Part No. 314724-C Rev 00
May 2004

4655 Great America Parkway
Santa Clara, CA 95054

Configuring and Managing Security

Passport 8000 Series Software Release 3.7

NORTEL NETWORKS™

Copyright © 2004 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and PASSPORT are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Figures

Tables

Preface

This guide describes the security features of the Passport 8000 Series switch and how to start and customize security services on a Nortel Networks* switch. It provides information on using the Device Manager graphical user interface (GUI) as well as the command line interface (CLI) to configure security services on a switch.

Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, Ethernet bridging, and IP routing
- Familiarity with networking concepts and terminology
- Experience with windowing systems or GUIs
- Basic knowledge of network topologies

Before using this guide, you must complete the following procedures. For a new switch:

- Install the switch (see the installation guide that came with your switch).
- Connect the switch to the network (see *Getting Started* for more information).

Make sure that you are running the latest version of Nortel Networks* Passport 8000 Series Switch and Device Manager software. For information about upgrading the Passport 8000 Series switch and Device Manager, see *Release Notes for the Passport 8000 Series Switch Release 3.7* and *Installing and Using Device Manager*, respectively.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `ping <ip_address>`, you enter `ping 192.32.10.12`
`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`info`** command. Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you must enter either `show ip alerts` or `show ip routes`, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is `ethernet/2/1 [<parameter> <value>]...`, you enter `ethernet/2/1` and as many parameter-value pairs as needed.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is `show at <valid_route>`, *`valid_route`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP command on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

Acronyms

This guide uses the following acronyms:

BSAC	Bay Secure Access Control
CLI	Command Line Interface
DNS	Domain Name Server
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
MIB	Management Information Base
PDU	Power Distrubution Unit
RADIUS	Remote Access Dial-In User Services

SNMP	Simple Network Management Protocol
SSH	Secure Shell
USM	User-based Security Model
VACM	View-based Access Control

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

A list of related publications for this manual can be found in the release notes that came with your software.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
Security features

This section describes the security features that allow you to restrict access to the switch. Network managers have restricted access to the *control path*; users have restricted access to the *data path*.

You protect the control path using:

- Login and passwords
- Access policies, which allow you to specify the network/address that is allowed to use a service/daemon
- Secure protocols (for example, Secure Shell [SSH], Secure Copy [SCP], or SNMPv3)
- MD5 in combination with OSPF or BGP (routing protocol updates)

You protect the data path using:

- MAC address filtering (source and/or destination)
- Layer 3 filtering (for example, IP, UDP/TCP filtering)
- Routing policies, which prevents users from accessing restricted areas of the network
- Mechanisms to prevent DOS (Denial of Service) attacks

You can use the command line interface (CLI) to set up passwords and community strings for access to all the management functions of the switch.

This manual does not include all security features available with the Passport 8000 Series software. The following table lists additional security features and the manuals where the documentation for these features can be found:

Security Feature	Manual
IP filters	*Configuring IP Routing Operations — Phase 1* and *Configuring IP Routing Operations — Phase 1*
IP route policies	*Configuring IP Routing Operations — Phase 1* and *Configuring IP Routing Operations — Phase 1*
DVMRP route policies	*Configuring IP Multicast Routing Protocols*
IPX route policies	*Configuring IPX Routing Operations*
route update protection (MD5)	*Configuring IP Routing Operations*
IGAP	*Configuring IGMP for User Authentication (IGAP)*

Note: When issuing a CLI command that is not supported on the slave CPU, the message `command not allowed on slave` will appear for each unsupported CLI command.

CLI passwords

The Passport 8000 Series switch is shipped with default passwords set for access to the CLI through a console or telnet session.

Caution: Please be aware that the default passwords/community strings are documented and well known. Nortel Networks strongly recommends that you change the default passwords/community strings immediately after the first login.

Note: For security purposes, if you fail to login correctly on the master CPU in three consecutive instances, the CPU locks for 60 seconds.

Port lock feature

The Port Lock feature allows you to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. Locked ports cannot be modified in any way until the port is first unlocked. For instructions on locking ports, see Chapter 2.

High secure bootconfig flag

The Passport 8000 Series switch supports the flag, **`hsecure`** (for High Secure), which you configure in bootconfig mode.

When the bootconfig flag, **`hsecure`**, is enabled, the software enforces the 8 characters rule for all passwords. When upgrading from a previous release, if the password does not have at least 8 characters, you will be prompted to change your password to the mandatory character length.

Access policies for services

You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the switch through various access services, such as Telnet, SNMP, HTTP, rlogin, or SSH.

Note: To access the backup CPU using the **`peer rlogin`** command, you must also set an access policy that enables rlogin access to the backup CPU. For information about the **`peer rlogin`** command, see the publication, *Getting Started.*

For information about enabling access services for a specific policy using the CLI, see “Enabling an access service” on page 83.

You can define network stations that are explicitly allowed to access the switch or network stations explicitly forbidden to access the switch. For each service you can also specify the level of access, such as read-only or read/write/all.

When you set up access policies, you can either:

- Globally enable the access policy feature, and then create and enable individual policies. Each policy takes effect immediately when you enable it.
- Create and enable individual access policies, and then globally enable the access policy feature to activate all the policies at the same time.

SNMP version 3 (SNMPv3)

The Simple Network Management Protocol (SNMP) allows you to remotely collect management data and configure devices. An SNMP agent is a software process that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to either retrieve or modify.

For information on configuring SNMPv3 using the CLI or Device Manager, see Chapter 6 and Chapter 7, respectively. For instructions on upgrading SNMP from the Passport 8000 Series Switch Release 3.3 to 3.7, or from Release 3.5 to 3.7, see *Release Notes for the Passport 8000 Series Switch Software 3.7*.

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

- New SNMP message formats
- Security for messages
- Access control
- Remote configuration of SNMP parameters

An SNMP entity is an implementation of this architecture. Each such SNMP entity consists of an SNMP engine and one or more associated applications. The following figure shows details about an SNMP entity and the components within it. SNMPv3 provides a means of security to the SNMP framework by supporting the following:

- Security for Messages
- Access Control
- Remote configuration of SNMP parameters
- New SNMP message format

SNMP engine

An SNMP engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one-to-one association between an SNMP engine and the SNMP entity, which contains it.

snmpEngineID

Within an administrative domain, an snmpEngineID is the unique identifier of an SNMP engine. Since there is a one-to-one association between SNMP engines and SNMP entities, the ID also uniquely and unambiguously identifies the SNMP entity within that administrative domain. The snmpEngineID is generated during the boot processing. The SNMP engine contains a:

- Dispatcher
- Message Processing Subsystem
- Security Subsystem
- Access Control Subsystem

Dispatcher

There is one dispatcher in an SNMP engine. It allows for concurrent support of multiple versions of SNMP messages in the SNMP engine. It does so by:

- Sending and receiving SNMP messages to/from the network
- Determining the SNMP message version and interacting with the corresponding message processing model
- Providing an abstract interface to SNMP applications for delivery of a PDU to an application
- Providing an abstract interface for SNMP applications that allows them to send a PDU to a remote SNMP entity.

Message processing

The Message Processing subsystem prepares messages for sending and extracts data from received messages. The subsystem can contain multiple message processing models.

Security

Authentication

Authentication within the User-based Security Model (USM) allows the recipient of a message to verify the message sender and whether the message has been altered. If authentication is used, the integrity of the message is verified. The authentication protocols supported using USM is HMAC-MD5 and HMAC-SHA-96.

Privacy

The USM is an encryption Protocol for privacy. Only the data portion of a message is encrypted, the header and the security parameters are not. The privacy protocol supported using the USM is CBC-DES Symmetric Encryption Protocol.

Security

SNMPv3 security protects against the following:

- Modification of information — protects against altering information in transit
- Masquerade — protects against an unauthorized entity assuming the identity of an authorized entity
- Message Stream Modification — protection against delaying or replaying messages
- Disclosure — protects against eavesdropping
- Discovery procedure — finds the SnmpEngineID of a SNMP entity for a given transport address or transport endpoint address.
- Time synchronization procedure— facilitates authenticated communication between entities

SNMPv3 does not protect against:

- Denial of service — prevention of exchanges between manager and agent
- Traffic analysis — general pattern of traffic between managers and agents

Access control

User-based Security Model (USM)

In a USM system, the security model uses a defined set of user identities for any authorized user on a particular SNMP engine. The user with authority on one SNMP engine must also have authorization on any SNMP engine with which the original SNMP engine communicates.

The USM security model provides the following levels of communication:

- NoAuthNoPriv

  Communication without authentication and privacy

- AuthNoPriv

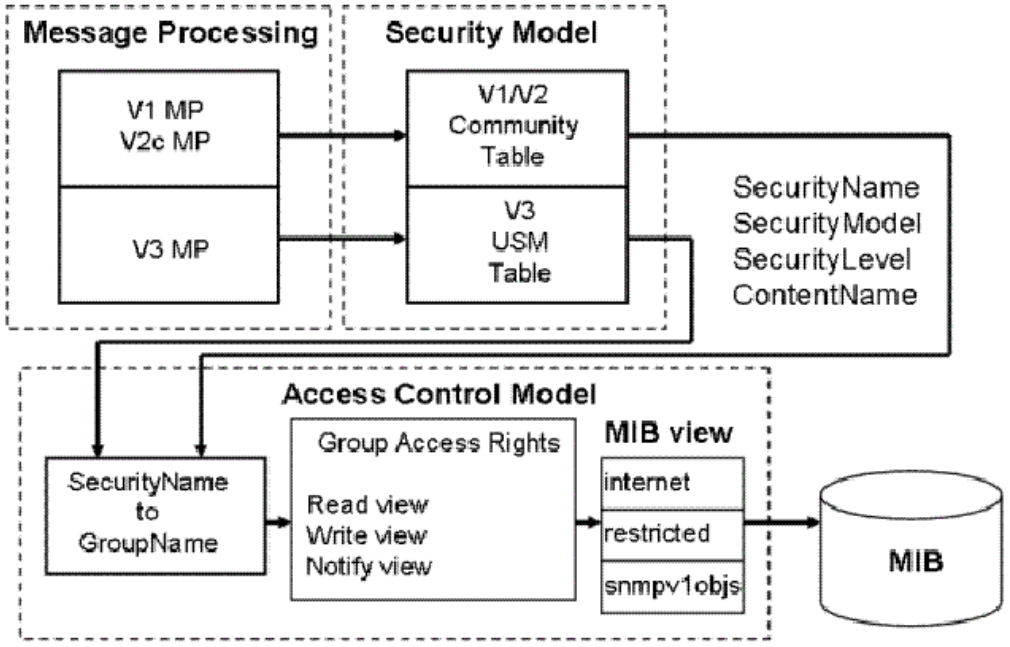
  Communication with authentication and without privacy

- AuthPriv

  Communication with authentication and privacy

Figure 1 shows the relationship between USM and View-based Access Control (VACM).

Figure 1 USM association with VACM



View-based Access Control (VACM)

VACM provides groups access, group security levels, and context based on a predefined subset of MIB objects. These MIB objects define a set of managed objects and instances.

VACM is the standard access control mechanism that provides:

- Authorization service to control access to MIB objects at the PDU level
- Alternative access control subsystems

The access is based on principal, security level, MIB context, object instance, and type of access requested (read/write). VACM MIB defines the policy and allows remote management.

SNMPv3 agent support for RFC compliance

The SNMPv3 agent engine code (Envoy 9.3) for the Passport 8600 switch provides full compliance with the following RFCs:

- RFC 2571
- RFC 2572
- RFC 2573
- RFC 2574
- RFC 2575
- RFC 2576

Trap notifications

You configure traps by creating SNMPv3 trap notifications, creating a target address to which you want to send the notifications, and specifying target parameters. Nortel Networks provides two default entries in the notify table: Inform and Trap. The tag values for these entries are informTag and trapTag, respectively. For more information about configuring traps using release 3.7, see *Release Notes for the Passport 8000 Series Switch Software 3.7*.

