one command.

It is possible to use MAC Lockout in conjunction with port-security. You can use MAC Lockout to lock out a single address—deny access to a specific device—but still allow the switch some flexibility in learning other MAC Addresses. Be careful if you use both together, however:

- If a MAC Address is locked out and appears in a static learn table in port-security, the apparently “authorized” address will still be locked out anyway.
- MAC entry configurations set by port security will be kept even if MAC Lockout is configured and the original port security settings will be honored once the Lockout is removed.
- A port security static address is permitted to be a lockout address. In that case (MAC Lockout), the address will be locked out (SA/DA drop) even though it’s an “authorized” address from the perspective of port security.
- When MAC Lockout entries are deleted, port security will then re-learn the address as needed later on.
Reading Intrusion Alerts and Resetting Alert Flags

Notice of Security Violations

When the switch detects an intrusion on a port, it sets an “alert flag” for that port and makes the intrusion information available as described below. While the switch can detect additional intrusions for the same port, it does not list the next chronological intrusion for that port in the Intrusion Log until the alert flag for that port has been reset.

When a security violation occurs on a port configured for Port Security, the switch responds in the following ways to notify you:

- The switch sets an alert flag for that port. This flag remains set until:
  - You use either the CLI, menu interface, or WebAgent to reset the flag.
  - The switch is reset to its factory default configuration.

- The switch enables notification of the intrusion through the following means:
  - In the CLI:
    - The `show port-security intrusion-log` command displays the Intrusion Log
    - The `log` command displays the Event Log
  - In the menu interface:
    - The Port Status screen includes a per-port intrusion alert
    - The Event Log includes per-port entries for security violations
  - In the WebAgent:
    - The Alert Log includes entries for per-port security violations
    - The Intrusion Log lists per-port security violation entries
  - In network management applications such as PCM+ via an SNMP trap sent to a network management station
How the Intrusion Log Operates

When the switch detects an intrusion attempt on a port, it enters a record of this event in the Intrusion Log. No further intrusion attempts on that port will appear in the Log until you acknowledge the earlier intrusion event by resetting the alert flag.

The Intrusion Log lists the 20 most recently detected security violation attempts, regardless of whether the alert flags for these attempts have been reset. This gives you a history of past intrusion attempts. Thus, for example, if there is an intrusion alert for port A1 and the Intrusion Log shows two or more entries for port 1, only the most recent entry has not been acknowledged (by resetting the alert flag). The other entries give you a history of past intrusions detected on port A1.

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC Address</th>
<th>Date / Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>080009-e93d4f</td>
<td>03/07/11 21:09:34</td>
</tr>
<tr>
<td>1</td>
<td>080009-e93d4f</td>
<td>03/07/11 10:18:43</td>
</tr>
</tbody>
</table>

Figure 13-18. Example of Multiple Intrusion Log Entries for the Same Port

The log shows the most recent intrusion at the top of the listing. You cannot delete Intrusion Log entries (unless you reset the switch to its factory-default configuration). Instead, if the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing and the newest entry appears at the top of the listing.

Keeping the Intrusion Log Current by Resetting Alert Flags

When a violation occurs on a port, an alert flag is set for that port and the violation is entered in the Intrusion Log. The switch can detect and handle subsequent intrusions on that port, but will not log another intrusion on the port until you reset the alert flag for either all ports or for the individual port.
Confuring and Monitoring Port Security

Reading Intrusion Alerts and Resetting Alert Flags

On a given port, if the intrusion action is to send an SNMP trap and then disable the port (send-disable), and an intruder is detected on the port, then the switch sends an SNMP trap, sets the port’s alert flag, and disables the port. If you re-enable the port without resetting the port’s alert flag, then the port operates as follows:

- The port comes up and will block traffic from unauthorized devices it detects.
- If the port detects another intruder, it will send another SNMP trap, but will not become disabled again unless you first reset the port’s intrusion flag.

This operation enables the port to continue passing traffic for authorized devices while you take the time to locate and eliminate the intruder. Otherwise, the presence of an intruder could cause the switch to repeatedly disable the port.

Menu: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags

The menu interface indicates per-port intrusions in the Port Status screen, and provides details and the reset function in the Intrusion Log screen.

1. From the Main Menu select:
   1. Status and Counters
   4. Port Status

   ![Figure 13-19. Example of Port Status Screen with Intrusion Alert on Port A3](image)

   The Intrusion Alert column shows “Yes” for any port on which a security violation has been detected.

   **Actions:**
   - **[i]** Intrusion log
   - **Help**

   Use up/down arrow keys to scroll to other entries, left/right arrow keys to change action selection, and <Enter> to execute action.

   **Figure 13-19. Example of Port Status Screen with Intrusion Alert on Port A3**

   2. Type [i] (Intrusion log) to display the Intrusion Log.
Figure 13-20. Example of the Intrusion Log Display

The example in Figure 7-11 shows two intrusions for port A3 and one intrusion for port A1. In this case, only the most recent intrusion at port A3 has not been acknowledged (reset). This is indicated by the following:

- Because the Port Status screen (figure 13-19 on page 13-37) does not indicate an intrusion for port A1, the alert flag for the intrusion on port A1 has already been reset.
- Since the switch can show only one uncleared intrusion per port, the alert flag for the older intrusion for port A3 in this example has also been previously reset.

(The intrusion log holds up to 20 intrusion records and deletes an intrusion record only when the log becomes full and a new intrusion is subsequently detected.)

Note also that the "prior to" text in the record for the earliest intrusion means that a switch reset occurred at the indicated time and that the intrusion occurred prior to the reset.

3. To acknowledge the most recent intrusion entry on port A3 and enable the switch to enter a subsequently detected intrusion on this port, type [R] (for Reset alert flags). (Note that if there are unacknowledged intrusions on two or more ports, this step resets the alert flags for all such ports.)

If you then re-display the port status screen, you will see that the Intrusion Alert entry for port A3 has changed to "No". That is, your evidence that the Intrusion Alert flag has been acknowledged (reset) is that the Intrusion Alert column in the port status display no longer shows "Yes" for the port on which the intrusion occurred (port A3 in this example). (Because the Intrusion Log provides a history of the last 20 intrusions detected by the switch, resetting the alert flags does not change its content. Thus, displaying the Intrusion Log again will result in the same display as in figure 13-20, above.)
CLI: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags

The following commands display port status, including whether there are intrusion alerts for any port(s), list the last 20 intrusions, and either reset the alert flag on all ports or for a specific port for which an intrusion was detected. (The record of the intrusion remains in the log. For more information, refer to “Operating Notes for Port Security” on page 13-42.)

**Syntax:**

- `show interfaces brief`
  
  *List intrusion alert status (and other port status information).*

- `show port-security intrusion-log`
  
  *List intrusion log content.*

- `clear intrusion-flags`
  
  *Clear intrusion flags on all ports.*

- `port-security [e] < port-number > clear-intrusion-flag`
  
  *Clear the intrusion flag on one or more specific ports.*

In the following example, executing `show interfaces brief` lists the switch’s port status, which indicates an intrusion alert on port 1.

```
HP Switch(config)# show int brief

Status and Counters - Port Status

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Intrusion</th>
<th>Enabled</th>
<th>Status</th>
<th>Mode</th>
<th>MDI</th>
<th>Flow</th>
<th>Bcast</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>100/1000T</td>
<td>Yes</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>MDI</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Figure 13-21. Example of an Unacknowledged Intrusion Alert in a Port Status Display

If you wanted to see the details of the intrusion, you would then enter the `show port-security intrusion-log` command. For example:
The above example shows three intrusions for port 1. Since the switch can show only one uncleared intrusion per port, the older two intrusions in this example have already been cleared by earlier use of the `clear intrusion-log` or the `port-security < port-list > clear-intrusion-flag` command. (The intrusion log holds up to 20 intrusion records, and deletes intrusion records only when the log becomes full and new intrusions are subsequently added.) The “prior to” text in the record for the third intrusion means that a switch reset occurred at the indicated time and that the intrusion occurred prior to the reset.

To clear the intrusion from port 1 and enable the switch to enter any subsequent intrusion for port 1 in the Intrusion Log, execute the `port-security < port-list > clear-intrusion-flag` command. If you then re-display the port status screen, you will see that the Intrusion Alert entry for port 1 has changed to “No”. (Executing `show port-security intrusion-log` again will result in the same display as above, and does not include the Intrusion Alert status.)

