
Contents

Product Documentation

About Your Switch Manual Set	xvii
Feature Index	xviii

1 Getting Started

Contents	1-1
Introduction	1-2
Conventions	1-2
Feature Descriptions by Model	1-2
Command Syntax Statements	1-3
Command Prompts	1-3
Screen Simulations	1-3
Port Identity Examples	1-4
Keys	1-4
Sources for More Information	1-4
Getting Documentation From the Web	1-6
Online Help	1-8
Need Only a Quick Start?	1-9
To Set Up and Install the Switch in Your Network	1-9
Overview of Access Security Features	1-10
General Switch Traffic Security Guideline	1-11
Applications for Access Control Lists (ACLs)	1-11

2 Configuring Username and Password Security

Contents	2-1
Overview	2-2
Configuring Local Password Security	2-5
Menu: Setting Passwords	2-5
CLI: Setting Passwords and Usernames	2-7
Web: Setting Passwords and Usernames	2-8
Front-Panel Security	2-8
When Security Is Important	2-9
Front-Panel Button Functions	2-10
Clear Button	2-11
Reset Button	2-11
Restoring the Factory Default Configuration	2-11
Configuring Front-Panel Security	2-13
Disabling the Clear Password Function of the Clear Button on the Switch's Front Panel	2-15
Re-Enabling the Clear Button on the Switch's Front Panel and Setting or Changing the "Reset-On-Clear" Operation	2-16
Changing the Operation of the Reset+Clear Combination	2-17
Password Recovery	2-18
Disabling or Re-Enabling the Password Recovery Process	2-18
Password Recovery Process	2-20

3 Virus Throttling (5300xl Switches Only)

Contents	3-1
Introduction	3-3
General Operation of Connection-Rate Filtering	3-5
Filtering Options	3-5
Sensitivity to Connection Rate Detection	3-6
Application Options	3-6
Terminology	3-7
Operating Rules	3-8
General Configuration Guidelines	3-9

For a network that is relatively attack-free:	3-9
For a network that appears to be under significant attack:	3-10
Basic Connection-Rate Filtering Configuration	3-11
Global and Per-Port Configuration	3-11
Enabling Connection-Rate Filtering and Configuring Sensitivity	3-12
Configuring the Per-Port Filtering Mode	3-13
Example of a Basic Connection-Rate Filtering Configuration . .	3-14
Viewing and Managing Connection-Rate Status	3-16
Viewing the Connection-Rate Configuration	3-16
Listing and Unblocking the Currently-Blocked Hosts	3-18
Configuring and Applying Connection-Rate ACLs	3-20
Connection-Rate ACL Operation	3-21
Configuring a Connection-Rate ACL Using Source IP Address Criteria	3-22
Configuring a Connection-Rate ACL Using UDP/TCP Criteria	3-23
Applying Connection-Rate ACLs	3-26
Using CIDR Notation To Enter the ACE Mask	3-26
Example of Using an ACL in a Connection-Rate Configuration	3-27
Connection-Rate ACL Operating Notes	3-30
Connection-Rate Log and Trap Messages	3-31

4 Web and MAC Authentication

Contents	4-1
Overview	4-2
Client Options	4-3
General Features	4-4
How Web and MAC Authentication Operate	4-5
Authenticator Operation	4-5
Web-based Authentication	4-5
MAC-based Authentication	4-7
Terminology	4-9
Operating Rules and Notes	4-10
General Setup Procedure for Web/MAC Authentication	4-12

Do These Steps Before You Configure Web/MAC Authentication . . .	4-12
Additional Information for Configuring the RADIUS Server To Support MAC Authentication	4-14
Configuring the Switch To Access a RADIUS Server	4-15
Configuring Web Authentication on the Switch	4-17
Overview	4-17
Configure the Switch for Web-Based Authentication	4-18
Configuring MAC Authentication on the Switch	4-22
Overview	4-22
Configure the Switch for MAC-Based Authentication	4-23
Show Status and Configuration of Web-Based Authentication	4-26
Show Status and Configuration of MAC-Based Authentication	4-28
Client Status	4-30

5 TACACS+ Authentication

Contents	5-1
Overview	5-2
Terminology Used in TACACS Applications:	5-3
General System Requirements	5-5
General Authentication Setup Procedure	5-5
Configuring TACACS+ on the Switch	5-8
Before You Begin	5-8
CLI Commands Described in this Section	5-9
Viewing the Switch's Current Authentication Configuration	5-9
Viewing the Switch's Current TACACS+ Server Contact Configuration	5-10
Configuring the Switch's Authentication Methods	5-11
Configuring the Switch's TACACS+ Server Access	5-15
How Authentication Operates	5-20
General Authentication Process Using a TACACS+ Server	5-20
Local Authentication Process	5-22
Using the Encryption Key	5-23