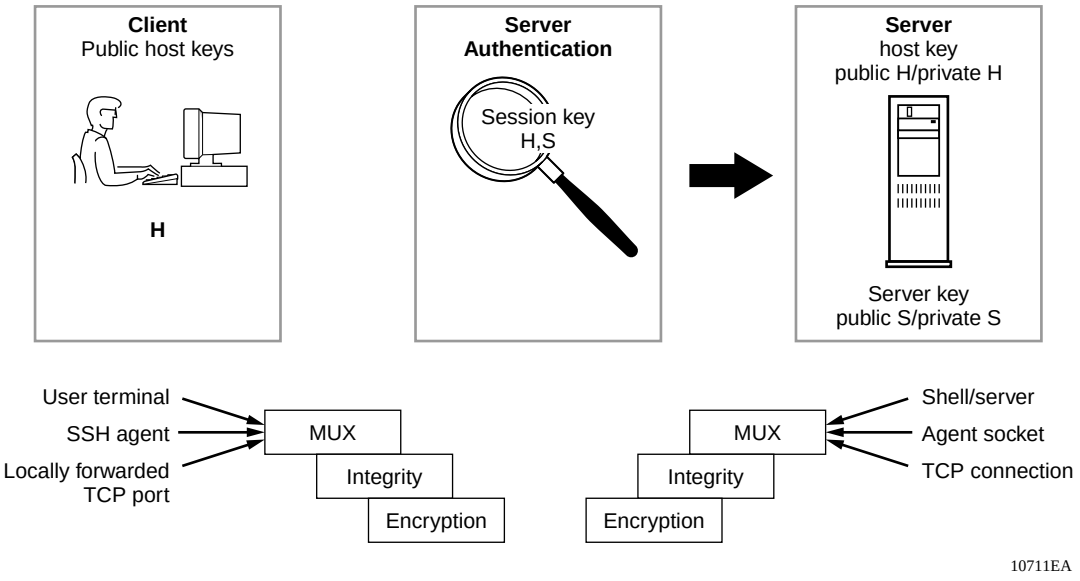
Secure Shell (SSH)

Secure Shell (SSH) is a client/server protocol that specifies the way to conduct secure communications over a network. Secure CoPy (SCP) is a secure file transfer protocol. When using other methods of remote access, such as Telnet or FTP, the traffic generated by these utilities is not encrypted. Anyone that can see the network traffic can see all data, including passwords and user names. SSH can replace Telnet and other remote logon utilities. SCP can replace FTP with an encrypted alternative.

SSH supports a variety of the many different public/private key encryption schemes available. Using the public key of the host server, the client and server negotiate to generate a session key known only to the client and the server. This one-time key is then used to encrypt all traffic between the client and the server.

Figure 2 gives an overview of the SSH protocol.

Figure 2 Overview of the SSH protocol



Using a combination of host, server, and session keys, the SSH protocol can provide strong authentication and secure communication over an unsecure network, offering protection from the following security risks:

- IP Spoofing
- IP source routing
- DNS spoofing
- Man-in-the-middle/TCP hijacking attacks
- Eavesdropping/Password sniffing

Even if network security is compromised, traffic cannot be played back or decrypted, and the connection cannot be hijacked.

The secure channel of communication provided by SSH does not provide protection against break-in attempts or denial-of-service (DoS) attacks.

The SSH protocol supports the following security features:

- Authentication. This determines in a reliable way to identify the SSH client. During the login process the SSH client is queried for a digital proof of identity.

  Supported authentications are RSA (SSH-1), DSA (SSH-2) and passwords (both SSH-1 and SSH-2).

- Encryption. The SSH server uses encryption algorithms to scramble data and rendered it unintelligible except to the receiver.

  Supported encryption is 3DES only.

- Integrity. This guarantees that the data is transmitted from the sender to the receiver without any alteration. If any third party captures and modifies the traffic, the SSH server will detect this alteration.

Note: Currently 3DES is the only encryption algorithm supported for the Passport 8000 Series switch. Due to export restrictions, the encryption capability has been separated from the main image. Refer to the release notes accompanying your software release for the latest information on how to download the 3DES encryption image. The SSH server will not function properly without the use of this image.

The implementation of the SSH server in the Passport 8000 Series switch enables the SSH client to make a secure connection to a Passport 8000 Series switch and will work with commercially available SSH clients.

Note: You must use CLI to initially configure SSH. You can use Device Manager to change the SSH configuration parameters. However, Nortel Networks recommends using CLI. Nortel Networks also recommends using the console port to configure the SSH parameters.

SSH version 2 (SSH-2)

SSH protocol, version 2 (SSH-2) is a complete rewrite of the SSH-1 protocol. While SSH-1 contains multiple functions in a single protocol, in SSH-2 the functions are divided among three layers:

- SSH Transport Layer (SSH-TRANS)

  The SSH transport layer manages the server authentication and provides the initial connection between the client and the server. Once established, the transport layer provides a secure, full-duplex connection between the client and server.

- SSH Authentication Protocol (SSH-AUTH)

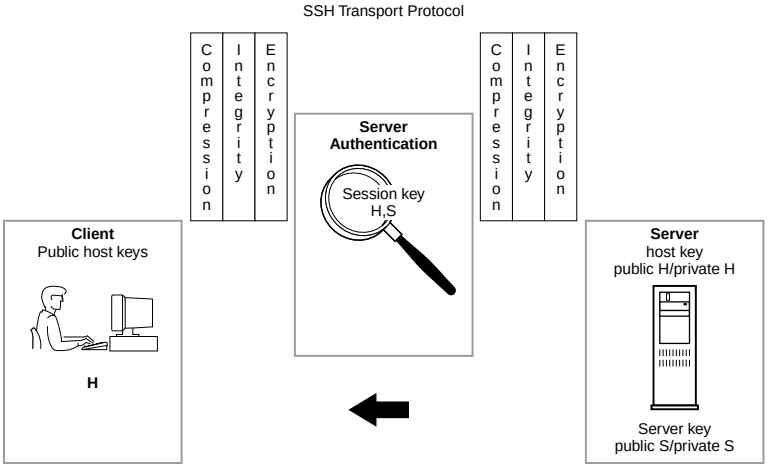
  The SSH authentication protocol runs on top of the SSH transport layer and authenticates the client-side user to the server. SSH-AUTH defines three authentication methods; public key, host-based, and password. SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- SSH Connection Protocol (SSH-CONN)

  The SSH connection protocol runs on top of the SSH transport layer and user authentication protocols. SSH-CONN provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. These richer services are multiplexed into the single encrypted tunnel provided by the SSH transport layer.

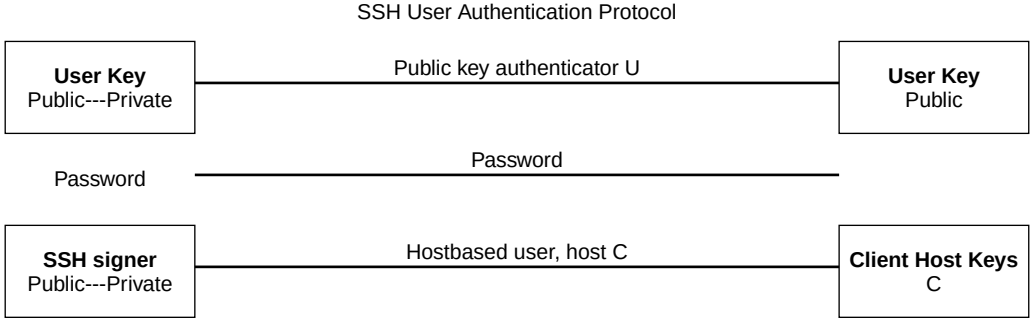
Figure 3 shows separate SSH version 2 protocols. Figure 4 shows SSH user authentication protocol. Figure 5 shows SSH connection protocol.

Figure 3 Separate SSH version 2 protocols



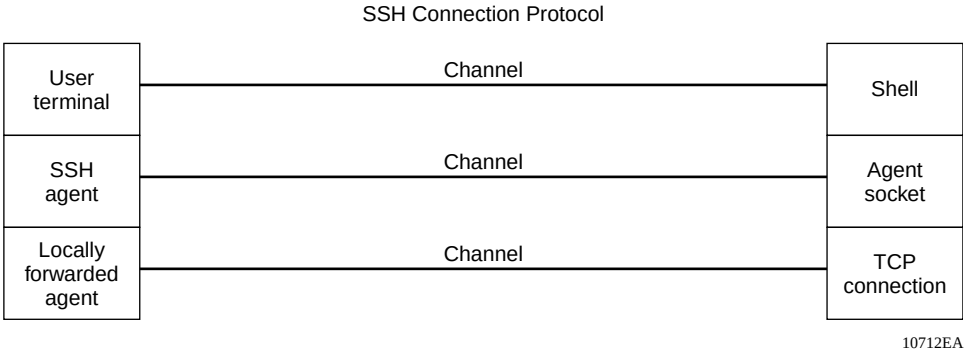
10714EA

Figure 4 SSH User Authentication Protocol



10713EA

Figure 5 SSH Connection Protocol



The modular approach of SSH-2 improves on the security, performance, and portability of the SSH-1 protocol.

Note: The SSH-1 and SSH-2 protocols are not compatible. While the SSH implementation in the Passport 8000 Series switch supports both versions of SSH, Nortel Networks recommends use of the more secure version, the SSH-2 protocol.

SSH guidelines

Key generation and removal

Generating keys requires that you have free space on the flash. A typical configuration requires less than 2KB of free space. Before you generate a key, verify that you have sufficient space on the flash, using the `dir` command. If the flash is full when you attempt to generate a key, an error message appears and the key is not generated. You will have to delete some unused files and re-generate the key.

If you remove only the public keys, enabling the SSH will not create new ones.

Block SNMP

The boot flag setting for block-snmp (`config bootconfig flags block-snmp <true|false>`) and the runtime config SSH secure (`config sys set ssh enable <true|false|secure>`) each modify the block-snmp boot flag. If you are enabling SSH secure, the block-snmp boot flag is modified to true and the change takes effect after reboot. To set the block-snmp boot flag to false, disable SSH secure mode first.

SSH server support

The SSH server is not supported on the Passport 8100 switch module.

SCP command

Nortel Networks recommends using short filenames with the **`SCP`** command. The entire **`SCP`** command, including all options, usernames, and filenames should NEVER exceed 80 characters.

Remote Access Dial-In User Services (RADIUS)

Remote Access Dial-In User Services (RADIUS) is a distributed client/server system that assists in securing networks against unauthorized access, allowing a number of communication servers and clients to authenticate users identity through a central database. The database within the RADIUS server stores information about clients, users, passwords, and access privileges including the use of “shared secret.”

RADIUS is a fully open and standard protocol, defined by RFCs (Authentication: 2865, Accounting 2866). In the Passport 8000 Series switch, you use RADIUS authentication and accounting to:

- Secure access to the switch (console/Telnet)
- Track the management sessions (CLI only) using RADIUS accounting

This section includes the following topics:

How RADIUS works

A RADIUS application has two components:

- RADIUS server

  A computer equipped with server software (for example, a UNIX* workstation) that is located at a central office or campus. It has authentication and access information in a form that is compatible with the client. Typically, the database in the RADIUS server stores client information, user information, password, and access privileges, including the use of "shared secret." A network can have one server for both authentication and accounting, or one server for each service.

- RADIUS client

  Can be a switch, router or a remote access server, equipped with client software, that typically resides on the same local area network (LAN) segment as the server. The client is the network access point between the remote users and the server.

The two RADIUS processes are:

- RADIUS authentication

  Lets you identify remote users before you give them access to a central network site.

- RADIUS accounting

  Enables data collection on the server during a remote user's dial-in session with the client.

Configuring the RADIUS server

The Passport 8600 software supports BaySecure Access Control (BSAC*), Merit Network, and freeRadius servers. For instructions on installing the BSAC, Merit Network, or freeRadius server software on the server that you will use, see the installation manual that came with your software. After the software is installed, you must make changes to one or more configuration files for these servers. For detailed information about the changes that must be made for the BSAC, Merit Network, or freeRadius server, see Chapter 10.

After you have installed the software, you must configure the RADIUS server to respond to each of its clients. Make sure that the RADIUS server will reach the client by pinging the IP address of the client. If the server's IP interface can successfully ping the client, the server can provide authentication to that client.

You must add user names ro, L1, L2, L3, rw, and rwa to the RADIUS server if authentication is enabled. Users not added to the server will be denied access. In addition to the user names, ro, L1, L2, L3, rw, and rwa, you can create additional user names to access the switch. You assign an access priority to an individual user. These access priorities, which range from Non-Access to Read-Write-All-Access, determine a user's access level. The RADIUS server authenticates the user name and access priority that is assigned to that name.

For detailed instructions on configuring a RADIUS server, including adding clients and adding users and access priorities, refer to the documentation that came with the server software.

You should configure at least two RADIUS servers in the network to provide redundancy. A maximum of ten RADIUS servers is allowed in a single network. Each server is assigned a priority and is contacted in that order.

Configuring the RADIUS client

You use the Passport 8600 CLI, the NNCLI, or Device Manager to configure the RADIUS client so that it can contact its RADIUS server. To configure the client, you must:

- Enable RADIUS.
- Configure the IP address of the RADIUS server to be used.