```bash
HP Switch(config)# port-security 1 clear-intrusion-flag
HP Switch(config)# show interfaces brief
```
Configuring and Monitoring Port Security
Reading Intrusion Alerts and Resetting Alert Flags

Figure 13-23. Example of Port Status Screen After Alert Flags Reset

For more on clearing intrusions, see “Note on Send-Disable Operation” on page 13-37.

Using the Event Log To Find Intrusion Alerts

The Event Log lists port security intrusions as:


where “W” is the severity level of the log entry and FFI is the system module that generated the entry. For further information, display the Intrusion Log, as shown below.

From the CLI. Type the log command from the Manager or Configuration level.

Syntax: log < search-text >

For < search-text >, you can use ffi, security, or violation. For example:
From the Menu Interface: In the Main Menu, click on 4. Event Log and use Next page and Prev page to review the Event Log contents.

For More Event Log Information. See “Using the Event Log To Identify Problem Sources” in the “Troubleshooting” chapter of the Management and Configuration Guide for your switch.

Operating Notes for Port Security

Identifying the IP Address of an Intruder. The Intrusion Log lists detected intruders by MAC address. If you are using PCM+ to manage your network, you can use the device properties page to link MAC addresses to their corresponding IP addresses.

Proxy Web Servers. If you are using the WebAgent through a switch port configured for Static port security, and your browser access is through a proxy web server, then it is necessary to do the following:

- Enter your PC or workstation MAC address in the port’s Authorized Addresses list.
- Enter your PC or workstation’s IP address in the switch’s IP Authorized Managers list. See “Using Authorized IP Managers” in the Management and Configuration Guide for your switch.)
Without both of the above configured, the switch detects only the proxy server’s MAC address, and not your PC or workstation MAC address, and interprets your connection as unauthorized.

“Prior To” Entries in the Intrusion Log. If you reset the switch (using the Reset button, Device Reset, or Reboot Switch), the Intrusion Log will list the time of all currently logged intrusions as “prior to” the time of the reset.

Alert Flag Status for Entries Forced Off of the Intrusion Log. If the Intrusion Log is full of entries for which the alert flags have not been reset, a new intrusion will cause the oldest entry to drop off the list, but will not change the alert flag status for the port referenced in the dropped entry. This means that, even if an entry is forced off of the Intrusion Log, no new intrusions can be logged on the port referenced in that entry until you reset the alert flags.

LACP Not Available on Ports Configured for Port Security. To maintain security, LACP is not allowed on ports configured for port security. If you configure port security on a port on which LACP (active or passive) is configured, the switch removes the LACP configuration, displays a notice that LACP is disabled on the port(s), and enables port security on that port. For example:

HP Switch(config)# port-security e a17 learn-mode static address-limit 2
LACP has been disabled on secured port(s).
HP Switch(config)#

The switch will not allow you to configure LACP on a port on which port security is enabled. For example:

HP Switch(config)# int e a17 lacp passive
Error configuring port A17: LACP and port security cannot be run together.
HP Switch(config)#

To restore LACP to the port, you must remove port security and re-enable LACP active or passive.
Using Authorized IP Managers

Overview

Authorized IP Manager Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>WebAgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listing (Showing) Authorized Managers</td>
<td>n/a</td>
<td>page 14-4</td>
<td>page 14-5</td>
<td>page 14-8</td>
</tr>
<tr>
<td>Configuring Authorized IP Managers</td>
<td>None</td>
<td>page 14-4</td>
<td>page 14-5</td>
<td>page 14-8</td>
</tr>
<tr>
<td>Building IP Masks</td>
<td>n/a</td>
<td>page 14-10</td>
<td>page 14-10</td>
<td>page 14-10</td>
</tr>
<tr>
<td>Operating and Troubleshooting Notes</td>
<td>n/a</td>
<td>page 14-13</td>
<td>page 14-13</td>
<td>page 14-13</td>
</tr>
</tbody>
</table>

The Authorized IP Managers feature uses IP addresses and masks to determine which stations (PCs or workstations) can access the switch through the network. This covers access through the following means:

- Telnet and other terminal emulation applications
- The WebAgent
- SSH
- SNMP versions 1, 2 and 3 (with a correct community name)
- TFTP

Also, when configured in the switch, the Authorized IP Managers feature takes precedence over local passwords, TACACS+, and RADIUS. This means that the IP address of a networked management device must be authorized before the switch will attempt to authenticate the device by invoking any other access security features. If the Authorized IP Managers feature disallows access to the device, then access is denied. Thus, with authorized IP managers configured, having the correct passwords is not sufficient for accessing the switch through the network unless the station attempting access is also included in the switch's Authorized IP Managers configuration.

You can use Authorized IP Managers along with other access security features to provide a more comprehensive security fabric than if you use only one or two security options.
Using Authorized IP Managers

Options

Note

When no Authorized IP manager rules are configured, the access method feature is disabled, that is, access is not denied.

Options

You can configure:

- Up to 100 authorized manager *addresses*, where each address applies to either a single management station or a group of stations
- Manager or Operator access privileges

Caution

Configuring Authorized IP Managers does not protect access to the switch through a modem or direct connection to the Console (RS-232) port. Also, if an unauthorized station "spoofs" an authorized IP address, it can gain management access to the switch even though a duplicate IP address condition exists. For these reasons, you should enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the username/password and other security features available in the switch, and preventing unauthorized access to data on your management stations.

Access Levels

For each authorized manager address, you can configure either of these access levels:

- **Manager**: Enables full access to all screens for viewing, configuration, and all other operations available.
- **Operator**: Allows read-only access. (This is the same access that is allowed by the switch’s operator-level password feature.)
Defining Authorized Management Stations

- **Authorizing Single Stations**: The table entry authorizes a single management station to have IP access to the switch. To use this method, just enter the IP address of an authorized management station in the Authorized Manager IP column, and leave the IP Mask set to 255.255.255.255. This is the easiest way to use the Authorized Managers feature. (For more on this topic, see “Configuring One Station Per Authorized Manager IP Entry” on page 14-10.)

- **Authorizing Multiple Stations**: The table entry uses the IP Mask to authorize access to the switch from a defined group of stations. This is useful if you want to easily authorize several stations to have access to the switch without having to type in an entry for every station. All stations in the group defined by the one Authorized Manager IP table entry and its associated IP mask will have the same access level—Manager or Operator. (For more on this topic, refer to “Configuring Multiple Stations Per Authorized Manager IP Entry” on page 14-10.)

To configure the switch for authorized manager access, enter the appropriate Authorized Manager IP value, specify an IP Mask, and select either Manager or Operator for the Access Level. The IP Mask determines how the Authorized Manager IP value is used to allow or deny access to the switch by a management station.

**Note**

If the management VLAN is configured, access can only be on that VLAN.

**Overview of IP Mask Operation**

The default IP Mask is 255.255.255.255 and allows switch access only to a station having an IP address that is identical to the Authorized Manager IP parameter value. (“255” in an octet of the mask means that only the exact value in the corresponding octet of the Authorized Manager IP parameter is allowed in the IP address of an authorized management station.) However, you can alter the mask and the Authorized Manager IP parameter to specify ranges of authorized IP addresses. For example, a mask of 255.255.255.0 and any value for the Authorized Manager IP parameter allows a range of 0 through 255 in the 4th octet of the authorized IP address, which enables a block of up to 254 IP addresses for IP management access (excluding 0 for the network and 255 for broadcasts). A mask of 255.255.255.252 uses the 4th octet of a given Autho-
Using Authorized IP Managers
Defining Authorized Management Stations

Authorized Manager IP address to authorize four IP addresses for management station access. The details on how to use IP masks are provided under “Building IP Masks” on page 14-10.

Note

The IP Mask is a method for recognizing whether a given IP address is authorized for management access to the switch. This mask serves a different purpose than IP subnet masks and is applied in a different manner.

Menu: Viewing and Configuring IP Authorized Managers

Only IPv4 is supported when using the menu to set the management access method.

From the console Main Menu, select:

2. Switch Configuration …
6. IP Authorized Managers

Figure 14-1. Example of How to Add an Authorized Manager Entry
Using Authorized IP Managers
Defining Authorized Management Stations

Figure 14-2. Example of Edit Menu for Authorized IP Managers

Editing or Deleting an Authorized Manager Entry. Go to the IP Managers List screen (figure 14-1), highlight the desired entry, and press [E] (for Edit) or [D] (for Delete).

CLI: Viewing and Configuring Authorized IP Managers

Authorized IP Managers Commands Used in This Section

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip authorized-managers</td>
<td>below</td>
</tr>
<tr>
<td>ip authorized-managers</td>
<td>14-7</td>
</tr>
<tr>
<td>(&lt;ip-address&gt;)</td>
<td>14-7</td>
</tr>
<tr>
<td>mask (&lt;mask-bits&gt;)</td>
<td>14-7</td>
</tr>
<tr>
<td>access (&lt;operator</td>
<td>manager&gt;)</td>
</tr>
<tr>
<td>access-method</td>
<td>14-6</td>
</tr>
</tbody>
</table>

Listing the Switch’s Current Authorized IP Manager(s)

Use the show ip authorized-managers command to list IP stations authorized to access the switch. For example:
Using Authorized IP Managers
Defining Authorized Management Stations

Figure 14-3. Example of show authorized-managers Command with Access Method Configured

Configuring IP Authorized Managers for the Switch

See the IPv6 Configuration Guide for information about Authorized IP manager configuration with IPv6 addresses.

Syntax:

[no] ip authorized-managers <ip-address> <ip-mask> access [manager | operator]
access-method [all | ssh | telnet | web | snmp | tftp]
[no] ipv6 authorized-managers <ip-address> <ip-mask> access [manager | operator]
access-method [all | ssh | telnet | web | snmp | tftp]

Configures one or more authorized IP addresses.

access [manager | operator]

Configures the privilege level for <ip-address>. Applies only to access through telnet, SSH, SNMPv1, SNMPv2c, and SNMPv3.

Default: manager

access-method [all | ssh | telnet | web | snmp | tftp]

Configures access levels by access method and IP address. Each management method can have its own set of authorized managers.

Default: all

Figure 14-4. Example of Configuring IP Authorized Manager Access Method SSH

HP Switch(config)# show ip authorized-manager
IPV4 Authorized Managers
------------------------
Address : 10.10.10.10
Mask    : 255.255.255.255
Access  : Manager
Access Method : ssh

HP Switch(config)# ip authorized-managers 10.10.10.2 255.255.255.255 manager
access-method ssh
To Authorize Manager Access. This command authorizes manager-level access for any station with an IP address of 10.28.227.0 through 10.28.227.255:

```
HP Switch(config)# ip authorized-managers 10.28.227.101 255.255.255.0 access manager
```

Similarly, the next command authorizes manager-level access for any station having an IP address of 10.28.227.101 through 103:

```
HP Switch(config)# ip authorized-managers 10.28.227.101 255.255.255.252 access manager
```

If you omit the `<mask bits>` when adding a new authorized manager, the switch automatically uses `255.255.255.255`. If you do not specify either Manager or Operator access, the switch assigns the Manager access.

To Edit an Existing Manager Access Entry. To change the mask or access level for an existing entry, use the entry's IP address and enter the new value(s). (Notice that any parameters not included in the command will be set to their default.):

```
HP Switch(config)# ip authorized-managers 10.28.227.101 255.255.255.0 access operator
```

The above command replaces the existing mask and access level for IP address 10.28.227.101 with `255.255.255.0` and `operator`.

The following command replaces the existing mask and access level for IP address 10.28.227.101 with `255.255.255.255` and `manager` (the defaults) because the command does not specify either of these parameters.