General Operation	5-23
Encryption Options in the Switch	5-23
Controlling Web Browser Interface Access When Using TACACS+ Authentication	5-24
Messages Related to TACACS+ Operation	5-25
Operating Notes	5-26

6 RADIUS Authentication and Accounting

Contents	6-1
Overview	6-3
Authentication Services	6-3
Accounting Services	6-4
RADIUS-Administered CoS and Rate-Limiting	6-4
Terminology	6-4
Switch Operating Rules for RADIUS	6-5
General RADIUS Setup Procedure	6-7
Configuring the Switch for RADIUS Authentication	6-8
Outline of the Steps for Configuring RADIUS Authentication	6-9
1. Configure Authentication for the Access Methods You Want RADIUS To Protect	6-10
2. Enable the (Optional) Access Privilege Option	6-12
3. Configure the Switch To Access a RADIUS Server	6-14
4. Configure the Switch's Global RADIUS Parameters	6-16
Local Authentication Process	6-20
Controlling Web Browser Interface Access	6-21
Configuring RADIUS Accounting	6-22
Operating Rules for RADIUS Accounting	6-23
Steps for Configuring RADIUS Accounting	6-24
1. Configure the Switch To Access a RADIUS Server	6-25
2. Configure Accounting Types and the Controls for Sending Reports to the RADIUS Server	6-26
3. (Optional) Configure Session Blocking and Interim Updating Options	6-28

Viewing RADIUS Statistics	6-29
General RADIUS Statistics	6-29
RADIUS Authentication Statistics	6-31
RADIUS Accounting Statistics	6-32
Changing RADIUS-Server Access Order	6-34
Messages Related to RADIUS Operation	6-36

7 Configuring RADIUS Server Support for Switch Services

Contents	7-1
Overview	7-2
Configuring a RADIUS Server To Specify Per-Port CoS and Rate-Limiting Services	7-3
Configuring the RADIUS Server	7-3
Viewing the Currently Active Per-Port CoS and Rate-Limiting Configuration Specified by a RADIUS Server	7-4
Configuring and Using RADIUS-Assigned Access Control Lists	7-7
Terminology	7-9
General Operation	7-11
How a RADIUS Server Applies a RADIUS-Based ACL to a Switch Port	7-11
The Packet-filtering Process	7-12
General Steps	7-17
Determining Traffic Policies	7-17
Planning the ACLs Needed To Enforce Designated Traffic Policies	7-19
Operating Rules for RADIUS-Based ACLs	7-20
Configuring an ACL in a RADIUS Server	7-22
Configuring the Switch To Support RADIUS-Based ACLs	7-26
Displaying the Current RADIUS-Based ACL Activity on the Switch	7-28
Event Log Messages	7-30
Causes of Client Deauthentication Immediately After Authenticating	7-31

8 Configuring Secure Socket Layer (SSL)

Contents	8-1
Overview	8-2
Terminology	8-3
Prerequisite for Using SSL	8-5
Steps for Configuring and Using SSL for Switch and Client Authentication	8-5
General Operating Rules and Notes	8-6
Configuring the Switch for SSL Operation	8-7
1. Assigning a Local Login (Operator) and Enable (Manager) Password	8-7
2. Generating the Switch's Server Host Certificate	8-8
To Generate or Erase the Switch's Server Certificate with the CLI	8-9
Comments on Certificate Fields	8-10
Generate a Self-Signed Host Certificate with the Web Browser Interface	8-12
Generate a CA-Signed server host certificate with the Web Browser Interface	8-15
3. Enabling SSL on the Switch and Anticipating SSL Browser Contact Behavior	8-17
Using the CLI interface to enable SSL	8-19
Using the web browser interface to enable SSL	8-19
Common Errors in SSL setup	8-21

9 Configuring Secure Shell (SSH)

Contents	9-1
Overview	9-2
Terminology	9-3
Prerequisite for Using SSH	9-5
Public Key Formats	9-5
Steps for Configuring and Using SSH for Switch and Client Authentication	9-6

General Operating Rules and Notes	9-8
Configuring the Switch for SSH Operation	9-9
1. Assigning a Local Login (Operator) and Enable (Manager) Password	9-9
2. Generating the Switch's Public and Private Key Pair	9-10
3. Providing the Switch's Public Key to Clients	9-12
4. Enabling SSH on the Switch and Anticipating SSH Client Contact Behavior	9-15
5. Configuring the Switch for SSH Authentication	9-18
6. Use an SSH Client To Access the Switch	9-21
Further Information on SSH Client Public-Key Authentication	9-22
Messages Related to SSH Operation	9-27