- Configure the shared secret. This secret must match the one defined in the RADIUS server.
- Configure the access priority attribute value. This value must match the type value set in the dictionary file on the RADIUS server. The default value, 192, is the recommended value.
- Configure the order or priority in which the RADIUS server will be used (if you have more than one RADIUS server in the network).
- Set the UDP port that will be used by the client and the server during the authentication process. The UDP port between the client and the server must have the same value. For example, if the server is configured with UDP 1812, then the client must use the same UDP port value.

RADIUS authentication

RADIUS authentication allows a remote server to authenticate logins. The RADIUS server also provides access authority. RADIUS assists network security and authorization by managing a database of users. Use of the database allows the switch to verify user names and passwords as well as information about the type of access priority available to the user.

When the RADIUS client sends an authentication request, if the RADIUS server requires additional information, such as a SecurID number, it sends a *challenge-response*. Along with the challenge-response, a reply-message attribute is sent. The reply-message is a text string, such as “Please enter the next number on your SecurID card:”. The maximum length of each reply-message attribute is 253 characters (as defined by the RFC). If you have multiple instances of reply-message attributes that together form a large message that can be displayed to the user, the maximum length is 2000 characters.

Features of the RADIUS software include:

- Additional user names

  Additional user names can be used to access the switch, in addition to the six existing user names of ro, L1, L2, L3, rw, and rwa. The RADIUS server authenticates the user name and assigns one of the existing access priorities to that name. Unauthenticated user names are denied access to the switch.

Note: User names ro, L1, L2, L3, rw, and rwa must be added to the RADIUS server if authentication is enabled. Users not added to the server will be denied access.

- User configurable
  - — Up to 10 RADIUS servers in each switch for fault tolerance (each server is assigned a priority and is contacted in that order)
  - — A secret key for each server to authenticate the RADIUS client
  - — The server's UDP port
  - — Maximum retries allowed
  - — Time-out period for each attempt

RADIUS accounting

RADIUS accounting logs all of the activity of each remote user in a session on the centralized RADIUS accounting server.

Session-IDs for each RADIUS account are generated as 12-character strings. The first 4 characters in the string form a random number in hexadecimal format. The last 8 characters in the string indicate the number of user sessions started since reboot in hexadecimal format.

The NAS IP Address for a session is the address of the switch interface to which the remote session is connected over the network. For a console session, modem session, and sessions running on debug ports, this value is set to 0.0.0.0 as is done with RADIUS authentication.

Table 1 summarizes events and associated accounting information logged at the RADIUS accounting server.

Table 1 Accounting events and logged information

Event	Accounting information logged at server
Accounting is turned on at router	• Accounting on request: Network Access Server (NAS) • IP address.
Accounting is turned off at router	• Accounting off request: NAS IP address.
User logs in	• Accounting start request: NAS IP address • Session Id • User Name
More than 40 CLI commands are executed	• Accounting Interim request: NAS IP address • Session Id • CLI commands • User Name
User logs off	• Accounting Stop request: NAS IP Address • Session Id • Session duration • User Name • number of input octets for session • number of octets output for session • number of packets input for session • number of packets output for session • CLI commands

When the switch communicates with the RADIUS accounting server, the following actions are taken:

1. If the server sends an invalid response, the response is silently discarded and no attempt is made to resend the request.
2. If the server does not respond within the user-configured time-out interval, a user-specified number of attempts is made. If a server does not respond to any of the retries, requests are sent to the next priority server (if configured). You can configure up to 10 RADIUS servers for redundancy.

Extensible Authentication Protocol over LAN (EAPoL)

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access control protocol. EAPoL provides security in that it prevents users from accessing network resources before they are authenticated. Without this authentication, users could access a network to assume a valid identity and access confidential material or launch denial of service attacks.

EAPoL allows you to set up network access control on internal LANs and to exchange authentication information between any end station or server connected to the Passport 8000 Series switch and an authentication server (such as a RADIUS server). This security feature extends the benefits of remote authentication to internal LAN clients. For example, if a new client PC fails the authentication process, EAPoL prevents it from accessing the network.

Note: In the 3.7 release, the Passport 8600 supports only one EAP supplicant per port. If the switch receives frames from different MAC addresses on the same port, that port will be disabled. Nortel Networks is currently working on a solution to support multiple supplicants. Please contact your local representative for more information. For a list of EAPoL configuration limitations, see "EAPoL configuration limitations" on page 48.

This section includes the following topics:

EAPoL terminology

Some components and terms used with EAPoL-based security are:

- **Supplicant** — a device, such as a PC, that applies for access to the network.
- **Authenticator** — software on the Passport 8000 Series switch that authorizes or rejects a Supplicant attached to the other end of a LAN segment.
  - **Port Access Entity (PAE)** — software that controls each port on the switch. The PAE, which resides on the Passport 8000 Series switch, supports the Authenticator functionality.
  - **Controlled Port** — any port on the switch with EAPoL enabled.
- **Authentication Server** — a RADIUS server that provides authorization services to the Authenticator.

Configuration process

The Authenticator facilitates the authentication exchanges that occur between the Supplicant and the Authentication Server. The Authenticator PAE encapsulates the EAPoL message into a RADIUS packet and then sends the packet to the Authentication Server.

The Authenticator also determines each controlled port's operational state. At system initialization, or when a Supplicant initially connects to one of the switch's controlled ports, the controlled port's state is set to Blocking. After the Authentication Server notifies the Authenticator PAE about the success or failure of the authentication, the Authenticator changes the controlled port's operational state accordingly.

The Passport 8000 Series switch transmits and receives EAPoL frames regardless of whether the port is authorized or unauthorized. Non-EAPoL frames are transmitted according to the rules below:

- If authentication succeeds, the controlled port's operational state is set to Forwarding. This means that all the incoming and outgoing traffic is allowed through the port.
- If authentication fails, the controlled port forwards traffic according to how you configure the port's traffic control. The traffic control command can have one of the following two values:

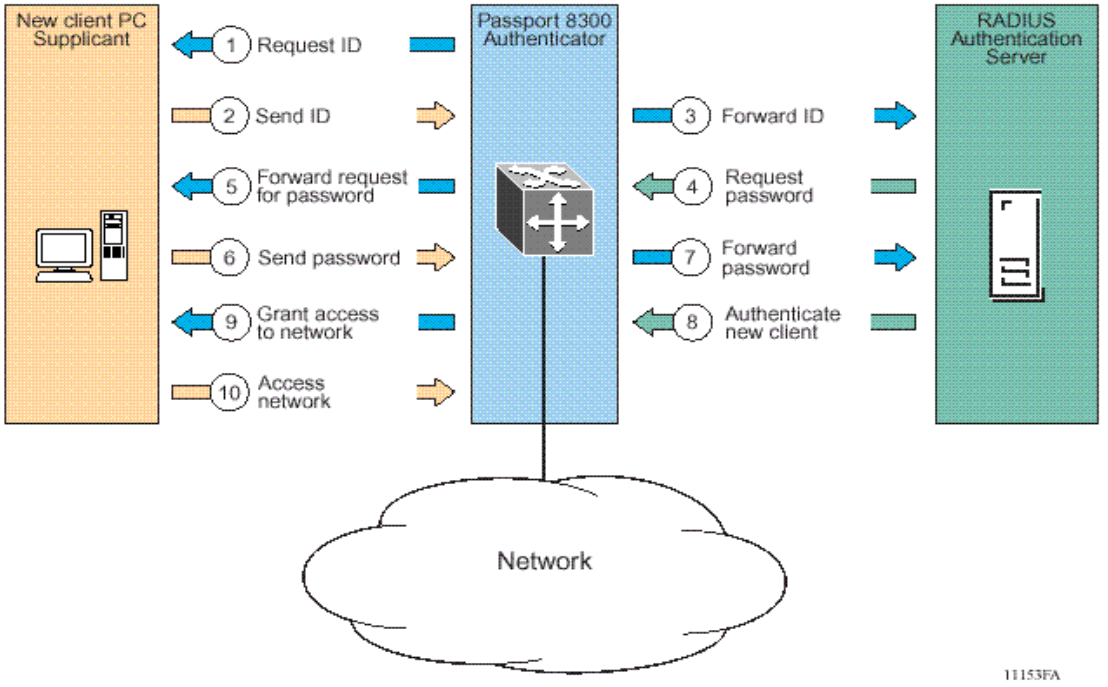
— Incoming and Outgoing—All non-EAPoL frames received on the controlled port are discarded, and the controlled port's state is set to Blocking.

— Incoming—All non-EAPoL frames received on the port are discarded, but transmit frames are forwarded through the port.

Configuration example

Figure 6 illustrates how the Passport 8000 Series switch, configured with EAPoL, reacts to a new network connection.

Figure 6 EAPoL configuration example



In the above example, the Passport 8000 Series switch uses the following steps to authenticate a new client:

1 The Passport 8000 Series switch detects a new connection on one of its EAPoL-enabled ports and requests a user ID from the new client PC.

2 The new client sends its user ID to the switch.

3 The switch uses RADIUS to forward the user ID to the RADIUS server.

4 The RADIUS server responds with a request for the user's password.

5 The switch forwards the RADIUS server's request to the new client.

6 The new client sends an encrypted password to the switch, within the EAPoL packet.

7 The switch forwards the EAPoL packet to the RADIUS server.

8 The RADIUS server authenticates the password.

9 The switch grants the new client access to the network.

10 The new client accesses the network.

Note: If the RADIUS server cannot authenticate the new client, it denies the new client access to the network.

EAPoL configuration limitations

The following limitations apply for configuring EAPoL on a port:

- EAPoL cannot be enabled on tagged ports.
- EAPoL cannot be enabled on ports belonging to an MLT group.
- Tagging cannot be enabled on EAPoL enabled ports.
- EAPoL enabled ports can not be added to an MLT group.

EAPoL dynamic VLAN assignment

If RADIUS server is configured to send VLAN Id in Access-Accept response, the EAPoL feature dynamically changes the port's VLAN configuration by moving it to the VLAN specified.

The following VLAN configuration values are affected:

- Port membership
- Port priority

When EAPoL is disabled on a port that was previously authorized, the port's VLAN configuration values are restored directly from the switch's non-volatile random access memory (NVRAM).

The following exception applies to dynamic VLAN assignments:

- The dynamic VLAN configuration values assigned by EAPoL are **not** stored in the switch's NVRAM.

You set up your Authentication Server (RADIUS server) for EAPoL dynamic VLAN assignments. The Authentication Server allows you to configure user-specific settings for VLAN memberships and port priority.

When you log on to a system that has been configured for EAPoL authentication, the Authentication Server recognizes your user ID and notifies the switch to assign preconfigured (user-specific) VLAN membership and port priorities to the switch. The configuration settings are based on configuration parameters that were customized for your user ID and previously stored on the Authentication Server.

RADIUS configuration prerequisites for EAPoL

The RADIUS server should be connected to a force-authorized port. This ensures that the port is always available and not tied to whether or not the switch is EAPoL-enabled. To set up the Authentication Server, set the following "Return List" attributes for all user configurations (refer to your Authentication Server documentation):

- VLAN membership attributes
  - Tunnel-Type: value 13, Tunnel-Type-VLAN
  - Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
  - Tunnel-Private-Group-Id: ASCII value 1 to 4094 (this value is used to identify the specified VLAN).

- Port priority (vendor-specific) attributes
  - — Vendor Id: value 562, Nortel Vendor Id and value 1584, Bay Networks Vendor Id
  - — Attribute Number: value 1, Port Priority
  - — Attribute Value: value 0 (zero) to 7 (this value is used to indicate the port priority value assigned to the specified user)

Note: You need to configure these attributes, only if Dynamic VLAN membership or Dynamic Port priority is required.

RADIUS accounting for EAPoL

Passport 8600 provides the ability to account EAPoL sessions using RADIUS accounting protocol. A user session is defined as the interval between the instance at which a user is successfully authenticated (port moves to authorized state) and the instance at which the port moves out of the authorized state.

Table 2 summarizes the accounting events and information logged.

Table 2 Summary of accounting events and information logged.

Event	Radius Attributes	Description
User is authenticated by EAPoL and port enters authorized state	Acct-Status-Type	start
	Nas-IP-Address	IP address to represent passport 8600
	Nas-Port	Port number on which the user is EAPoL authorized
	Acct-Session-Id	Unique string representing the session
	User-Name	EAPoL user name
User logs off and port enters un-authorized state	Acct-Status-Type	stop
	Nas-IP-Address	IP address to represent passport 8600
	Nas-Port	Port number on which the user is EAPoL un-authorized
	Acct-Session-Id	Unique string representing the session
	User-Name	EAPoL user name
	Acct-Input-Octets	Number of octets input to the port during the session
	Acct-Output-Octets	Number of octets output to the port during the session
	Acct-Terminate-Cause	Reason for terminating user session. Please see Table 3 for the mapping of 802.1x session termination cause to RADIUS accounting attribute.
	Acct-Session-Time	Session interval

Table 3 describes the mapping of 802.1x session termination cause to RADIUS accounting attribute.