```
HP Switch(config)# ip authorized-managers 10.28.227.101
```

To Delete an Authorized Manager Entry. This command uses the IP address of the authorized manager you want to delete:

```
HP Switch(config)# no ip authorized-managers 10.28.227.101
```
WebAgent: Configuring IP Authorized Managers

In the WebAgent you can configure IP Authorized Managers as described below.

To Add, Modify, or Delete an IP Authorized Manager address:
1. In the navigation tree, click on Security.
2. Click on IP Authorization.
3. Click on Add Address to add an IP Authorized Manager. Enter the appropriate parameter settings for the operation you want.
4. To delete an IP authorized Manager, select the Authorized Address and click on Delete.
5. To change IP Authorization parameters, click on Change in the IP Authorization Details box. Enter the information and click on Save.

Figure 14-5. Example of Configuring Authorized Manager Access Method in the WebAgent
Web Proxy Servers

If you use the WebAgent to access the switch from an authorized IP manager station, it is highly recommended that you avoid using a web proxy server in the path between the station and the switch. This is because switch access through a web proxy server requires that you first add the web proxy server to the Authorized Manager IP list. This reduces security by opening switch access to anyone who uses the web proxy server.

How to Eliminate the Web Proxy Server

There are two ways to eliminate a web proxy server from the path between a station and the switch:

1. Add the IP address or DNS name of the switch to the non-proxy or Exceptions list in the web browser interface used on the authorized station.
2. If you don’t need proxy server access on the authorized station, disable the proxy server feature in the station’s web browser interface.

Note

IP or MAC authentication can be used without a web proxy server.

Using a Web Proxy Server to Access the WebAgent

Caution

This is NOT recommended. Using a web proxy server between the stations and the switch poses a security risk. If the station uses a web proxy server to connect to the switch, any proxy user can access the switch.

If it is necessary to use the WebAgent and your browser access is through a web proxy server, perform these steps:

1. Enter the web proxy server's MAC address in the port's Authorized Addresses list.
2. Enter the web proxy server's IP address in the switch's IP Authorized Managers list.

You must perform both of these steps or the switch only detects the proxy server's MAC address and IP address instead of your workstation addresses, and your connection is considered unauthorized.
Building IP Masks

The IP Mask parameter controls how the switch uses an Authorized Manager IP value to recognize the IP addresses of authorized manager stations on your network.

Configuring One Station Per Authorized Manager IP Entry

This is the easiest way to apply a mask. If you have ten or fewer management and/or operator stations, you can configure them by adding the address of each to the Authorized Manager IP list with 255.255.255.255 for the corresponding mask. For example, as shown in figure 14-3, if you configure an IP address of 10.28.227.125 with an IP mask of 255.255.255.255, only a station having an IP address of 10.28.227.125 has management access to the switch.

Figure 14-6. Analysis of IP Mask for Single-Station Entries

<table>
<thead>
<tr>
<th>IP Mask</th>
<th>1st Octet</th>
<th>2nd Octet</th>
<th>3rd Octet</th>
<th>4th Octet</th>
<th>Manager-Level or Operator-Level Device Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Manager IP</td>
<td>10</td>
<td>28</td>
<td>227</td>
<td>125</td>
<td>The “255” in each octet of the mask specifies that only the exact value in that octet of the corresponding IP address is allowed. This mask allows management access only to a station having an IP address of 10.33.248.5.</td>
</tr>
</tbody>
</table>

Configuring Multiple Stations Per Authorized Manager IP Entry

The mask determines whether the IP address of a station on the network meets the criteria you specify. That is, for a given Authorized Manager entry, the switch applies the IP mask to the IP address you specify to determine a range of authorized IP addresses for management access. As described above, that range can be as small as one IP address (if 255 is set for all octets in the mask), or can include multiple IP addresses (if one or more octets in the mask are set to less than 255).

If a bit in an octet of the mask is “on” (set to 1), then the corresponding bit in the IP address of a potentially authorized station must match the same bit in the IP address you entered in the Authorized Manager IP list. Conversely, if a bit in an octet of the mask is “off” (set to 0), then the corresponding bit in the IP address of a potentially authorized station on the network does not have to match its counterpart in the IP address you entered in the Authorized Manager IP list. Thus, in the example shown above, a “255” in an IP Mask octet (all bits
Using Authorized IP Managers  
Building IP Masks

in the octet are “on”) means only one value is allowed for that octet—the value you specify in the corresponding octet of the Authorized Manager IP list. A “0” (all bits in the octet are “off”) means that any value from 0 to 255 is allowed in the corresponding octet in the IP address of an authorized station. You can also specify a series of values that are a subset of the 0-255 range by using a value that is greater than 0, but less than 255.

**Figure 14-7. Analysis of IP Mask for Multiple-Station Entries**

<table>
<thead>
<tr>
<th></th>
<th>1st Octet</th>
<th>2nd Octet</th>
<th>3rd Octet</th>
<th>4th Octet</th>
<th>Manager-Level or Operator-Level Device Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Mask</strong></td>
<td>255</td>
<td>255</td>
<td>255</td>
<td>0</td>
<td>The “255” in the first three octets of the mask specify that only the exact value in the octet of the corresponding IP address is allowed. However, the zero (0) in the 4th octet of the mask allows any value between 0 and 255 in that octet of the corresponding IP address. This mask allows switch access to any device having an IP address of 10.28.227.xxx, where xxx is any value from 0 to 255.</td>
</tr>
<tr>
<td><strong>Authorized Manager IP</strong></td>
<td>10</td>
<td>28</td>
<td>227</td>
<td>125</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>1st Octet</th>
<th>2nd Octet</th>
<th>3rd Octet</th>
<th>4th Octet</th>
<th>Manager-Level or Operator-Level Device Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Mask</strong></td>
<td>255</td>
<td>255</td>
<td>255</td>
<td>249</td>
<td>In this example (figure 14-8, below), the IP mask allows a group of up to 4 management stations to access the switch. This is useful if the only devices in the IP address group allowed by the mask are management stations. The “249” in the 4th octet means that bits 0 and 3 - 7 of the 4th octet are fixed. Conversely, bits 1 and 2 of the 4th octet are variable. Any value that matches the authorized IP address settings for the fixed bits is allowed for the purposes of IP management station access to the switch. Thus, any management station having an IP address of 10.28.227.121, 123, 125, or 127 can access the switch.</td>
</tr>
<tr>
<td><strong>Authorized IP Address</strong></td>
<td>10</td>
<td>28</td>
<td>227</td>
<td>125</td>
<td></td>
</tr>
</tbody>
</table>
Using Authorized IP Managers
Building IP Masks

Figure 14-8. Example of How the Bitmap in the IP Mask Defines Authorized Manager Addresses

<table>
<thead>
<tr>
<th>4th Octet of IP Mask:</th>
<th>249</th>
</tr>
</thead>
<tbody>
<tr>
<td>4th Octet of Authorized IP Address:</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bit Numbers</th>
<th>Bit 7</th>
<th>Bit 6</th>
<th>Bit 5</th>
<th>Bit 4</th>
<th>Bit 3</th>
<th>Bit 2</th>
<th>Bit 1</th>
<th>Bit 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit Values</td>
<td>128</td>
<td>64</td>
<td>32</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Bits 1 and 2 in the mask are “off”, and bits 0 and 3 - 7 are “on”, creating a value of 249 in the 4th octet. Where a mask bit is “on”, the corresponding bit setting in the address of a potentially authorized station must match the IP Authorized Address setting for that same bit. Where a mask bit is “off” the corresponding bit setting in the address can be either “on” or “off”. In this example, in order for a station to be authorized to access the switch:
- The first three octets of the station’s IP address must match the Authorized IP Address.
- Bit 0 and Bits 3 through 6 of the 4th octet in the station’s address must be “on” (value = 1).
- Bit 7 of the 4th octet in the station’s address must be “off” (value = 0).
- Bits 1 and 2 can be either “on” or “off”.

This means that stations with the IP address 13.28.227.X (where X is 121, 123, 125, or 127) are authorized.

Entries for Authorized Manager List

<table>
<thead>
<tr>
<th>IP Mask</th>
<th>Authorized Manager IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>255</td>
<td>10 33 248 1</td>
</tr>
</tbody>
</table>

This combination specifies an authorized IP address of 10.33.xxx.1. It could be applied, for example, to a subnetted network where each subnet is defined by the third octet and includes a management station defined by the value of “1” in the fourth octet of the station’s IP address.

<table>
<thead>
<tr>
<th>IP Mask</th>
<th>Authorized Manager IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>255</td>
<td>10 247 100 195</td>
</tr>
</tbody>
</table>

Allows 230, 231, 246, and 247 in the 2nd octet, and 194, 195, 198, 199 in the 4th octet.
Operating Notes

- **Network Security Precautions**: You can enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, using the additional security features described in this manual, and preventing unauthorized access to data on your management stations.

- **Modem and Direct Console Access**: Configuring authorized IP managers does not protect against access to the switch through a modem or direct Console (RS-232) port connection.

- **Duplicate IP Addresses**: If the IP address configured in an authorized management station is also configured (or “spoofed”) in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists.

- **Web Proxy Servers**: If you use the WebAgent to access the switch from an authorized IP manager station, it is recommended that you avoid the use of a web proxy server in the path between the station and the switch. This is because switch access through a web proxy server requires that you first add the web proxy server to the Authorized Manager IP list. *This reduces security by opening switch access to anyone who uses the web proxy server.* The following two options outline how to eliminate a web proxy server from the path between a station and the switch:
  - Even if you need proxy server access enabled in order to use other applications, you can still eliminate proxy service for web access to the switch. To do so, add the IP address or DNS name of the switch to the non-proxy, or “Exceptions” list in the web browser interface you are using on the authorized station.
  - If you don’t need proxy server access at all on the authorized station, then just disable the proxy server feature in the station’s web browser interface.
Key Management System

Overview

The switches covered in this guide provide support for advanced routing capabilities. Security turns out to be extremely important as complex networks and the internet grow and become a part of our daily life and business. This fact forces protocol developers to improve security mechanisms employed by their protocols, which in turn becomes an extra burden for system administrators who have to set up and maintain them. One possible solution to the problem is to centralize the mechanisms used to configure and maintain security information for all routing protocols. The Key Management System (KMS) can carry this burden.

KMS is designed to configure and maintain key chains. A key chain is a set of keys with a timing mechanism for activating and deactivating individual keys. KMS provides specific instances of routing protocols with one or more Send or Accept keys that must be active at the time of a request. A protocol instance is usually an interface on which the protocol is running.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating a Key Chain</td>
<td>n/a</td>
<td>n/a</td>
<td>page 15-3</td>
<td>n/a</td>
</tr>
<tr>
<td>Generating a Time-Independent key</td>
<td>n/a</td>
<td>n/a</td>
<td>page 15-4</td>
<td>n/a</td>
</tr>
<tr>
<td>Generating a Time-Dependent key</td>
<td>n/a</td>
<td>n/a</td>
<td>page 15-5</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Terminology

- **Key Chain**: A key or set of keys assigned for use by KMS-enabled protocols. A key chain may optionally contain the time to activate and deactivate a particular key.

- **Time-Independent Key**: A key that has no activate or deactivate time associated with it. This type of key does not expire, which eliminates the need for a key chain.

- **Time-Dependent Key**: A key that has an activate and deactivate time associated with the Accept and Send processes. Time-Dependent keys expire, which means a key chain is needed to keep the assigned protocols supplied with keys.

- **Key Management System (KMS) Enabled Protocol**: A protocol that uses KMS to store authentication key information.

Configuring Key Chain Management

<table>
<thead>
<tr>
<th>KMS-Related CLI Commands in This Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show key-chain &lt; chain_name &gt;</td>
<td>page 15-3</td>
</tr>
<tr>
<td>[ no ] key-chain chain_name</td>
<td>page 15-3</td>
</tr>
<tr>
<td>[ no ] key-chain chain_name key Key_ID</td>
<td>page 15-4</td>
</tr>
</tbody>
</table>

The Key Management System (KMS) has three configuration steps:

1. Create a key chain entry.
2. Assign a time-independent key or set of time-dependent keys to the Key Chain entry. The choice of key type is based on the level of security required for the protocol to which the key entry will be assigned.
3. Assign the key chain to a KMS-enabled protocol.

This procedure is protocol-dependent. For information on a specific protocol, refer to the chapter covering that protocol in the *Management and Configuration Guide* for your switch.
Creating and Deleting Key Chain Entries

To use the Key Management System (KMS), you must create one or more key chain entries. An entry can be the pointer to a single time-independent key or a chain of time-dependent keys.

Note

The key chain information is copied to the standby management module (if redundancy is enabled and the standby module has passed self-test).

Syntax:  

[ no ] key-chain < chain_name >

Generate or delete a key chain entry. Using the optional no form of the command deletes the key chain. The < chain_name > parameter can include up to 32 characters.

show key-chain

Displays the current key chains on the switch and their overall status.

For example, to generate a new key chain entry:

HP Switch(config)# key-chain Networking1
HP Switch(config)# show key-chain

<table>
<thead>
<tr>
<th>Chain Name</th>
<th>Keys Active</th>
<th>Keys Expired</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 15-1. Adding a New Key Chain Entry

After you add an entry, you can assign key(s) to it for use by a KMS-enabled protocol.
Assigning a Time-Independent Key to a Chain

A time-independent key has no Accept or Send time constraints. It is valid from boot-up until you change it. If you use a time-independent key, then it is the only key needed for a key chain entry.

**Syntax:**
```
[no] key-chain <chain_name> key <key_id>
```
Generates or deletes a key in the key chain entry `<chain_name>`. Using the optional `no` form of the command deletes the key. The `<key_id>` is any number from 0-255.