10 Traffic/Security Filters

Contents	10-1
Overview	10-2
Introduction	10-2
Filter Limits	10-3
Using Port Trunks with Filters	10-3
Filter Types and Operation	10-3
Source-Port Filters	10-4
Operating Rules for Source-Port Filters	10-4
Example	10-5
Named Source-Port Filters	10-6
Operating Rules for Named Source-Port Filters	10-6
Defining and Configuring Named Source-Port Filters	10-7
Viewing a Named Source-Port Filter	10-8
Using Named Source-Port Filters	10-8
Static Multicast Filters (5300xl Only)	10-14
Protocol Filters (5300xl Only)	10-16
Configuring Traffic/Security Filters	10-17
Configuring a Source-Port Traffic Filter	10-17
Example of Creating a Source-Port Filter	10-18
Configuring a Filter on a Port Trunk	10-19

Editing a Source-Port Filter	10-20
Configuring a Multicast or Protocol Traffic Filter (5300xl Switches Only)	10-21
Filter Indexing	10-22
Displaying Traffic/Security Filters	10-23

11 Configuring Port-Based and Client-Based Access Control (802.1X)

Contents	11-1
Overview	11-3
Why Use Port-Based or Client-Based Access Control?	11-3
General Features	11-3
User Authentication Methods	11-4
Terminology	11-5
General 802.1X Authenticator Operation	11-8
Example of the Authentication Process	11-8
VLAN Membership Priority	11-9
General Operating Rules and Notes	11-11
General Setup Procedure for Port-Based Access Control (802.1X)	11-13
Do These Steps Before You Configure 802.1X Operation	11-13
Overview: Configuring 802.1X Authentication on the Switch	11-13
Configuring Switch Ports as 802.1X Authenticators	11-15
1. Enable 802.1X Authentication on Selected Ports	11-15
3. Configure the 802.1X Authentication Method	11-19
4. Enter the RADIUS Host IP Address(es)	11-20
5. Enable 802.1X Authentication on the Switch	11-21
802.1X Open VLAN Mode	11-21
Introduction	11-21
VLAN Membership Priorities	11-22
Use Models for 802.1X Open VLAN Modes	11-23
Operating Rules for Authorized-Client and Unauthorized-Client VLANs	11-27
Setting Up and Configuring 802.1X Open VLAN Mode	11-31
802.1X Open VLAN Operating Notes	11-35

Option For Authenticator Ports: Configure Port-Security To Allow Only 802.1X-Authenticated Devices	11-36
Port-Security on 5300xl Switches Running Software Release E.09.xx or Greater	11-36
Port-Security on 3400cl and 6400cl Switches, and on 5300xl Switches Running Software Earlier than E.09.xx	11-37
Configuring Switch Ports To Operate As	
Supplicants for 802.1X Connections to Other Switches	11-38
Example	11-38
Supplicant Port Configuration	11-40
Displaying 802.1X Configuration, Statistics, and Counters	11-42
Show Commands for Port-Access Authenticator	11-42
Viewing 802.1X Open VLAN Mode Status	11-44
Show Commands for Port-Access Supplicant	11-49
How RADIUS/802.1X Authentication Affects VLAN Operation	11-50
Messages Related to 802.1X Operation	11-54

12 Configuring and Monitoring Port Security

Contents	12-1
Overview	12-3
Port Security	12-4
Basic Operation	12-4
Eavesdrop Protection (Series 5300xl Switches and Series 4200vl Switches)	12-5
Blocking Unauthorized Traffic	12-6
Trunk Group Exclusion	12-7
Planning Port Security	12-7
Port Security Command Options and Operation	12-8
Port Security Display Options	12-8
Configuring Port Security	12-12
Retention of Static Addresses	12-17
MAC Lockdown	12-22
Differences Between MAC Lockdown and Port Security	12-24
MAC Lockdown Operating Notes	12-25
Deploying MAC Lockdown	12-26

MAC Lockout	12-30
Port Security and MAC Lockout	12-32
Web: Displaying and Configuring Port Security Features	12-33
Reading Intrusion Alerts and Resetting Alert Flags	12-33
Notice of Security Violations	12-33
How the Intrusion Log Operates	12-34
Keeping the Intrusion Log Current by Resetting Alert Flags	12-35
Menu: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags	12-36
CLI: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags	12-38
Using the Event Log To Find Intrusion Alerts	12-40
Web: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags	12-41
Operating Notes for Port Security	12-41

13 Using Authorized IP Managers

Contents	13-1
Overview	13-2
Options	13-3
Access Levels	13-3
Defining Authorized Management Stations	13-4
Overview of IP Mask Operation	13-4
Menu: Viewing and Configuring IP Authorized Managers	13-5
CLI: Viewing and Configuring Authorized IP Managers	13-6
Listing the Switch's Current Authorized IP Manager(s)	13-6
Configuring IP Authorized Managers for the Switch	13-7
Web: Configuring IP Authorized Managers	13-9

Building IP Masks	13-9
Configuring One Station Per Authorized Manager IP Entry	13-9
Configuring Multiple Stations Per Authorized Manager IP Entry ..	13-10
Additional Examples for Authorizing Multiple Stations	13-11
Operating Notes	13-12

Index