Table 3 802.1x session termination mapping

IEEE 802.1X dot1xAuthSessionTerminateCause Value	RADIUS Acct-Terminate-Cause Value
supplicantLogoff(1)	User Request (1)
portFailure(2)	Lost Carrier (2)
supplicantRestart(3)	Supplicant Restart (19)
reauthFailed(4)	Reauthentication Failure (20)
authControlForceUnauth(5)	Admin Reset (6)
portReInit(6)	Port Reinitialized (21)
portAdminDisabled(7)	Port Administratively Disabled (22)
notTerminatedYet(999)	N/A

System requirements

The following are minimum system requirements for EAPoL:

- Passport 8000 Series switch running software release 3.7 or later
- RADIUS server (Microsoft Windows 2000 IAS server)
- Client software that supports EAPoL (Microsoft Windows XP Client)

You must specify the Microsoft 2000 IAS server (or any generic RADIUS server that supports EAP) as the primary RADIUS server for these devices. You must also configure your switch for VLANs and EAPoL security.

User-based policy support

You can set up a user-based policy (UBP) system, using Optivity Policy Services (OPS), a RADIUS server, and a Passport 8000 Series switch with EAP enabled.

Optivity Policy Services (OPS) is an application designed to manage the traffic prioritization and network access security for business applications. It provides centralized control of advanced packet classification and the ability to priority mark, police, meter, or block traffic.

OPS 4.0 supports user-based policies (UBP), which allow security administrators to establish and enforce roles and conditions on a per-user basis for any access port in the network. The UBP feature in Optivity Policy Services works in conjunction with Extensible Access Protocol (EAP) technology to enhance the security of the network. Users log in to the networks and are authenticated as the network connection is established.

The UBP feature works as an extension to the Roles feature in OPS. In a UBP environment, role objects are linked directly to specific users (as RADIUS attributes), as opposed to being linked simply to device interfaces. The role object then links the user to specific policies that control the user's access to the network.

When a user is successfully authenticated by the RADIUS server, the switch sends an EAP session start event to the OPS policy server. The policy server then sends user-based policy configuration information for the new user roles to the interface, based on the role attribute that was assigned to that user on the RADIUS server.

Configuring the Passport 8600 for EAP and RADIUS

The Passport 8600 switch through which UBP users will connect must be configured to communicate with the RADIUS server to exchange EAP authentication information, as well as user role information. You must specify the IP address of the RADIUS server, as well as the "shared secret" (a password that authenticates the device with the RADIUS server as an EAP access point). EAP must be enabled globally on each device, and EAP authentication settings must be set on each device port through which EAP/UBP users will connect.

Use the following procedure to set up the Passport 8600 for EAP and RADIUS:

1. Using the CLI, open a Telnet session and log in to the Passport 8600 switch.
2. To create a RADIUS server that will be used by EAPoL, enter the following command:

   ```
   config radius server create <IPaddr> secret <secretkey>
   usedby eapol
   ```

where:

— *IPaddr* is the IP address of your RADIUS server. This address tells the switch where to find the RADIUS server from which it will obtain EAP authentication and user role information.

— *secretkey* is the shared secret for RADIUS authentication. The shared secret is held in common by the RADIUS server and all EAP-enabled devices in your network. It authenticates each device with the RADIUS server as an EAP access point. When you configure your RADIUS server, you will need to use the same shared secret value as you used here.

3 To enable the switch to communicate through EAP, and to globally enable session management, enter the following commands:

```
config sys set eapol enable
config sys set eapol sess-manage true
```

Note: When OPS learns interfaces on the switch, it sets the `config ethernet slot/port sess-manage-mode` command to `true` on individual interfaces.

4 To enable switch ports for EAP authentication, enter the following commands:

```
config ethernet <slot/port> eapol admin-status auto
config ethernet <slot/port> eapol reauthentication true
```

5 To save your changes, enter the following command:

```
save
```

For more information about configuring RADIUS and EAP for the Passport 8000 Series switch, see the appropriate chapters in this manual.

For more information about OPS and UBP, see the user documentation for your Optivity Policy Services 4.0 application.

Chapter 2
Setting passwords, locking ports, and enabling high-secure mode using the CLI

This chapter describes how to set passwords and lock ports using the Passport 8600 CLI. It includes the following topics:

Roadmap of CLI password, port lock, and high-secure commands

The following roadmap lists the CLI password, lock port, and high-secure mode commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
config cli password	aging <days>
	info
	ro <username>
	l1 <username>
	l2 <username>

Command	Parameter
	l3 <username>
	rw <username>
	rwa <username>
	slboper <username>
	l4oper <username>
	oper <username>
	slbadmin <username>
	l4admin <username>
	ssladmin <username>
config sys set reset-passwd login-user {l1|l2|l3|ro|rw}	
config sys set reset-passwd wsm-passwd {l4admin|slbadmin|oper|l4oper|slboper}	
config sys set reset-passwd sam-passwd ssladmin	
config sys set reset-passwd web-server-passwd ro	
config sys set reset-passwd snmp-community-strings {l1|l2|l3|ro|rw}	
config sys set portlock <on|off>	
config ethernet <slot/port[-<slot/port>][,...] lock <true|false>	
config bootconfig flag hsecure <true|false>	

Changing passwords

The switch ships with default passwords set for access to the CLI. To set new passwords for each access level or to change the login or password for the different access levels of the switch, use the following command:

```
config cli password
```

Note: The optional parameter *password* is the password associated with the user name or login name. You must have read-write-all privileges in order to change passwords. For security, passwords are saved to a hidden file.

This command includes the following options:

config cli password followed by:	
aging <days>	Sets the age-out time for passwords. The valid options are 1 to 365.
info	Shows current level parameter settings.
ro <*username*>	Changes the read-only login and/or password. *username* is the login name.
l1 <username>	Changes the layer 1 read/write login and/or password. *username* is the login name.
l2 <*username*>	Changes the layer 2 read/write login and/or password. *username* is the login name.
l3 <*username*>	Changes the layer 3 read/write login and/or password (applies only to the Passport 8600 switch). *username* is the login name.
rw <*username*>	Changes the read/write login and/or password. *username* is the login name.

config cli password followed by:	
`rwa <username>`	Changes the read/write/all login and/or password. *username* is the login name.
`slboper <username>`	Changes the login user name. The valid options are 1 to 20.
`l4oper <username>`	Changes the login user name. The valid options are 1 to 20.
`oper <username>`	Changes the login user name. The valid options are 1 to 20.
`slbadmin <username>`	Changes the login user name. The valid options are 1 to 20.
`l4admin <username>`	Changes the login user name. The valid options are 1 to 20.
`ssladmin <username>`	Changes the login user name. The valid options are 1 to 20.

Configuration example: passwords

The following configuration example uses the commands described above to:

- Change the “ro” username to “test”
- Change the old password of “ro” to “12345”
- View the password information.

Figure 7 shows sample output using these commands.

Figure 7 config cli password command sample output

```
TOKYO>:5# config cli password ro test

Enter the old password : **
Enter the New password : ******
Re-enter the New password : ******

Password changed successfully
TOKYO>:5# config cli password info

Sub-Context: clear config monitor show test trace
Current Context:

        ACCESS    LOGIN
        rwa       rwa
        rw        rw
        l3        l3
        l2        l2
        l1        l1
        ro        test

TOKYO>:5#
```

Synchronizing the master and slave CPU passwords

CLI passwords are synchronized to the standby CPU automatically when it is changed on the master CPU. The CLI passwords must be configured only from the master CPU.

Note: The RADIUS protocol is not used on the slave CPU for authenticating users logging onto the slave CPU.

The CLI passwords can not be changed on the slave CPU.

The command `save config file config.cfg verbose standby standby.cfg` saves only the configuration file to the slave CPU, and does not change the runtime configuration on the slave CPU.

Resetting passwords

For recovery (passwords lost), you have to reset the switch and then apply the following command in **Boot Monitor** mode:

```
monitor#
reset-passwd
```

For any other issue related to passwords, please contact Nortel Networks customer support.

Resetting usernames and passwords

If you have read-write access (rwa), you can reset usernames and passwords using the CLI.

You can reset login user names and passwords for the following access levels: l1, l2, l3, ro, and rw (you cannot modify rwa access), using the following command:

```
config sys set reset-passwd login-user {l1|l2|l3|ro|rw}
```

You can reset wsm usernames and passwords for the following access levels: l4admin, slbadmin, oper, l4oper, and slboper, using the following command:

```
config sys set reset-passwd wsm-passwd
{l4admin|slbadmin|oper|l4oper|slboper}
```

You can reset the ssladmin username and password, using the following command:

```
config sys set reset-passwd sam-passwd ssladmin
```

You can reset the webserver username and password for ro access, using the following command:

```
config sys set reset-passwd web-server-passwd ro
```

You can reset the following SNMP community strings: l1, l2, l3, ro, rw (you cannot reset rwa), using the following command:

```
config sys set reset-passwd snmp-community-strings
{l1|l2|l3|ro|rw}
```

Setting the port lock

The Port Lock feature allows you to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. Locked ports cannot be modified in any way until the port is first unlocked.

To enable or disable the port lock feature globally, use the following command:

```
config sys set portlock <on|off>
```

where:
`on` locks all ports.
`off` unlocks all ports.

To enable or disable the port lock feature for a specific port or ports, use the following command:

```
config ethernet <slot/port[-<slot/port>][,...] lock
<true|false>
```

where:
`true` locks the specified port or ports.
`false` unlocks the specified port or ports.

Enabling or disabling bootconfig hsecure

When the bootconfig flag, **`hsecure`**, is enabled, the software enforces the 8 characters rule for all passwords. When upgrading from a previous release, if the password does not have at least 8 characters, you will be prompted to change your password to the mandatory character length.

To enable (or disable) **hsecure**, use the following command:

```
config bootconfig flag hsecure <true|false>
```

A warning message will display prompting you to reboot the switch for the change to take effect:

```
Warning: Please save boot configuration and reboot the
switch for this to take effect.
```

Changing an invalid-length password

Once you have enabled **hsecure** and rebooted the switch, any user with an invalid-length password will be prompted to change their password. Figure 8 shows a sample output.

Figure 8 config cli password command sample output

```
Login: rwa
Password: ***
Your password is valid but less than mandatory 8 characters.
Please change the password to continue.
Enter the New password : *********
Re-enter the New password : *********
Password changed successfully
```

New default passwords and community strings

If the switch boots in high secure mode after default factory settings, without any password previously configured, the default passwords have been changed to respect this rule. Table 4 describes the new default passwords.

Table 4 New default setting passwords

User ID	New default password
rwa	rwarwarrw
rw	rwrwrwrw
ro	rorororo

Table 4 New default setting passwords (continued)

User ID	New default password
l3	`l3l3l3l3`
l2	`l2l2l2l2`
l1	`l1l1l1l1`
l4admin	`l4adminl`
slbadmin	`slbadmin`
oper	`operoper`
l4oper	`l4operl4`
slboper	`slbopers`
ssladmin	`ssladmin`

Table 5 describes the new default community strings.

Table 5 New default community strings

User ID	New default password
ro	publiconly
l1	privateonly
l2	privateonly
l3	privateonly
rw	privateonly
rwa	secretonly

Aging enforcement

When the **`hsecure`** flag is enabled, after a certain duration (configurable, default = 90 days), you will be asked to change your password, as described previously.

The aging parameter is configurable, by executing the following CLI command:

```
config cli password aging <days>
Set age-out time for passwords
Required parameters: <days>           = age-out time for passwords/
community strings {1..365}
Command syntax: aging <days>
```

Note: For SNMP and FTP, when a password expires, access is denied. Community strings have to be changed to a new string made up of more than 8 characters before accessing the system.

In hsecure mode, the password aging time is synchronized to the slave CPU, so that it is in sync with the master.

Once the password expires, you are required to change the password in the master CPU in order to log in to the slave CPU.

Note that when the **`hsecure`** flag is enabled:

- The Webserver cannot be enabled at any time
- The SSH password-authentication cannot be enabled at any time.