```
[ key-string <key_str> ]
```
This option lets you specify the key value for the protocol using the key. The `<key_str>` can be any string of up to 14 characters in length.

```
[ accept-lifetime infinite ] [ send-lifetime infinite ]
```

- **accept-lifetime infinite:** Allows packets with this key to be accepted at any time from boot-up until the key is removed.
- **send-lifetime infinite:** Allows the switch to send this key as authorization, from boot-up until the key is removed.

```
show key-chain <chain_name>
```
Displays the detail information about the keys used in the key chain named `<chain_name>`.

For example, to generate a new time-independent key for the Networking1 key chain entry:

```
HP Switch(config)# key-chain Networking1 key 1
HP Switch(config)# show key-chain Networking1
```

<table>
<thead>
<tr>
<th>Key</th>
<th>Accept Start GMT</th>
<th>Accept Stop GMT</th>
<th>Send Start GMT</th>
<th>Send Stop GMT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bootup</td>
<td>Infinite</td>
<td>Bootup</td>
<td>Infinite</td>
</tr>
</tbody>
</table>

---

Figure 15-2. Example of Adding and Displaying a Time-Independent Key to a Key Chain Entry
Assigning Time-Dependent Keys to a Chain

A time-dependent key has Accept or Send time constraints. It is valid only during the times that are defined for the key. If a time-dependent key is used, there is usually more than one key in the key chain entry.

**Syntax:**

```
[no] key-chain < chain_name > key < key_id >
```

Generates or deletes a key in the key chain entry < chain_name >. Using the optional **no** form of the command deletes the key. The < key_id > is any number from 0-255.

```
[ key-string < key_str > ]
```

This option specifies the key value referenced by the protocol using the key. The < key_str > can be any string up to 14 characters in length.

```
accept-lifetime < mm/dd/yy [ yy ] hh:mm:ss | now >
```

Specifies the **start** date and time of the valid period in which the switch can use this key to authenticate inbound packets.

```
duration < mm/dd/yy [ yy ] hh:mm:ss | seconds >
```

Specifies the **time period** during which the switch can use this key to authenticate inbound packets. Duration is either an end date and time or the number of seconds to allow after the start date and time (which is the accept-lifetime setting).

```
send-lifetime < mm/dd/yy [ yy ] hh:mm:ss | now >
```

Specifies the **start** date and time of the valid period in which the switch can transmit this key as authentication for outbound packets.

```
show key-chain < chain_name >
```

Displays the detail information about the keys used in the key chain named < chain_name >.

---

**Note**

Using time-dependent keys requires that all the switches have accurate, synchronized time settings. You can manually set the time or use the Time protocol feature included in the switches. For more information, refer to the chapter covering time protocols in the *Management and Configuration Guide* for your switch.
For example, to add a number of keys to the key chain entry “Networking2”:

```
HP Switch(config)# key-chain Networking2 key 1 accept-lifetime now 06/17/11 8:00:00
```

```
HP Switch(config)# key-chain Networking2 key 2 accept-lifetime 06/18/11 8:00:00 duration 87000 send-lifetime 06/18/11 8:00:00 duration 86400
```

```
HP Switch(config)# key-chain Networking2 key 3 accept-lifetime 06/19/11 8:00:00 duration 87000 send-lifetime 06/19/11 8:00:00 duration 86400
```

```
HP Switch(config)# key-chain Networking2 key 4 accept-lifetime 06/20/11 8:00:00 duration 87000 send-lifetime 06/20/11 8:00:00 duration 86400
```

```
HP Switch(config)# key-chain Networking2 key 5 accept-lifetime 06/21/11 8:00:00 duration 87000 send-lifetime 06/21/11 8:00:00 duration 86400
```

**Figure 15-3. Adding Time-Dependent Keys to a Key Chain Entry**

**Note**

Given transmission delays and the variations in the time value from switch to switch, it is advisable to include some flexibility in the Accept lifetime of the keys you configure. Otherwise, the switch may disregard some packets because either their key has expired while in transport or there are significant time variations between switches.

To list the result of the commands in figure 15-4:

```
HP Switch(config)# show key-chain Networking2
```

**Figure 15-4. Display of Time-Dependent Keys in the Key Chain Entry**
You can use `show key-chain` to display the key status at the time the command is issued. Using the information from the example configuration in figures 15-3 and 15-4, if you execute `show key-chain` at 8:05 on 01/19/03, the display would appear as follows:

```
HP Switch(config)# show key-chain

Key Chains

<table>
<thead>
<tr>
<th>Chain Name</th>
<th>Keys</th>
<th>Active</th>
<th>Expired</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Networking2</td>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Figure 15-5. Status of Keys in Key Chain Entry “Networking2”**

The “Networking1” key chain entry is a time-independent key and will not expire. “Networking2” uses time-dependent keys, which result in this data:

- **Expired = 1**  
  Key 1 has expired because its lifetime ended at 8:10 on 01/18/03, the previous day.

- **Active = 2**  
  Key 2 and 3 are both active for 10 minutes from 8:00 to 8:10 on 1/19/03.

Keys 4 and 5 are either not yet active or expired. The total number of keys is 5.
Key Management System
Configuring Key Chain Management
Index