Chapter 3
Setting passwords, locking ports, and viewing SNMP errors using Device Manager

This chapter describes how to set up CLI passwords, specify the number of allowed Telnet sessions and rlogin sessions, lock a port, and view SNMP statistics. It includes the following topics:

Controlling access to the CLI

If you have read/write/all access authority, you can use Device Manager to change the passwords for access to the CLI through a console or Telnet session. You can change passwords that are in encrypted format when using SNMP version 3 (SNMPv3) only. If you do not have read/write/all privileges, the user name and password fields will be blank.

Caution: For security reasons, Nortel Networks recommends that you set the passwords to values other than the factory defaults.

To change passwords for access to the CLI:

1 From the Device Manager menu bar, choose Edit > Security.

The Security dialog box opens with the EAPOL tab displayed. (Figure 9)

Figure 9 Security dialog box—EAPOL tab

2 Click the CLI tab.

The CLI tab opens. (Figure 10)

Figure 10 Security dialog box—CLI tab top part

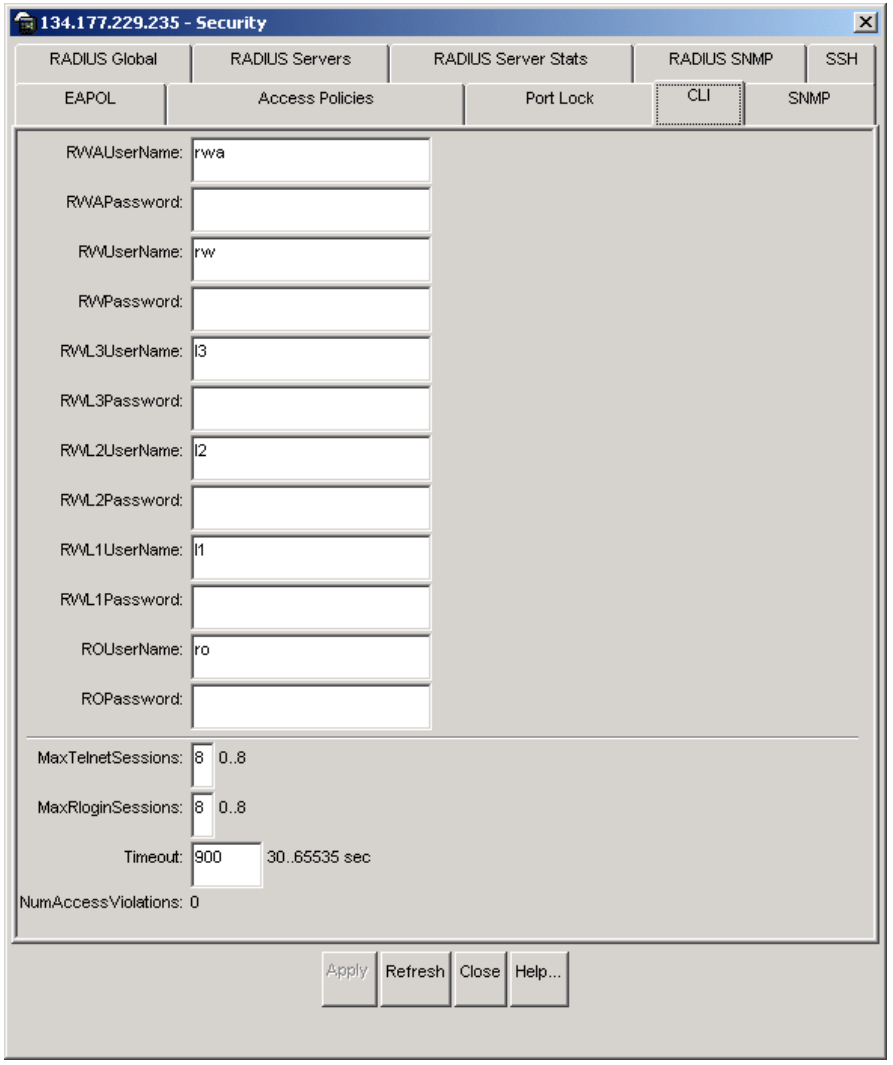


Table 6 describes the Security CLI tab fields.

Table 6 Security CLI tab fields

Field	Description
RWAUserName	Specifies the user name for the read/write/all CLI account.
RWAPassword	Specifies the password for the read/write/all CLI account.
RWUserName	Specifies the user name for the read/write CLI account.
RWPassword	Specifies the password for the read/write CLI account.
RWL3UserName	Specifies the user name for the Layer 3 read/write CLI account.
RWL3Password	Specifies the password for the Layer 3 read/write CLI account.
RWL2UserName	Specifies the user name for the Layer 2 read/write CLI account.
RWL2Password	Specifies the password for the Layer 2 read/write CLI account.
RWL1UserName	Specifies the user name for the Layer 1 read/write CLI account.
RWL1Password	Specifies the password for the Layer 1 read/write CLI account.
ROUserName	Specifies the user name for the read-only CLI account.
ROPassword	Specifies the password for the read-only CLI account.
MaxTelnetSessions	Indicates the maximum number of concurrent Telnet sessions that are allowed (from zero to 8).
MaxRloginSessions	Indicates the maximum number of concurrent rlogin sessions that are allowed (from zero to 8).
Timeout	Indicates the number of seconds of inactivity for a Telnet or rlogin session before automatic time-out and disconnect (30 to 65535 seconds).
NumAccessViolations	Indicates the number of CLI access violations detected by the system. This is a read-only field.

Locking a port

The Port Lock feature allows you to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. Locked ports cannot be modified in any way until the port is first unlocked.

To set port locking and unlocking:

1 From the Device Manager menu bar, choose Edit > Security.

The Security dialog box opens with the EAPOL tab displayed. (Figure 9)

2 Click the Port Lock tab.

The Port Lock tab opens.

Figure 11 Security dialog box—Port Lock tab

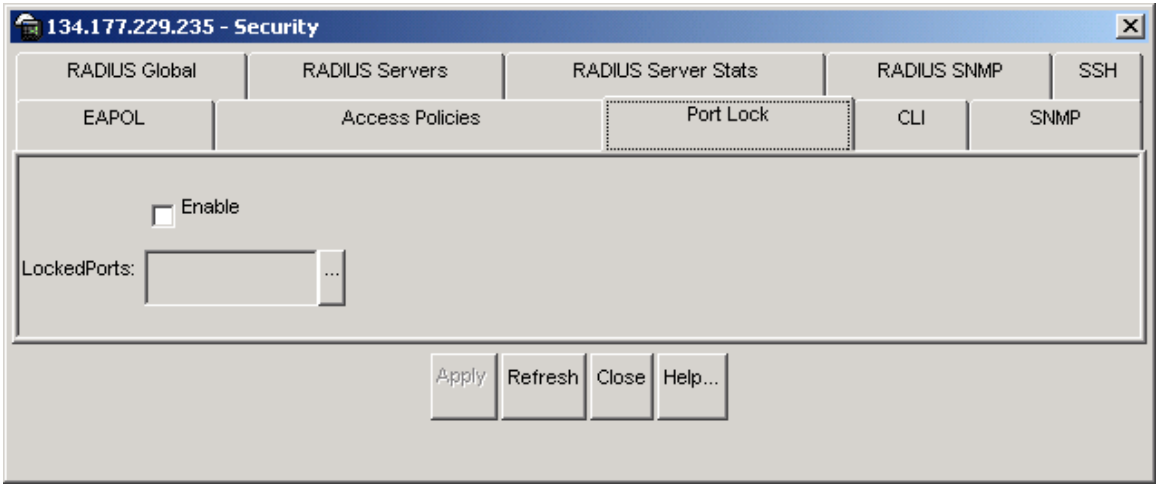


Table 7 describes the Security Port Lock tab fields.

Table 7 Port Lock tab fields

Field	Description
Enable	Selecting this box locks the ports selected.
LockedPorts	Lists the locked ports. Click on the ellipsis button to select the ports you want to lock.

Viewing SNMP errors

To view SNMP errors:

1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the EOPOL tab displayed.

2. Click the SNMP tab.

   The SNMP tab opens (Figure 12).

Figure 12 Security dialog box—SNMP tab

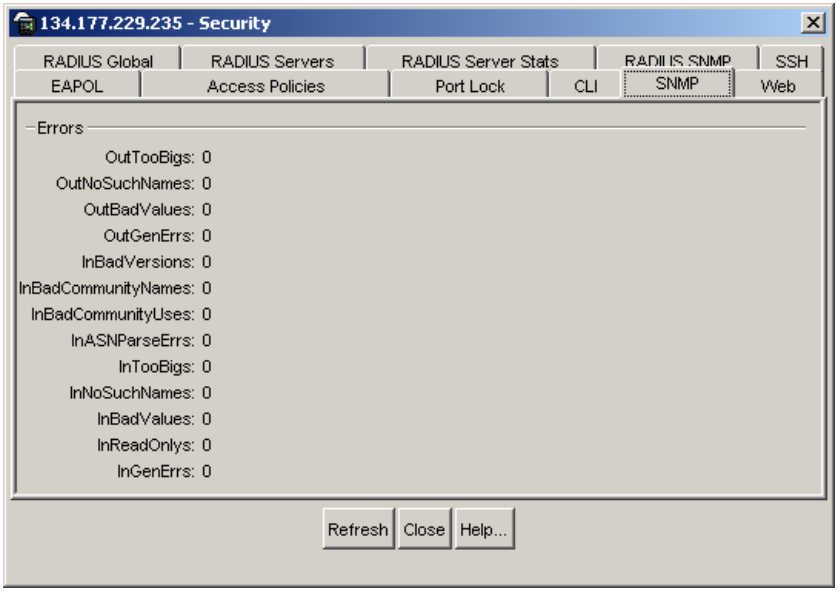


Table 8 describes the SNMP tab fields.

Table 8 SNMP tab fields

Field	Description
OutTooBigs	The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is “tooBig.”
OutNoSuchNames	The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status is “noSuchName.”
OutBadValues	The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is “badValue.”
OutGenErrs	The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is “genErr.”
InBadVersions	The total number of SNMP messages that were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
InBadCommunityNames	The total number of SNMP messages delivered to the SNMP protocol entity that used an SNMP community name not known to said entity.
InBadCommunityUses	The total number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation not allowed by the SNMP community named in the message.
InASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages.
InTooBigs	The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “tooBig.”
InNoSuchNames	The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “noSuchName.”
InBadValues	The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “badValue.”

Table 8 SNMP tab fields (continued)

Field	Description
InReadOnlys	The total number valid SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “read-only”. It should be noted that it is a protocol error to generate an SNMP PDU that contains the value “read-only” in the error-status field; as such this object is provided as a means of detecting incorrect implementations of the SNMP.
InGenErrs	The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “genErr.”

Chapter 4
Configuring access policies using the CLI

You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the switch through various services, such as Telnet, SNMP, HTTP, rlogin, or SSH. You can enable or disable access services by setting flags from the Boot Monitor CLI or the CLI.

Note: To access the backup CPU using the **`peer rlogin`** command, you must set an access policy that enables rlogin access to the backup CPU. See *Getting Started* for more information about the **`peer rlogin`** command.

For information about enabling access services for a specific policy using the CLI, see "Enabling an access policy" on page 87.

You can define network stations explicitly allowed to access the switch or network stations explicitly forbidden to access the switch. For each service you can also specify the level of access, such as read-only or read/write/all.

When you set up access policies, you can either:

- Globally enable the access policy feature, and then create and enable individual policies. Each policy takes effect immediately when you enable it.
- Create and enable individual access policies, and then globally enable the access policy feature to activate all the policies at the same time.

This chapter includes the following topics:

Roadmap of CLI access policy commands

The following roadmap lists the CLI access policy commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config sys access-policy enable <true|false>`	
`config sys access-policy policy <pid>`	`info`
	`accesslevel <level>`
	`create`
	`delete`
	`disable`
	`enable`
	`host <ipaddr>`

Command	Parameter
	mode <mode>
	name <name>
	network <addr/mask>
	precedence <precedence>
	username <string>
config sys access-policy policy <pid> service	info
	ftp <enable|disable>
	http <enable|disable>
	rlogin <enable|disable>
	snmp <enable|disable>
	telnet <enable|disable>
	tftp <enable|disable>
config sys access-policy policy <pid> network <addr/mask>	
config sys access-policy policy <pid> mode <allow|deny>	
config sys access-policy policy <pid> accesslevel <level>	
config sys access-policy policy <pid> host <ipaddr>	
config sys access-policy policy <pid> username <string>	
config sys access-policy policy <pid> precedence <precedence>	
config sys access-policy policy <pid> name <name>	
config sys access-policy policy <pid> <enable|disable>	

Enabling the access policy feature globally

To enable the access policy feature globally, use the following command:

```
config sys access-policy enable <true|false>
```

where:
true enables the access-policy feature globally.
false disables the access-policy feature globally.