Numerics
3DES ... 8-2
802.1X
ACL, effect on ... 9-13
802.1X access control
authenticate users ... 12-3
authentication
local ... 12-4
methods ... 12-2
user-based ... 12-3
authenticator ... 12-18
backend state ... 12-64
operation ... 12-8
show commands ... 12-55
state ... 12-64
unblock port ... 12-4
authorized-client VLAN, defined ... 12-5
auth-vid ... 12-23
auto ... 12-21
blocked port, trunked ... 12-12
caution, unauthorized-client VLAN ... 12-40
CHAP ... 12-1
chap-radius ... 12-24
clear-statistics ... 12-27
client, effect of disconnect ... 12-40
client-limit, no ... 12-20
configure
commands ... 12-17
displaying configuration ... 12-55
overview ... 12-16
port ... 12-18
configuring method ... 12-24
control all clients ... 12-11
control command ... 12-21
convert to port-based ... 12-20
CoS override ... 12-64
counters ... 12-55
delay move to unauthorized-client
VLAN ... 12-36
delay Unauth-Client VLAN ... 12-23
DHCP server ... 12-41
display all 802.1X, Web, and MAC authentication
configuration ... 3-13
EAP ... 12-1
EAPOL ... 12-6, 12-59
eap-radius ... 12-24
enabling
controlled directions ... 12-27
on ports ... 12-18
on switch ... 12-27
event log messages ... 12-78
features ... 12-1
force authorized ... 12-21, 12-65
force unauthorized ... 12-21, 12-65
general setup ... 12-13
guest VLAN ... 12-5, 12-6, 12-32, 12-39
GVRP ... 12-69, 12-71
effect ... 12-71, 12-77
hierarchy of precedence in authentication
session ... 1-16
initialize ... 12-27
LACP not allowed ... 12-78
local ... 12-24
logoff-period ... 12-23
max-requests ... 12-22
MD5 ... 12-5, 12-51
meshing, not supported ... 12-12
messages ... 12-78
multiple clients ... 12-40
multiple clients, same VLAN ... 12-3
open port ... 12-2
open VLAN
authorized client ... 12-34
configuration ... 12-43, 12-46
general operation ... 12-32
mode ... 12-32, 12-38
operating notes ... 12-47
operating rules ... 12-39
PVID, no ... 12-64
security breach ... 12-47
set up ... 12-42
status ... 12-58, 12-65
status, viewing ... 12-64
suspended VLAN ... 12-65
unauthorized client ... 12-34
A

aaa
  gvrp-vlans ... 12-76, 12-77
  port-access gvrp-vlans ... 12-76, 12-77
aaa authentication ... 4-7
  authorized ... 12-24
  chap-radius ... 5-10
  peap-mschapv2 ... 5-10
  privilege-mode ... 4-10
  defined ... 4-11
aaa port-access
  See Web or MAC authentication.
access
  methods, determining ... 5-6
access levels
  authorized IP managers ... 14-2
accounting
  See RADIUS.
ACL
  802.1X, effect on ... 9-13
ACE
  after match not used ... 9-23, 9-36
  defined ... 9-7
  general rules ... 9-39
  insert in list ... 9-74
  limit ... 9-24
  minimum number ... 9-96
  not used ... 9-19

ACE, order in list
  See sequence, ACEs.
AppleTalk ... 9-23
application point ... 9-15
application points ... 9-21
applications ... 9-3, 9-11, 9-13, 9-15, 9-17
assign nonexistent i.d. ... 9-38
assign to VLAN ... 9-38
assigning ... 9-31
assigning to a VLAN ... 9-70
assignment not deleted ... 9-71
basic structure ... 9-32
character limit ... 9-42
CIDR ... 9-8
  mask ... 9-40
  mask bits, IP address ... 9-44, 9-48
command summary
  extended ... 9-5
  standard ... 9-4
command syntax ... 9-43, 9-47
configuration planning ... 9-15
configured but not used ... 9-38
configured, not used ... 9-38
configuring ... 9-31
configuring offline ... 9-14
copy operation appends ... 9-92
create, CLI method ... 9-39
DA, defined ... 9-8, 9-9
defined ... 9-1, 9-7
definitions ... 9-7
deleting from config ... 9-71
deny any, implicit ... 9-14, 9-17, 9-20, 9-22, 9-23, 9-24, 9-33, 9-37, 9-38
deny any, implicit, defined ... 9-8
deny any, implicit, supersede ... 9-33
deny, defined ... 9-8
display
  ACLs and assignments ... 9-88
  assignments ... 9-85
  configuration details ... 9-84
  content of an ACL ... 9-86
  data types ... 9-87
  summary, configured ACLs ... 9-83
dynamic ... 9-3, 9-17
dynamic port ACL ... 9-8
denied traffic ... 9-12
  multiple clients connected ... 9-12
dynamic port ACL application ... 9-12
dynamic port ACL operation defined ... 9-11
dynamic, IPv4 and IPv6 ... 9-12, 9-13, 9-17
editing ... 9-72
editing offline ... 9-91
effect of replacing ... 9-38
end ... 9-38
established ... 9-59
exit statement ... 9-38
extended
   command summary ... 9-5
   configure ... 9-50, 9-62
   create ... 9-5, 9-50
   defined ... 9-8, 9-32
   delete ... 9-6, 9-51
   named, configure ... 9-52
   numbered, configure ... 9-63
   numeric I.D. range ... 9-32
   protocol options ... 9-32
   remark ... 9-6, 9-51
   resequence ... 9-5, 9-50
   sequence number ... 9-5, 9-50
   structure ... 9-34
   use ... 9-11
features, common to all ... 9-13
filtering methods ... 9-11
filtering process ... 9-19, 9-23
host option ... 9-28
ICMP
   code ... 9-68
   configure ... 9-68
   options ... 9-60, 9-68
   traffic ... 9-15
   type ... 9-68
   type names ... 9-61
ID, defined ... 9-7
identifier ... 9-8
IGMP
   configure ... 9-62
   option ... 9-68
   traffic ... 9-15
   type ... 9-69
implicit deny
   See deny any, implicit.
inbound traffic, defined ... 9-9
interface assignment, options ... 9-17
inverse mask
   See ACL, wildcard.
IPX ... 9-23
log function, with mirroring ... 9-14
log message
   See ACL, logging.
logging ... 9-14, 9-15, 9-45
   described ... 9-93
   session ... 9-14
logging, notes ... 9-96
mask ... 9-8, 9-14, 9-26, 9-44
   CIDR ... 9-40
      defined ... 9-8
      multiple IP addresses ... 9-29
      one IP address ... 9-28
match, always ... 9-38
match, criteria ... 9-27
match, example ... 9-28
match, ignored ... 9-23
maximum allowed ... 9-24
mirroring, with log function ... 9-14
multiple ACLs on interface ... 9-13
multiple applications ... 9-13
multiple on same interface ... 9-13
name or number assignment ... 9-38
name string, maximum characters ... 9-32
named ... 9-9
named, character limit ... 9-42
named, rule ... 9-39
nonexistent i.d., assign ... 9-38
non-IPv4 traffic ... 9-23
number of entries ... 9-13
numbered ... 9-9
   manage as named ... 9-42
   rule ... 9-39
offline editing ... 9-91
operator, comparison ... 9-58, 9-59
override implicit deny ... 9-20
permit any forwarding ... 9-9, 9-23
permit, defined ... 9-9
permit, with multiple ACLs ... 9-13
permit/deny policies, defined ... 9-32
planning ... 9-15, 9-21
policies ... 9-21
policy application points ... 9-2
policy type ... 9-32
policy, permit/deny ... 9-32
port ... 9-25
port ACL operation defined ... 9-11
port added to trunk ... 9-25
port removed from trunk ... 9-25
port-based 802.1X ... 9-13
port-based security ... 9-13
precedence ... 9-15, 9-67
precedence, numbers and names ... 9-56
purpose ... 9-1
RACL
  operation defined ... 9-11
RADIUS-assigned ... 9-3, 9-7, 9-8, 9-12, 9-13, 9-17
  remark ... 9-9
  remove from an ACE ... 9-80
removing from a VLAN ... 9-70
replacing ... 9-25
replacing active ACEs ... 9-38
resequence ... 9-64
resource monitor ... 9-97
rules, configuration ... 9-24
rules, operation ... 9-24
SA, defined ... 9-9
security use ... 9-2, 9-22
security use, caution ... 9-23
sequence number ... 9-10, 9-73
  use to delete ACE ... 9-76
  use to insert ACE ... 9-74
sequence number interval ... 9-64
source routing, caution ... 9-16, 9-31
standard
  command summary ... 9-4
  configure ... 9-41
  create ... 9-4, 9-41
  defined ... 9-10, 9-32
  delete ... 9-41
  example ... 9-49
  named, configure ... 9-44
  numbered, configure ... 9-47
  numeric I.D. range ... 9-32
  remark ... 9-4, 9-41
  resequence ... 9-4, 9-41
  sequence number ... 9-4, 9-41
  structure ... 9-33
  use ... 9-11, 9-42
static port ACL ... 9-6, 9-10
static port ACL application ... 9-12
static VLAN requirement ... 9-25
static, defined ... 9-3
supermetting ... 9-27
supersede implicit deny any ... 9-37
syntax
  See command syntax.
Syslog
  See ACL, logging.
TCP or UDP port number, IANA ... 9-59
TCP/UDP operators ... 9-58
TCP/UDP, port names ... 9-59
terms ... 9-7
ToS setting ... 9-15
ToS, numbers and names ... 9-57, 9-67
traffic not filtered ... 9-23
traffic types filtered ... 9-2, 9-21
trunk ... 9-25
trunk, adding port ... 9-25
type ... 9-37, 9-42, 9-75, 9-82, 9-85, 9-86
user-based 802.1X ... 9-13
user-based security ... 9-13
VACL
  operation defined ... 9-11
VLANs ... 9-25
wildcard ... 9-8, 9-28
wildcard, defined ... 9-10
ACL, IPv4
  monitoring ... 9-89
ACL, IPv4 statistics counters, ACE ... 9-89
ACL, IPv6
  hit count
    See statistics, ACE.
    monitoring ... 9-89
    statistics counters, ACE, IPv4 ... 9-89
    troubleshooting ... 9-89
ACLs
  See also RADIUS-assigned ACLs.
address
  authorized for port security ... 13-3
alerts
  generating for monitored events ... 10-35
ARP
  adding IP-to-MAC binding ... 10-20, 10-28
debugging ... 10-23
displaying statistics ... 10-22
dynamic ARP protection ... 10-16
requests ... 10-34
trusted ports ... 10-18
validation checks on ARP packets,
configuring ... 10-21
authentication
  concurrent Web/MAC ... 3-3
  DCA-applied parameters to non-authenticated client sessions ... 1-16
display all 802.1X, Web, and MAC configurations ... 3-13
display custom messages ... 3-37
failures ... 10-34
NIM override ... 1-16
RADIUS override ... 1-17, 6-4
RADIUS server groups ... 5-22
authentication session
  client-specific configuration applied with DCA ... 1-16
authenticator
  backend state ... 12-64
  state ... 12-64
authorization
  creating a local user ... 5-72
  creating local groups ... 5-71
  local privilege levels ... 5-70
authorized addresses
  for IP management security ... 14-3
  for port security ... 13-3
authorized IP managers
  access levels ... 14-2
  access-method ... 14-6
  building IP masks ... 14-10
  configuring ... 14-6
  configuring in browser interface ... 14-8
  configuring in console ... 14-4
  definitions of single and multiple ... 14-3
  effect of duplicate IP addresses ... 14-13
  IP mask for multiple stations ... 14-10
  IP mask for single station ... 14-10
  IP mask operation ... 14-3
  manager, operator ... 14-6
  operating notes ... 14-13
  overview ... 14-1
  troubleshooting ... 14-13
authorized server ... 10-5
authorized server address, configuring ... 10-8
authorized, option for authentication ... 5-11, 12-24
autorun
  autorun-key ... 7-10
autorun-key ... 7-10

B
binding database ... 10-12
bindings
adding IP to MAC ... 10-28
displaying configuration ... 10-30
BPDU filtering ... 1-8
BPDU protection ... 1-8

C
cert, RSA key ... 7-10
certificate
  CA-signed ... 8-3
  root ... 8-3
  self-signed ... 8-3
CHAP ... 5-10
chap-radius ... 5-10
cipher, SSH ... 7-17
Class of Service
  See CoS.
Clear button
to delete password protection ... 2-5
configuration
  encrypt password ... 2-27
  filters ... 11-2
  port security ... 13-7
  RADIUS
    See RADIUS.
  saving security credentials in multiple files ... 2-25
  SSH
    See SSH.
  storage of security credentials
console
  authorized IP managers, configuring ... 14-4
  CoS
    configuring using RADIUS server ... 6-2
    non-default priority ... 6-6
    override ... 6-2, 12-64
    priority assignment ... 5-2
    RADIUS override ... 6-5
    viewing per-port config ... 6-4
crypto
  babble ... 7-11
  fingerprint ... 7-11

D
DA, defined ... 6-8, 9-8, 9-9
database, snooping ... 10-5
debug logging
DHCP snooping ... 10-13

default configuration and security ... 1-13
default settings

802.1X
  access control, none ... 1-5
aaa authentication parameters ... 4-12
aaa port-access mac-based ... 3-35–3-36
aaa port-access web-based ... 3-22–3-24
ACLs, none ... 1-4
authorized ip managers, none ... 1-4
client public-key authentication, disabled ... 7-1
DHCP snooping
database parameters ... 10-12
on VLANs, disabled ... 10-7
Option 82 remote-id, MAC address ... 10-11
Option 82 untrusted-policy, drop ... 10-10
trusted ports, disabled ... 10-7
DHCP snooping, none ... 1-8
DSA keysize, 1024 bits ... 7-12
dynamic arp protection, none ... 1-8
dynamic IP lockdown, none ... 1-8
dyn-autz-port 3799 ... 5-18
factory reset, enabled ... 2-36
front panel security ... 2-1, 2-36
instrumentation monitor
  SNMP traps, disabled ... 10-36
  thresholds and parameters ... 10-36
instrumentation monitor, disabled ... 10-36
key management system, none ... 1-8
MAC authentication, disabled ... 1-5
MAC lockdown and lockout, none ... 1-7
manager password, no password ... 1-2
multicast filters, none ... 11-2
passwords
clear password, enabled ... 2-36
password recovery, enabled ... 2-37, 2-43
password-clear, enabled ... 2-38
reset-on-clear, disabled ... 2-36
username and passwords, none ... 2-1
port security, none ... 1-7
port security, off or 'continuous' ... 13-2
protocol filters, none ... 11-2
RADIUS
  accounting, none ... 5-1
  authentication, none ... 5-1
  authorization, none ... 5-1
  global parameters ... 5-9
  radius-server dead-time, 0 minutes ... 5-18
  radius-server retransmit, 3 seconds ... 5-19
  radius-server timeout, 3 seconds ... 5-19
  server key, null ... 5-9
RADIUS authentication, disabled ... 1-4
RSA keysize, 2048 bits ... 7-12
secure management vlan, disabled ... 1-4
security
  access security and authentication ... 1-2
  network security ... 1-6
SNMP access ... 1-13
SNMP access to the security MIB, open ... 5-27
SNMP, public, unrestricted ... 1-4
source-port filters, none ... 11-2
spanning tree
  bpdu filtering, none ... 1-8
  bpdu protection, none ... 1-8
SSH, disabled ... 1-3, 7-1
SSL, disabled ... 1-4, 8-1
TACACS+
  authentication configuration ... 4-8
  authentication, disabled ... 1-4, 4-1
  login attempts, 3 ... 4-5
tacacs-server-timeout, 5 seconds ... 4-23
TCP port number for SSH connections, 22 ... 7-18
TCP port number for SSL connections, 443 ... 8-16
Telnet access, enabled ... 1-3
time-window, 300 seconds ... 5-16
traffic filters, none ... 11-2
traffic/security filters, none ... 1-6
UDP destination port for accounting, 1813 ... 5-7
UDP destination port for authentication, 1812 ... 5-7
usb autorun, disabled(if password) ... 1-6
usb autorun, enabled(if no password) ... 1-6
user authentication, disabled ... 7-1
Web and MAC authentication ... 3-1–3-36
Web authentication, disabled ... 1-5
Web-browser access, enabled ... 1-3
default settings
dyn-authorization, disabled ... 5-15
denial-of-service
  avoid attacks using DHCP snooping ... 10-4
  monitoring system resources ... 10-34
DES ... 8-2
DHCP Option 82
IP-to-MAC binding database … 10-20, 10-28

**DHCP protection**
See DHCP snooping.

**DHCP snooping** … 10-3
authorized server … 10-5
binding database … 10-12
changing remote-id … 10-11
configuring authorized server address … 10-8
database … 10-5
denial-of-service attack … 10-4
DHCPACK … 10-4
DHCPDECLINE … 10-4
DHCPNACK … 10-4
DHCPOFFER … 10-4
DHCPRELEASE … 10-4
disable MAC check … 10-11
disabling … 10-5
dropping packets … 10-4
enabling … 10-5
debug logging … 10-13
on trusted ports … 10-7
on VLANs … 10-5, 10-7
IP-to-MAC binding database … 10-20, 10-28
log messages … 10-14
Option 82 … 10-9
option parameter … 10-5
remote-id … 10-10
show configuration … 10-5
stats … 10-6
trust … 10-5
untrusted-policy … 10-10
verify … 10-5

**documentation**
feature matrix … -xxii
latest versions … -xxi
release notes … -xxi

**downgrading software** … 2-8
duplicate IP address
 effect on authorized IP managers … 14-13
dynamic ARP protection
 additional validation checks on ARP packets … 10-21
ARP packet debugging … 10-23
displaying ARP statistics … 10-22
enabling … 10-16
IP-to-MAC binding, adding to DHCP database … 10-20, 10-28
trusted ports, configuring … 10-18
verifying configuration … 10-21

**Dynamic Configuration Arbiter (DCA)**
applying settings to non-authenticated clients … 1-16
hierarchy of precedence in authentication sessions … 1-17
overview … 1-15
dynamic IP lockdown
debugging … 10-31
DHCP binding database … 10-25
DHCP leases … 10-25
DHCP snooping … 10-24
enabling … 10-26
filtering IP addresses … 10-25
overview … 10-23
platform differences … 10-32
spoofing protection … 10-24
verifying configuration … 10-29
VLAN binding … 10-25
dyn-autz-port … 5-18

**E**
eavesdrop prevention
 configured mode … 13-4
continuous learn mode … 13-4
disabling … 13-3
interactions with learn modes … 13-4
limited-continuous mode … 13-4
mib support … 13-5
overview … 13-3
port-security command … 13-4
static mode … 13-4
Eavesdrop Protection … 13-2
encrypt-credentials … 2-27, 2-28
affected commands … 2-30
displaying state of … 2-29
encrypted-secret for 802.1X … 12-53
operating notes … 2-31
pre-shared-key … 2-28
encrypted-secret … 12-53
encryption key
 RADIUS … 2-12, 2-17
TACACS … 2-12, 2-16
enhancing network security … 6-11
event log
 alerts for monitored events … 10-35
Event Log Message Reference Guide … -xxi
intrusion alerts 13-41

F
filetransfer, SSH 7-17
filter, source-port
  applicable models 11-1
  editing 11-19
  filter indexing 11-21
  filter type 11-8
  idx 11-8, 11-21
  index 11-8, 11-21
  named 11-6
  operating rules 11-3, 11-6
  port-trunk operation 11-2, 11-18
  show 11-8
  value 11-8
  viewing 11-8
See also source port filters.
filtering MAC addresses 10-25
filters
  effect of IGMP 11-15
  multicast 11-14
  overview 11-2
  protocol 11-15
  source port 11-3
  source-port filter value 11-21
  static 11-2
  types 11-3
Framed-IP-Address 5-48

G
guest VLAN 12-5, 12-6, 12-32
GVRP
dynamic VLANs 12-76
  effect on client authentication 12-69, 12-71
  static VLAN not advertised 12-72, 12-77

H
hierarchy of precedence, used by DCA 1-16
HP E-Network Immunity Manager (NIM) 1-16
HP Networking
  switch documentation -xxi
HP PCM
IDM as a plug-in to 1-20
  port security alerts 13-2

HP PMC Identity Driven Manager (IDM) 1-20

I
IANA 9-59
IANA, protocol numbers 9-55, 9-60
IDM 6-7, 6-28
  overview 1-20
  RADIUS-based security classifiers 1-20
  See also RADIUS-assigned ACLs
  RADIUS-assigned ACLs.
IGMP
  effect on filters 11-15
  IP multicast address range 11-15
include credentials command 2-11
  See also security credentials.
include-credentials
  displaying status 2-22
  RADIUS-TACACS only 2-18
  store-in-config 2-12
interface
  unknown-vlans command 12-76
intrusion alarms
  entries dropped from log 13-43
  event log 13-41
  prior to 13-43
Intrusion Log
  prior to 13-38, 13-40
IP
  address count 10-34
  authorized IP managers 14-1
  reserved port numbers 7-18
IP attribute 5-48
IP masks
  building 14-10
  for multiple authorized manager stations 14-10
  for single authorized manager station 14-10
  operation 14-3
IP routing
  dynamic ARP protection, enabling 10-16
  validation checks on ARP packets, configuring 10-21
ip source-binding 10-29
ip source-lockdown 10-26, 10-27
  bindings 10-30, 10-31
IP spoofing
  protection against 10-24
IP-to-MAC binding ... 10-20, 10-28
IPv4, ACL
  vendor-specific attribute ... 6-16
IPv6, ACL
  vendor-specific attribute ... 6-16
ip-version, ipv4or6 ... 7-17