Configuring access policies

To configure access policy, use the following command:

```
config sys access-policy policy <pid>
```

where:
pid is the number that identifies the policy.

This command includes the following parameters:

config sys access-policy policy <*pid*> followed by:	
`info`	Shows the current level parameter settings and next level directories.
`accesslevel <level>`	Allows you to specify the level of access if the policy is to allow access. • *level* is the access level (ro, rw, or rwa) or equivalent community string designation (read-only, read/write, or read/write/all).
`access-strict <true|false>`	Enable (true) or disable (false) the access level strictly.
`create`	Creates the specified access policy on the switch.
`delete`	Removes the specified access policy from the switch.
`disable`	Disables the access policy on the switch.

config sys access-policy policy <*pid*> followed by:	
`enable`	Enables the access policy on the switch
`host <ipaddr>`	For rlogin access, specifies the trusted host address.
`mode <mode>`	Specifies whether this network address is allowed or denied access through the specified access service. The default is allow.
`name <name>`	Specifies the name of the policy. The default name is policy<*policy_ID*>
`network <addr/mask>`	Specifies the IP address and subnet mask that are being permitted or denied access through the specified access service.
`precedence <precedence>`	Specifies a precedence for the policy. • *precedence* is a number from 1 to 128. This value determines which policy to use if multiple policies apply. Lower numbers have higher precedence. The default is 10.
`username <string>`	For rlogin access, specifies the trusted host user name.

Configuration example: access policies

The following configuration example uses the commands described above to:

- Create access policy 2345.
- View the information for the access policy.
- Set the network information for access policy 2345 to 12.12.12.12/ 255.255.255.255.
- Set the username for access policy 2345 to test.
- Set the host for access policy 2345 to 5.5.5.5.
- Set the name for access policy 2345 to testpolicy.
- Set the precedence for access policy 2345 to 100.
- Set the host for access policy 2345 to 6.6.6.6.
- View the information for the access policy.

Figure 13 shows sample output using these commands.

Figure 13 config sys access-policy policy command sample output

```
TOKYO>:5# config sys access-policy policy 2345 create
TOKYO>:5# config sys access-policy policy 2345 info

Sub-Context: clear config monitor show test trace
Current Context:

                     create :
                     delete : N/A
                       name : policy2345
               policy enable : true
                       mode : allow
                  precedence : 10
                     network : 0.0.0.0/0.0.0.0
                        host : 0.0.0.0
                    username : none
                 accesslevel : readOnly
               access-strict : false

TOKYO>:5# config sys access-policy policy 2345 network 12.12.12.12/255.255.255.255
TOKYO>:5# config sys access-policy policy 2345 username test
TOKYO>:5# config sys access-policy policy 2345 host 5.5.5.5
TOKYO>:5# config sys access-policy policy 2345 name testpolicy
TOKYO>:5# config sys access-policy policy 2345 precedence 100
TOKYO>:5# config sys access-policy policy 2345 host 6.6.6.6
TOKYO>:5# config sys access-policy policy 2345 info

Sub-Context: clear config monitor show test trace
Current Context:

                     create :
                     delete : N/A
                       name : testpolicy
               policy enable : true
                       mode : allow
                  precedence : 100
                     network : 12.12.12.12/255.255.255.255
                        host : 6.6.6.6
                    username : test
                 accesslevel : readOnly
               access-strict : false

TOKYO>:5#
```

Creating an access policy

To create an access policy, use the following command:

```
config sys access-policy policy <pid> create
```

where:
pid is the number that identifies the policy that you are creating.

Setting access policy strict access functionality

A new parameter `access-strict` has been added to the CLI access policy tree. This parameter, if set to `true`, grants access to the configured level only. This allows access policies to be created to allow only, read only or only read write access. Command syntax is shown below.

```
config sys access-policy policy access-strict [true/false]
```

If `access-strict` is set to `false`, the access policy will operate as before. A configured access level of `ro` will grant access to read only and above access levels.

If `access-strict` is `true`, a configured access level of `ro` will grant access to only read only access levels.

The default value of access-strict is `false`.

Changing user access

As a network administrator, you can override a user's access to CLI commands by configuring the RADIUS server for user authentication. You must still give access based on the existing six access levels in the Passport 8000 Series switch, but you can customize user access by allowing and disallowing specific CLI commands.

Subscriber and/or Administrative Interaction

You must configure the following three returnable attributes for each user:

- Access priority (single instance) - the access levels currently available on Passport 8600: ro, l1, l2, l3, rw, rwa.
- Command access (single instance) - indicates whether the CLI commands configured on the RADIUS server are allowed or disallowed for the user.
- CLI commands (multiple instances) - the list of commands that the user can/cannot use.

Radius server configuration:

To configure BSAC server:

1 Create a new file (for example, pprtl2l3.dct) and update the following info:

```
ATTRIBUTE Radlinx-Vendor-Specific 26 [vid=648 data=string] R
ATTRIBUTE Access-Priority 26[vid=1584 type1=192 len1=+2 data=integer]r
ATTRIBUTE Command-Access 26[vid=1584 type1=194 len1=+2 data=integer]r
ATTRIBUTE Cli-Commands 26[vid=1584 type1=195 len1=+2 data=string]R
```

192,194,195 are the default values. You can change these on the Passport 8600.

The following are the Access Levels you can give to a user:

```
VALUE Access-Priority RWA-Access 6
VALUE Access-Priority RW-Access 5
VALUE Access-Priority RO-Access 1
VALUE Access-Priority L3-Access 4
VALUE Access-Priority L2-Access 3
VALUE Access-Priority L1-Access 2
VALUE Access-Priority None-Access 0
```

The following are the values that are valid for the Command-Access Attribute:

```
VALUE Command-Access TRUE 1
VALUE Command-Access FALSE 0
```

2 In the file dictiona.ini add the new file pprtl2l3.dct

```
@pprtl2l3.dct
```

3 Update the file `vendor.ini` as follows:

```
vendor-product = Nortel Passport 1000 and 8000 L2L3
Switches
dictionary = pprtl2l3
ignore-ports = no
help-id = 0
```

4 To change the configuration of the Free Radius Server, create a new file dictionary.passport and include it in dictionary file.

5 Add the following to the file:

```
VENDOR Passport 1584
ATTRIBUTE Access-Priority 192 integer Passport
ATTRIBUTE Cli-Commands 195 string Passport
ATTRIBUTE Command-Access 194 integer Passport
```

192,193 are the default values. You can change these on the Passport 8600.

The following the Access Levels you can give to a user:

```
VALUE Access-Priority RWA-Access 6
VALUE Access-Priority RW-Access 5
VALUE Access-Priority RO-Access 1
VALUE Access-Priority L3-Access 4
VALUE Access-Priority L2-Access 3
VALUE Access-Priority L1-Access 2
VALUE Access-Priority None-Access 0
```

The following are the values that are valid for the Command-Access Attribute.

```
VALUE Command-Access FALSE 0
VALUE Command-Access TRUE 1
```

6 The file `clients` has to be modified to provide access to the Passport 8600 and to specify the `secret value configure` while configuring the radius server.

```
x.x.x.x mysecret
```

where x.x.x.x is the Passport 8600 IP Address.
`mysecret` is the secret configured while creating RADIUS server.

7 The file users must have the following access:

```
rwa Auth-Type:= Local, Password == rwa
Access-Priority = RWA-Access,
```

The user must be configured like `rwa` and the password you have to keep and the Access-Priority has to be amongst the aforementioned values in dictionary.

Example 1:

```
User- john
Access-Priority – L2-Access
Command-Access - True
Cli-Commands - Config ip ospf
```

Though John has only L2 access, he can use the command `config ip ospf`, which normally requires L3 access.

Example 2:

```
User- Mike
Access-Priority - RWA-Access
Command-Access – False
Cli-Commands – reset
```

Although Mike has `rwa` access, he is prevented from using the `reset` command to reboot the switch.

8 If a user displays `help`, the system displays help for only those commands the user can access.

Note: If you disallow any command, only the lowest option in the command tree is disallowed. For example, if you disallow `config sys set` for a user, the user can display or execute `config`, or `config sys`. Only `set` is disallowed.

Enabling an access service

To enable or disable an access service for the specified policy, use the following command:

`config sys access-policy policy <pid> service`

where:
pid is the number that identifies the policy.

This command includes the following parameters:

config sys access-policy policy <*pid*> service followed by:	
`info`	Shows current level parameter settings and next level directories.
`ftp <enable|disable>`	Enables or disables FTP for the specified policy.
`http <enable|disable>`	Enables or disables HTTP for the specified policy.
`rlogin <enable|disable>`	Enables or disables rlogin for the specified policy.
`snmp <enable|disable>`	Enables or disables SNMP for the specified policy.
`ssh <enable|disable>`	Enables or disables SSH for the specified policy.

config sys access-policy policy <*pid*> service followed by:	
`telnet <enable|disable>`	Enables or disables Telnet for the specified policy.
`tftp <enable|disable>`	Enables or disables TFTP for the specified policy.

Configuration example: access policy and service

The following configuration example uses the commands described above to:

- Enable FTP for access policy 2345.
- Enable SNMP for access policy 2345.
- Enable telnet for access policy 2345.
- View the information for the access policy.

Figure 14 show sample output using these commands.

Figure 14 config sys access-policy policy service commands output

```
TOKYO>:5# config sys access-policy policy 2345 service ftp enable
TOKYO>:5# config sys access-policy policy 2345 service snmp enable
TOKYO>:5# config sys access-policy policy 2345 service telnet enable
TOKYO>:5# config sys access-policy policy 2345 service info

Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:

                      http : disable
                    rlogin : disable
                      snmp : enable
                    telnet : enable
                       ssh : disable
                      tftp : disable
                       ftp : enable

TOKYO>:5#
```

Allowing a network access to the switch

To specify the network to which you want to allow access, use the following command:

```
config sys access-policy policy <pid> network <addr/mask>
```

where:
pid is the number that identifies the policy that you are creating.
addr/mask is the IP address and subnet mask that are being permitted or denied access through the specified access service.

To specify whether this network address is allowed or denied access through an access service, use the following command:

```
config sys access-policy policy <pid> mode <allow|deny>
```

where:
pid is the number that identifies the policy that you are creating.
`allow|deny` allows or denies access through the specified access service.

If the policy is to allow access, to specify a level of access, use the following command:

```
config sys access-policy policy <pid> accesslevel <level>
```

where:
pid is the number that identifies the policy that you are creating.
level is the access level (ro, rw, rwa) or equivalent community string designation (read-only, read/write, or read/write/all).

Specifying the host and username for rlogin

For rlogin access, you must specify a trusted host address and a trusted host user name. To specify the host address and user name, use the following commands:

```
config sys access-policy policy <pid> host <ipaddr>
```

```
config sys access-policy policy <pid> username <string>
```

where:
pid is the number that identifies the policy that you are creating.
ipaddr is the trusted host address.
string is the associated user name for this address.

To access the switch, you must log in using the user name and host address that you specified in this section.

Assigning a precedence for the policy

To assign a precedence for the policy, use the following command:

```
config sys access-policy policy <pid> precedence
<precedence>
```

where:
pid is the number that identifies the policy that you are creating.
precedence is a number from 1 to 128. This value determines which policy to use if multiple policies apply. Lower numbers have higher precedence.

Naming an access policy

To assign a name to the policy, use the following command:

```
config sys access-policy policy <pid> name <name>
```

where:
pid is the number that identifies the policy that you are creating.
name is a string from 1 to 15 characters.

Enabling an access policy

To enable an access policy, use the following command:

```
config sys access-policy policy <pid> <enable|disable>
```

where:
pid is the number that identifies the policy that you are creating.
enable|disable enables or disables the specified policy.

Chapter 5
Configuring access policies using Device Manager

You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the switch through various services, such as Telnet, SNMP, TFTP, FTP, HTTP, rlogin, and SSH.

You can define network stations that are explicitly allowed to access the switch or network stations that are explicitly forbidden to access the switch. For each service you can also specify the level of access, such as read-only or read/write/all.