K
key chain
  See KMS key chain.
key management system
  See KMS.
KMS
  accept key time ... 15-5, 15-6
  assigning a time-dependent key ... 15-5
  assigning a time-independent key ... 15-4
  generating a key chain ... 15-3
  generating a time-dependent key ... 15-5
  generating a time-independent key ... 15-4
  key chain ... 15-2
  key chain entry ... 15-3
  key chain generation ... 15-2
  overview ... 15-1
  send key time ... 15-5
  time protocol ... 15-5
  time-dependent key ... 15-2, 15-5
  time-independent key ... 15-2, 15-4

L
LACP
  802.1X not allowed ... 12-12, 12-18, 12-78
local privilege levels ... 5-70
login attempts, monitoring ... 10-34

M
MAC address
  count, monitoring ... 10-34
  inconsistent value ... 13-20
  moves, monitoring ... 10-34
MAC authentication
  address limit ... 3-35
  authenticator operation ... 3-5
  blocked traffic ... 3-1
  CHAP
    defined ... 3-9
    usage ... 3-1
    client status ... 3-49
    concurrent with Web ... 3-3
    configuration commands ... 3-32
    configuring
      on the switch ... 3-31
      switch for RADIUS access ... 3-15
      the RADIUS server ... 3-15
    general setup ... 3-12
    hierarchy of precedence in authentication
      session ... 1-16
    LACP not allowed ... 3-12
    overview ... 1-5
    port access ... 12-2
    rules of operation ... 3-10
    show status and configuration ... 3-42
    terminology ... 3-9
MAC Lockdown ... 13-1
MAC lockout ... 13-1
  number of vlans ... 13-33
MAC-Based VLAN ... 5-46
manager password ... 2-2, 2-4, 2-5
  recommended ... 4-6
  saving to configuration file ... 2-14
MD5
  See RADIUS.
message
  inconsistent value ... 13-20
messages
  custom when not authenticated ... 3-37
MIB
  SNMP access ... 1-13
  SNMP access to authentication MIB ... 1-13
MSCHAPv2 ... 5-10
multicast
  filter ... 11-3, 11-14
multicast address, spanning tree
  protocol ... 11-15
multicast MAC address, STP

N
named source port filters
  configuring ... 11-6
  displaying ... 11-8
  operating rules ... 11-6
  See also source port filters.
NAS ... 6-8
Network Immunity Manager (NIM)
hierarchy of precedence in authentication session ... 1-16
overview ... 1-16
no switch access ... 2-9

O
open VLAN mode
See 802.1X access control.
OpenSSH ... 7-2
OpenSSL ... 8-1
operating notes
authorized IP managers ... 14-13
port security ... 13-42
operator password ... 2-2, 2-4, 2-5
saving to configuration file ... 2-14
Option 82
snooping ... 10-5

P
packet validation ... 10-5
password ... 2-8, 2-9
802.1X port-access ... 2-12
browser/console access ... 2-3
case-sensitive ... 2-4
cautions ... 2-3
configuring manager and operator ... 2-15
delete ... 2-5
deleting with the Clear button ... 2-5
disables usb autorun ... 2-3
if you lose the password ... 2-5
included with security credentials ... 2-12
incorrect ... 2-3
length ... 2-4
length limit ... 2-7
locally configured, hierarchy of precedence in authentication session ... 1-16
operator only, caution ... 2-3
password pair ... 2-1
rules for characters ... 2-7
setting ... 2-4
SNMP configuration ... 2-1
upgrading software ... 2-8
with Setmib ... 2-8
password security ... 7-20
saved to configuration file ... 2-14
peap-mschapv2 ... 5-10
port
security configuration ... 13-1
trusted ... 10-18
untrusted ... 10-20, 10-28
port access
client limit ... 12-19, 12-20
current ... 12-19, 12-20
MAC authentication ... 12-2
tracking client authentication failures ... 10-34
Web authentication ... 12-2
Web/MAC ... 12-19, 12-20
See also 802.1X access control.
port scan, detecting ... 10-34
port security
802.1X, learn mode requirement ... 13-14
authorized address definition ... 13-3
basic operation ... 13-2
cautions, device limit ... 13-14
configuring ... 13-7
event log ... 13-41
notice of security violations ... 13-35
operating notes ... 13-42
overview ... 1-7, 13-1
prior to ... 13-43
proxy web server ... 13-42
TCP/UDP closed ports ... 10-34
port-based access control
password ... 2-12
port-security learn mode ... 13-14
VLAN, tagged member ... 13-44
See also 802.1X access control.
ports, trusted ... 10-5
port-security, eavesdrop prevention ... 13-4
prior to ... 13-38, 13-40, 13-43
Privacy Enhanced Mode (PEM)
See SSH.
privilege-mode ... 4-10, 4-11
protocol filters ... 11-15
proxy
web server ... 13-42
R
RADIUS
accounting ... 5-2, 5-52
accounting, configuration outline ... 5-52
accounting, configure server access ... 5-53
accounting, configure types on switch ... 5-56
accounting, exec ... 5-47, 5-56
accounting, interim updating ... 5-61
accounting, network ... 5-56
accounting, operating rules ... 5-48
accounting, server failure ... 5-49
accounting, session-blocking ... 5-61
accounting, statistics terms ... 5-57
accounting, stop-only method ... 5-57
accounting, system ... 5-47, 5-56
administrative-user service-type value ... 5-13
authentication limits ... 5-75
authentication options ... 5-1
authentication, authorized ... 5-11
authentication, local ... 5-31
authentication, web ... 5-1
authentication, webagent ... 5-10, 5-13
authorization ... 5-33
bypass RADIUS server ... 5-12
change of authorization ... 5-44
change-of-authorization attribute ... 5-44
Class of Service ... 6-6
commands authorization ... 5-33
commands, accounting ... 5-52
commands, switch ... 5-7
configuration outline ... 5-8
configure server access ... 5-14
configuring commands authorization ... 5-35
configuring switch global parameters ... 5-17
CoS override ... 6-2
display custom msgs ... 3-37
displaying group information ... 5-25
dynamic port access changes ... 5-75
dynamic port ACL ... 6-8
dyn-autz-port ... 5-18
Egress-VLAN ID attribute ... 5-42
Egress-VLAN-Name attribute ... 5-42
Framed-IP-Address ... 5-48
general setup ... 5-6
HP-acct-terminate-cause attribute ... 5-43
HP-Command-Exception ... 5-36
HP-command-string ... 5-35
IP attribute ... 5-48
local authentication ... 5-12
login privilege-mode, application options ... 5-13
login-privilege mode ... 5-12
manager access denied ... 5-13
manager access privilege ... 5-12
manager access privilege, service type value ... 5-7
MD5 ... 5-5
messages ... 5-79
MS-RAS-Vendor attribute ... 5-43
multiple ACL application types in use ... 6-13
multiple server groups ... 5-22
NAS-Prompt-User service-type value ... 5-13
network accounting ... 5-47
operating rules, switch ... 5-5
override CoS ... 6-5
override CoS, example ... 6-6
override Rate-Limiting ... 6-5
override Rate-Limiting, example ... 6-6
override, precedence, multiple clients ... 6-6
rate-limiting ... 6-2, 6-4
rate-limiting override ... 6-2
security ... 5-12
security note ... 5-2
server access order ... 5-48
server access order, changing ... 5-67
server key with tilde character ... 12-26, 12-45
server-group command ... 5-23, 5-24
servers, multiple ... 5-19
service type value ... 5-7
service-type value ... 5-13
service-type value, null ... 5-13
shared secret key, saving to configuration file ... 2-12, 2-17
show accounting ... 5-66
show authentication ... 5-64
SNMP access security not supported ... 5-2
SNMP access to auth config MIB ... 5-3
statistics, viewing ... 5-62
terminology ... 5-4
TLS ... 5-5
Tunnel-Type attribute ... 5-43
vendor specific attributes ... 5-43
vendor-specific attributes ... 5-35, 6-2
VSAs ... 5-37, 5-75
VSAs for client limit ... 5-76
web browser security not supported ... 5-6
webagent access controls ... 5-32
webagent security not supported ... 5-32
web-browser security not supported ... 5-2

**RADIUS accounting**

See *RADIUS*. 

---

12 – Index
RADIUS-assigned ACLs ... 6-7, 9-3
S02.1X port-based access ... 6-15
S02.1X user-based access ... 6-15
ACE, defined ... 6-7
application type ... 6-8
contrasting dynamic and static ... 6-11
DA, defined ... 6-8
defined ... 6-7
definitions ... 6-7
deny any, implicit, switched packets ... 6-14
deny, defined ... 6-8
dynamic port ACL ... 6-8
dynamic port ACL, effect ... 6-15
filters ... 6-11
implicit deny, defined ... 6-8
inbound traffic, defined ... 6-8
inverse mask
See wildcard.
mask ... 6-8
mask, defined ... 6-8
multiple application types in use ... 6-13
multiple clients, access restriction ... 6-15
multiple dynamic ACLs ... 6-15
outbound traffic, defined ... 6-8
permit, defined ... 6-9
resource monitor ... 6-28
See also ACLs.
source routing, caution ... 6-12
standard attribute ... 6-16
static-port ACL ... 6-9
switched packets ... 6-14
terminology ... 6-7
terms ... 6-7
vendor-specific attribute ... 6-16
wildcard ... 6-8, 6-9
wildcard, defined ... 6-9
radius-server
host
key with tilde character ... 3-16
key with tilde character ... 3-16
rate-limiting ... 10-35
override ... 12-64
RADIUS administered ... 5-2
RADIUS override ... 6-5
RADIUS server specified ... 6-4
RADIUS server support ... 6-2
RADIUS-assigned vs. applied ... 6-3
RADIUS-assigned, increments ... 6-3
remote-id
changing ... 10-11
snooping ... 10-10
reserved port numbers ... 7-18, 8-17
Reset-on-clear
disabled when saving security credentials to
configuration file ... 2-25
resource monitor
See Management and Configuration Guide.
RFCs
RFC 2548 ... 5-43
RFC 3580 ... 5-43
RFC 4675 ... 5-42
routing
source-routing, caution ... 6-12, 9-16, 9-31
RSA key, cert ... 7-10
S
SA ... 9-9
security
authorized IP managers ... 14-1
per port ... 13-1
security credentials
802.1X credentials saved to configuration
file ... 2-26
copying configurations on the switch ... 2-25
copying startup configuration ... 2-24
disabling Reset-on-clear option ... 2-25
downloading a configuration file ... 2-24
downloading from a server ... 2-10
enabling storage in configuration file ... 2-11
manager username and password ... 2-14
operator username and password ... 2-14
RADIUS ... 2-17
saving to running configuration with include-
credentials ... 2-24
saving to startup configuration ... 2-24
saving to startup configuration with write
memory ... 2-24
SNMPv3 ... 2-15
SSH ... 2-19
SSH private keys not saved ... 2-26
TACACS ... 2-16
viewing in running configuration ... 2-11
viewing in startup configuration ... 2-24
when SNMPv3 credentials in downloaded file
are not supported ... 2-26
security violations
  detecting … 10-34
  notices of … 13-35

security, ACL
  See ACL, security use.

security, password
  See SSH.

setting a password … 2-4

shared secret key
  RADIUS … 2-12, 2-17
  TACACS … 2-12, 2-16

single sign-on … 4-10

SNMP
  authentication failures … 10-34
  password and username configuration … 2-1
  RADIUS access to auth config MIB … 5-3
  trap generation … 10-36

SNMPv3
  saving security credentials to configuration
  file … 2-12, 2-15
  security credentials not supported in download-
  ed file … 2-26

snooping
  authorized server … 10-5
  authorized server address … 10-8
  binding database … 10-12
  changing remote-id … 10-11
  DHCP … 10-3
  disable MAC check … 10-11
  Option 82 … 10-5, 10-9
  statistics … 10-6
  untrusted-policy … 10-10
  verify … 10-5

source port filters
  configuring … 11-3
  named … 11-5
  operating rules … 11-3
  See also named source port filters.
  selection criteria … 11-3

source-routing, caution … 6-12, 9-16, 9-31

spanning tree
  caution about filtering … 11-15
  edge port configuration … 3-20, 12-28
  security features … 1-8

spanning tree protocol
  See STP.

spoofing
  protection against … 10-24

SSH
  authenticating switch to client … 7-2
  authentication, client public key … 7-1
  authentication, user password … 7-1
  caution, security … 7-19
  cipher … 7-17
  CLI commands … 7-8
  client
  copy client-known-hosts file … 7-33
  copy host public key … 7-35
  copy private key … 7-31
  initiate session … 7-30
  remove client key pair … 7-35
  remove client known hosts file … 7-36
  view open sessions … 7-36
  client behavior … 7-15
  client public-key authentication … 7-20, 7-24
  client public-key, clearing … 7-28
  client public-key, creating file … 7-25
  client public-key, displaying … 7-27
  configuring authentication … 7-20
  configuring key lengths … 7-12
  crypto key … 7-10
  disabling … 7-10
  enable … 7-16, 8-16
  enabling … 7-15
  erase host key pair … 7-10
  filetransfer … 7-17
  generate host key pair … 7-10
  generating key pairs … 7-9
  host key pair … 7-10
  ip-version … 7-17
  key, babble … 7-11
  key, fingerprint … 7-11
  keys, zeroing … 7-10
  keysize … 7-12
  known-host file … 7-13, 7-15
  mac selection … 7-18
  man-in-the-middle spoofing … 7-16
  messages, operating … 7-38
  OpenSSH … 7-2
  operating rules … 7-7
  password security … 7-20
  password-only authentication … 7-20
  passwords, assigning … 7-8
  PEM … 7-3
  prerequisites … 7-4
private keys not saved to configuration
   file ... 2-26
public key ... 7-4, 7-13
public key, displaying ... 7-14
public key, saving to configuration file ... 2-12, 2-19
reserved IP port numbers ... 7-18
security ... 7-19
SSHv2 ... 7-1
steps for configuring ... 7-5
switch key to client ... 7-13
terminology ... 7-3, 15-2
unauthorized access ... 7-29
version ... 7-1
view open sessions ... 7-36
zeroing a key ... 7-10
zeroize ... 7-11
SSL
   CA-signed ... 8-3, 8-13
   CA-signed certificate ... 8-3, 8-13
cert ... 8-7
   CLI commands ... 8-6
   client behavior ... 8-15
crypto key ... 8-8
disabling ... 8-7, 8-15
   enabling ... 8-15
   erase certificate key pair ... 8-7
   erase host key pair ... 8-7
generate CA-signed ... 8-13
generate CA-signed certificate ... 8-13
generate host key pair ... 8-7
generate self-signed ... 8-12
generate self-signed certificate ... 8-7, 8-12
generate server host certificate ... 8-7
generating Host Certificate ... 8-6
host key pair ... 8-7
key, babble ... 8-10
key, fingerprint ... 8-10
man-in-the-middle spoofing ... 8-15
OpenSSL ... 8-1
operating notes ... 8-5
operating rules ... 8-5
passwords, assigning ... 8-6
prerequisites ... 8-4
remove self-signed certificate ... 8-7
remove server host certificate ... 8-7
reserved TCP port numbers ... 8-17
root ... 8-3
root certificate ... 8-3
self-signed ... 8-3, 8-12
self-signed certificate ... 8-3, 8-7, 8-12
server host certificate ... 8-7
SSL server ... 8-3
SSLv3 ... 8-1
steps for configuring ... 8-4
supported encryption methods ... 8-2
terminology ... 8-3
TLSv1 ... 8-1
troubleshooting, operating ... 8-18
unsecured web browser access ... 8-15
version ... 8-1
zeroize ... 8-8, 8-9
static ACL ... 9-3
static filter limit ... 11-2
static multicast filter ... 11-14
STP
   prerequisite for 802.1X controlled
directions ... 12-28
   prerequisite for web-based controlled
directions ... 3-20
   STP multicast MAC address
superhosting ... 9-27
supersede implicit deny any ... 9-33
Syslog
   See ACL, logging.
system delay ... 10-34
system resource usage ... 10-34
T
TACACS
   aaa parameters ... 4-12
   authentication ... 4-2
   authentication process ... 4-23
   authentication, local ... 4-24
   authorized IP managers, effect ... 4-29
   configuration, authentication ... 4-10
   configuration, encryption key ... 4-21
   configuration, server access ... 4-17
   configuration, timeout ... 4-23
   configuration, viewing ... 4-9
   encryption key ... 4-5, 4-17, 4-21
   encryption key exclusion ... 4-20
   encryption key, general operation ... 4-25
   encryption key, global ... 4-22

Index – 15
encryption key, saving to configuration file … 2-12
general operation … 4-1
IP address, server … 4-17
local manager password requirement … 4-29
messages … 4-28
NAS … 4-2
precautions … 4-4
preparing to configure … 4-7
preventing switch lockout … 4-17
privilege level code … 4-6
server access … 4-17
server priority … 4-21
setup, general … 4-4
shared secret key, saving to configuration file … 2-16
show authentication … 4-7
single login … 4-12
single sign-on … 4-12
system requirements … 4-4
TACACS+ server … 4-2, 4-7
testing … 4-4
TFTP, configuration … 4-29
timeout … 4-17
troubleshooting … 4-5
unauthorized access, preventing … 4-6
web access, controlling … 4-27
web access, no effect on … 4-4
trusted ports
  enabling snooping … 10-7
U
untrusted policy, snooping … 10-10
USB
autorun and passwords … 2-3
user name
cleared … 2-5
SNMP configuration … 2-1
V
Vendor-Specific Attribute … 6-9
vendor-specific attribute
  configured in RADIUS server … 6-2
  configuring … 6-2
  configuring support for HP VSAs … 5-37
defining … 5-38
virus detection
  monitoring ARP requests … 10-34
VLAN
  802.1X … 12-69
  802.1X, ID changes … 12-72, 12-77
  802.1X, suspend untagged VLAN … 12-65
guest access … 12-29
not advertised for GVRP … 12-72, 12-77
port-access mixed … 12-29
Tagged egress VLAN in authentication session … 5-42
tagged egress VLAN in authentication session … 5-43
unauthenticated access … 12-29
untagged VLAN in authentication session … 5-42, 5-43
VLANs
  GVRP-created … 12-76
  GVRP-learned … 12-76
See also VLAN.
VSA … 6-9
  See vendor-specific attribute.
  with RADIUS … 5-75
W
Wake-on-LAN
  on 802.1X-aware ports … 12-28
on web-authenticated ports ... 3-21

**warranty** ... ii

**Web authentication**
- authenticator operation ... 3-5
- blocked traffic ... 3-1
- CHAP
  - defined ... 3-9
  - usage ... 3-1
- client limit ... 3-22
- client status ... 3-49
- concurrent with MAC ... 3-3
- configuration commands ... 3-19
- configuring
  - access control on unauthenticated ports ... 3-20
  - controlled directions ... 3-20
  - on the switch ... 3-18
  - switch for RADIUS access ... 3-15
- display all 802.1X, Web, and MAC authentication configuration ... 3-13, 12-14
- general setup ... 3-12
- hierarchy of precedence in authentication session ... 1-16
- LACP not allowed ... 3-12
- overview ... 1-5
- port access ... 12-2
- redirect URL ... 3-9
- rules of operation ... 3-10
- show status and configuration ... 3-25
- terminology ... 3-9
- Wake-on-LAN traffic ... 3-21

**web browser interface**
- authorized IP managers, configuring ... 14-6, 14-8
- SSL ... 8-15
- unsecured access, SSL ... 8-15

**web server, proxy** ... 13-42

**webagent**
- access ... 5-6

**wildcard**
- See ACL, wildcard.
- See ACL

**wildcard, ACL, defined** ... 6-9