This chapter includes the following topics:

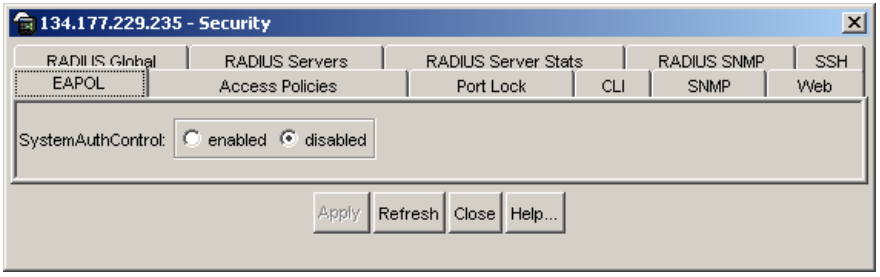
Creating a new access policy

To create a new access policy:

1 From the Device Manager menu bar, choose Edit > Security.

The Security dialog box opens with the EAPOL tab displayed. (Figure 15)

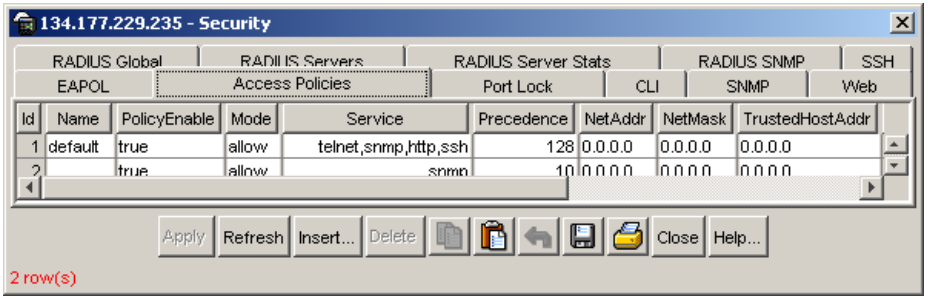
Figure 15 EAPOL dialog box



2 Click the Access Policies tab.

The Security dialog box opens with the Access Policies tab active. (Figure 16)

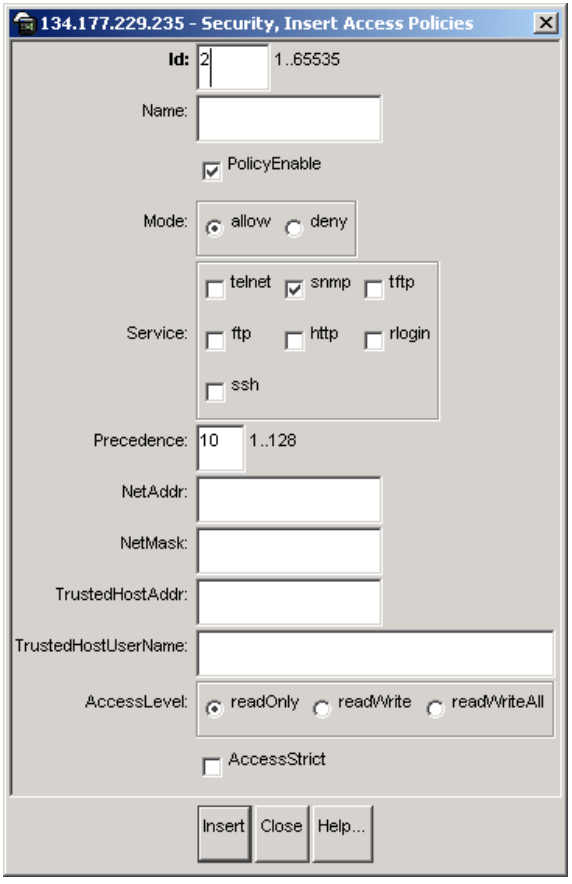
Figure 16 Security dialog box—Access Policies tab



3 In the Security dialog box, click Insert.

The Security, Insert Access Policies dialog box (Figure 17) opens. The fields are defined in the Access Policies fields table (Table 9). All fields are optional except ID.

Figure 17 Security dialog box—Insert Access Policies tab



4 Make sure PolicyEnable is checked.

5 Select the mode to allow or deny a service.

6 Select a service either telnet, SNMP, TFTP, FTP, HTTP, rlogin, or SSH.

7 Set a precedence number for the service (lower numbers mean higher precedence).

8 Enter an IP address in the NetAddr field.

9 Enter the NetMask used for the NetAddr field.

10 Enter an IP address for the TrustedHostAddr.

11 Enter a user name for the TrustedHostUserName.

12 Select the access level for the service. Choose readOnly, readWrite, or readWriteAll.

13 AccessStrict box can be checked if required

14 Click Insert.

Table 9 describes the items on the Insert Access Policies fields.

Table 9 Access Policies fields

Field	Description
Id	Specifies the policy ID.
Name	Specifies the name of this policy.
PolicyEnable	Enables the access policy.
Mode	Indicates whether a packet having a source IP address that matches this entry should be permitted to enter the device or denied access.
Service	Indicates the protocol to which this entry should be applied.
Precedence	Indicates the precedence of the policy. The lower the number, the higher the precedence (1 to 128).
NetAddr	Indicates the source network IP address. An address of 0.0.0.0 specifies any address on the network.
NetMask	Indicates the source network masks.
TrustedHostAddr	Indicates the trusted IP address of the host performing rlogin or rsh into the device. Applies only to rlogin and rsh. **Note:** You cannot use wildcard entries.
TrustedHostUserName	Specifies the user name assigned to the trusted host. Applies only to rlogin and rsh. This name is the same user name that you used to log on to the network (not the switch user name, such as rwa). **Note:** You cannot use wildcard entries. The user must already be logged in with the user name to be assigned to the trusted host. For example, using “rlogin -l newusername xx.xx.xx.xx” will not work from a UNIX workstation.
AccessLevel	Specifies the access level of the trusted host (readOnly, readWrite, or readWriteAll).

Table 9 Access Policies fields (continued)

Field	Description
Usage	A read-only field that appears on the Access Policies tab. This field indicates the number of times that the policy has been used.
AccessStrict	Checking the box sets the access level strictly.

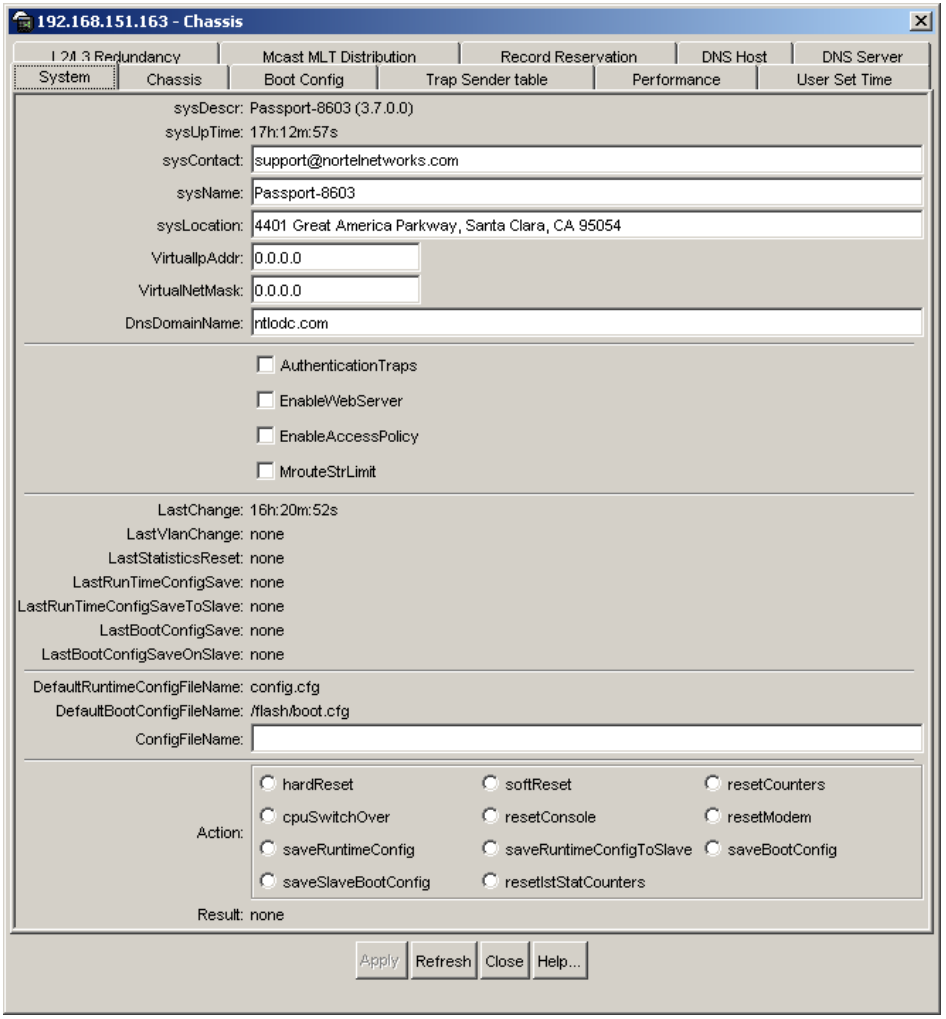
Enabling Access Policy feature Globally

To enable the Access Policy feature for rlogin or rsh access:

1 From the Device Manager menu bar, select Edit > Chassis.

The Chassis dialog box opens with the System tab displayed. (Figure 18)

Figure 18 Chassis dialog box—System tab



2 Check EnableAccessPolicy.

3 Click Apply.

4 Click Close.

Chapter 6
Configuring SNMPv3 using the CLI

An SNMPv3 engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one-to-one association between an SNMP engine and the SNMP entity, which contains it.

This chapter describes how to set up your SNMP configuration using the CLI:

Roadmap of CLI SNMPv3 commands

The following roadmap lists the CLI SNMPv3 commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
config snmp-v3 usm create <User Name> [<auth protocol>] [auth <value>] [priv <value>] [engid <value>]	
config snmp-v3 group-member create <user name> <model> [<group name>]	
config snmp-v3 group-access create <group name> <prefix> <model> <level>	
config snmp-v3 mib-view create <View Name> <subtree oid> [mask <value>] [type <value>]	
config snmp-v3 community create <Comm Idx> <name> <security> [tag <value>]	
config snmp-v3 community commname <Comm Idx> new-commname <value>	
config snmp-v3 community info	
config snmp-v3 notify create <Notify Name> [tag <value>] [type <value>]	
config snmp-v3 ntfy-profile create <Params Name> [profile <value>]	
config snmp-v3 ntfy-filter create <Profile Name> <subtree oid> [mask <value>] [type <value>]	
config snmp-v3 target-addr create <Target Name> <Ip addr:port> <Target parm> [timeout <value>] [retry <value>] [taglist <value>] [mask <value>] [mms <value>]	

Command	Parameter
config snmp-v3 target-param create <target param name> mp-model <value> sec-level <value> sec-name <value>	
show config module sys	

Loading the encryption module

Before you can access the switch using SNMPv3 with DES encryption, you must load the encryption module, p80c3700.des, which allows you to use the Privacy protocol.

Note: You must install the p80c3700.des encryption module only when encryption is required (that is, communication between a network management application and the Passport 8600). The SNMPv3 protocol can work successfully without this module.

1. Open a browser and enter the following URL:

   www.nortelnetworks.com

2. Select “Software Downloads” under the Support heading.
3. Select “Passport” under Product family.
4. Find “Passport 8600 Routing Switch”.
5. Click on the “Software” link.
6. Click on the “Passport 8600 SNMPv3/DES” link.
7. Log in.
8. Answer the questions on the questionnaire.
9. Click submit.
10. Right mouse click on file download link and enter a file location in which to copy the DES encryption module.
11. Click OK.

12 The file is downloaded.

Note: Note the location of this file. You will need to load the file on the switch before you can use the protocol.

13 Now, FTP this file to the switch. Open the DOS window.

14 FTP to the Passport 8600 switch. Figure 19 shows sample output from an FTP session.

Figure 19 FTP sample output from DOS window

```
c:\ftp <10.10.10.10>
Connected to <10.10.10.10>
220 Passport FTP server ready
User (<10.10.10.10>:(none)): rwa
331 Password required
Password: ***
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put <path to file on the PC>
```

15 Go back to the Passport 8000 Series switch and load the module.

```
config load-module DES /flash/p80c3700.des
```

Upgrading SNMP to release 3.7

In release 3.3, you set SNMP community strings by using the following command (this command is now obsolete):

```
config sys set snmp community rwa <commstring>
```

After you save the configuration, this command appears in the configuration file.

In release 3.5, you set SNMP community strings by using the following command (this command is now obsolete):

```
config sys set snmp community rwa <commstring>
```

After you save the configuration, this command will NOT appear in the configuration file. However, the community strings are stored in a hidden file.

In release 3.7, you set SNMP community strings by using the following command:

```
config snmp-v3 community create <Comm Idx> <name> <security>
[tag <value>]
```

After you save the configuration, information regarding SNMP community strings is stored in a separate file and will not be found in configuration files.

For detailed instructions on how to upgrade SNMP from release 3.3 to 3.7, or from release 3.5 to release 3.7, see *Release Notes for the Passport 8000 Series Switch Software 3.7*.

Creating a new user in the USM table

To create a new user in the USM table on the Passport 8000 Series switch, enter the following command:

```
config snmp-v3 usm create <User Name> [<auth protocol>]
[auth <value>] [priv <value>] [engid <value>]
```

The `config snmp-v3 usm create` command creates a new user in the USM table. The command includes the following options:

config snmp-v3 usm create followed by:	
`user name`	Creates the new entry with this security name. The name is used as an index to the table. The range is 1 to 32 characters.
`auth protocol`	Specifies an authentication protocol. If no value is entered, the entry has no authentication capability. The protocol choices are: MD5 and SHA.
`auth <value>`	Specifies an authentication password. If no value is entered, the entry has no authentication capability. The range is 1 to 32 characters.
`priv <value>`	Assigns a privacy password. If no value is entered, the entry has no privacy capability. The range is 1 to 32 characters. **Note:** You must set authentication before you can set the privacy option.
`engid <value>`	Specifies the engine Id of the authoritative engine for which the user is being created. By default, engine Id of the switch will be used.

Other USM commands

The following are additional **`config snmp-v3 usm`** commands:

config snmp-v3 usm followed by:	
`info`	Displays the current level parameter settings and next level directories.
`delete <user name>`	Deletes a user for the USM table.
`auth <user name> old-pass <value> new-pass <value> engid <value>` `(Optional)`	Changes the authentication password.
`priv <user name> old-pass <value> new-pass <value> engid <value>` `(Optional)`	Changes privacy password.

Configuration example: USM

The following configuration example uses the commands described above to:

- Create a new USM user, testing.
- Set the authentication protocol to MD5.
- Set the authentication password to test.
- Display information on the user.

Figure 20 shows sample output using these commands.

Figure 20 USM command sample output

```
Passport-8603:3# config snmp-v3 usm create testing md5 auth test

WARNING : For security purpose, we are strongly recommanded
          that NOT to use repeated pattern for your password.

Passport-8603:3# config snmp-v3 usm info

Engine ID = 80:00:08:E0:03:00:04:38:7E:84:00

================================================================================
                                      USM Configuration
================================================================================
User Name             Engine Id                        Protocol
--------------------------------------------------------------------------------
testing              800008e0030004387e8400           HMAC_MD5, NO  PRIVACY

1 out of 1 Total entries displayed
--------------------------------------------------------------------------------

Passport-8603:3#
```

Creating a new user group member

To create a new group member on the Passport 8000 Series switch, enter the following command:

```
config snmp-v3 group-member create <user name> <model>
[<group name>]
```

The **`config snmp-v3 group-member create`** command includes the following options:

`config snmp-v3 group-member create` followed by:	
`user name`	Creates the new entry with this user name. The range is 1 to 32 characters.
`model`	Specifies the message processing model to use when generating an SNMP message. The valid options are usm, snmpv1, and snmpv2c.
`group name`	Assigns the user to the group for data access. The range is 1 to 32 characters.

Other group-member commands

The following are additional **`config snmp-v3 group-member`** commands:

`config snmp-v3 group-member` followed by:	
`info`	Displays the VACM group membership configuration.
`delete <user name> <model>`	Deletes a user group for the v3 VACM table.
`name <user name> <model> <group name>`	Changes group name for the v3 VACM table.

Configuration example: SNMPv3 group

The following configuration example uses the commands described above to:

- Create a new group user, john, using security model USM for group.
- Create a new group user, nick, using security model SNMPv2 for group.
- View the group member information.
- Delete group user nick.
- View the group member information.

Figure 21 shows sample output using these commands.

Figure 21 SNMPv3 group configuration sample output

```
TOKYO>:5# config snmp-v3 group-member create john usm group
TOKYO>:5# config snmp-v3 group-member create nick snmpv2c group
TOKYO>:5# config snmp-v3 group-member info

================================================================================
                                        VACM Group Membership Configuration
================================================================================
Sec Model  User Name                      Group Name
--------------------------------------------------------------------------------
snmpv1     initialview                    v1v2grp
snmpv2c    nick                           group
snmpv2c    initialview                    v1v2grp
usm        john                           group
4 out of 4 Total entries displayed
--------------------------------------------------------------------------------

TOKYO>:5# config snmp-v3 group-member delete nick snmpv2c
TOKYO>:5# config snmp-v3 group-member info

================================================================================
                                        VACM Group Membership Configuration
================================================================================
Sec Model  User Name                      Group Name
--------------------------------------------------------------------------------
snmpv1     initialview                    v1v2grp
snmpv2c    initialview                    v1v2grp
usm        john                           group

3 out of 3 Total entries displayed
--------------------------------------------------------------------------------

TOKYO>:5#
```

Creating v3 group access

To create new access for a group in the VACM table on the Passport 8000 Series switch, use the following command:

```
config snmp-v3 group-access create <group name> <prefix>
<model> <level>
```

The **`config snmp-v3 group-access create`** command includes the following options:

`config snmp-v3 group-access create` followed by:	
`group name`	Creates the new entry with this group name. The range is 1 to 32 characters.
`prefix`	Assigns a context prefix. The range is 1 to 32 characters. **Note:** The *`prefix`* option is not supported in the current release of the Passport 8600; however, because it is part of the index for the table, it must be configured. When you configure prefix, enter "" to indicate an empty string.
`model`	Assigns the authentication checking to communicate to the switch. The valid options are usm, snmpv1, and snmpv2c.
`level`	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row.

Other group-access commands

The following are additional **`config snmp-v3 group-access`** commands:

`config snmp-v3 group-access` followed by:	
`info`	Displays the current level parameter settings and next level directories.

config snmp-v3 group-access followed by:	
`delete <group name> <prefix> <model> <level>`	Removes group access for the v3 VACM table.
`view <group name> <prefix> <model> <level> [read <value>] [write <value>] [notify <value>]`	Changes group access view name for the v3 VACM table.

Configuration example: SNMPv3 group access

The following configuration example uses the commands described above to:

- Create a new group access, secondary, the security model as USM, and level as NoAuthNoPriv.
- Create a new group access, tertiary, security model as USM, and level as NoAuthNoPriv.
- View the group access information.
- Delete group access for secondary.
- Change the group access for tertiary to read as tertiary and write as tertiary.
- View the group access information.

Figure 22 shows sample output using these commands.

Figure 22 SNMPv3 group access configuration sample output

```
Passport-8603:3# config snmp-v3 group-access create secondary "" usm noAuthNoPriv
Passport-8603:3# config snmp-v3 group-access create tertiary "" usm noAuthNoPriv
Passport-8603:3# config snmp-v3 group-access view secondary "" usm noAuthNoPriv
read org write org notify org
Passport-8603:3#  config snmp-v3 group-access view tertiary "" usm noAuthNoPriv
read org write org notify org
Passport-8603:3#  config snmp-v3 group-access info
================================================================================
                                    VACM Group Access Configuration
================================================================================
Group      Prefix Model   Level        ReadV      WriteV     NotifyV
--------------------------------------------------------------------------------
initial           usm     authPriv     root       root       root
readgrp           snmpv1  noAuthNoPriv v1v2only
readgrp           snmpv2c noAuthNoPriv v1v2only
v1v2grp           snmpv1  noAuthNoPriv v1v2only   v1v2only   v1v2only
v1v2grp           snmpv2c noAuthNoPriv v1v2only   v1v2only   v1v2only
tertiary          usm     noAuthNoPriv org        org        org
sBladeGrp         snmpv1  noAuthNoPriv sBladeView sBladeView sBladeView
sBladeGrp         snmpv2c noAuthNoPriv sBladeView sBladeView sBladeView
secondary         usm     noAuthNoPriv org        org        org
9 out of 9 Total entries displayed
--------------------------------------------------------------------------------
Passport-8603:3# config snmp-v3 group-access delete secondary "" usm noAuthNoPriv
Passport-8603:3# config snmp-v3 group-access view tertiary "" usm noAuthNoPriv
read 1.3
Passport-8603:3# config snmp-v3 group-access info
================================================================================
                                    VACM Group Access Configuration
================================================================================
Group      Prefix Model   Level        ReadV      WriteV     NotifyV
--------------------------------------------------------------------------------
initial           usm     authPriv     root       root       root
readgrp           snmpv1  noAuthNoPriv v1v2only
readgrp           snmpv2c noAuthNoPriv v1v2only
v1v2grp           snmpv1  noAuthNoPriv v1v2only   v1v2only   v1v2only
v1v2grp           snmpv2c noAuthNoPriv v1v2only   v1v2only   v1v2only
tertiary          usm     noAuthNoPriv 1.3        org        org
sBladeGrp         snmpv1  noAuthNoPriv sBladeView sBladeView sBladeView
sBladeGrp         snmpv2c noAuthNoPriv sBladeView sBladeView sBladeView

8 out of 8 Total entries displayed
--------------------------------------------------------------------------------
Passport-8603:3#
================================================================================
                                    VACM Group Access Configuration
================================================================================
Group      Prefix Model   Level        ReadV      WriteV     NotifyV
--------------------------------------------------------------------------------
initial           usm     authPriv     root       root       root
readgrp           snmpv1  noAuthNoPriv v1v2only
readgrp           snmpv2c noAuthNoPriv v1v2only
v1v2grp           snmpv1  noAuthNoPriv v1v2only   v1v2only   v1v2only
v1v2grp           snmpv2c noAuthNoPriv v1v2only   v1v2only   v1v2only
tertiary          usm     noAuthNoPriv 1.3        org        org
sBladeGrp         snmpv1  noAuthNoPriv sBladeView sBladeView sBladeView
sBladeGrp         snmpv2c noAuthNoPriv sBladeView sBladeView sBladeView

8 out of 8 Total entries displayed
--------------------------------------------------------------------------------
Passport-8603:3#
```

Creating a new entry for the MIB in the View table

To create a new entry for the MIB View table on the Passport 8000 Series switch, enter the following command:

```
config snmp-v3 mib-view create <View Name> <subtree oid>
[mask <value>] [type <value>]
```

The **config snmp-v3 mib-view create** command includes the following options:

config snmp-v3 mib-view create followed by:	
view Name	Creates a new entry with this group name. The range is 1 to 32 characters.
subtree oid	The prefix that defines the set of MIB objects accessible by this SNMP entity. The range is 1 to 32 characters.
mask <*value*> (Optional)	Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.
type <*value*> (Optional)	Determines whether access to a mib object is granted or denied. The valid options are include and exclude.

Other MIB-view commands

The following are additional **config snmp-v3 mib-view** commands:

config snmp-v3 mib-view followed by:	
info	Displays the current level parameter settings and next level directories.
delete <*View name*> <*subtree oid*>	Deletes an entry an entry for the MIB-view table.

config snmp-v3 mib-view followed by:	
mask *<View Name> <subtree oid> <new-mask>*	Changes the view mask for an entry in the MIB-view table.
type *<View Name> <subtree oid> <new-type>*	Changes the type for an entry in the MIB-view table.

Configuration example: MIB view

The following configuration example uses the commands described above to:

- Create a new MIB view, dev, using a subtree oid of 1.3.8.7.1.4, a mask of ffff, and a type of include.
- View the MIB view information.
- Change the type to exclude.
- View the MIB view information.

Figure 23 shows sample output using these commands.

Figure 23 MIB view commands sample output

```
TOKYO:5# config snmp-v3 mib-view create dev 1.3.8.7.1.4 mask ffff type
include
TOKYO:5# config snmp-v3 mib-view info

================================================================================
                                      MIB View
================================================================================
View Name           Subtree                      Mask               Type
--------------------------------------------------------------------------------
dev                1.3.8.7.1.4                  0xffff             include
org                 1                                               include
root                1                                               include
snmp               1.3.6.1.6.3                                      include
snmp               1.3.6.1.2.1.1                                    include
layer1              1.3                                             exclude
layer1             1.3.6.1.2.1.1                                    include
layer1             1.3.6.1.2.1.2.2.1.7                              include

8 out of 8 Total entries displayed
--------------------------------------------------------------------------------
TOKYO:5# config snmp-v3 mib-view type dev 1.3.8.7.1.4 exclude
TOKYO:5# config snmp-v3 mib-view info

================================================================================
                                      MIB View
================================================================================
View Name           Subtree                      Mask               Type
--------------------------------------------------------------------------------
dev                1.3.8.7.1.4                  0xffff             exclude
org                 1                                               include
root                1                                               include
snmp               1.3.6.1.6.3                                      include
snmp               1.3.6.1.2.1.1                                    include
layer1              1.3                                             exclude
layer1             1.3.6.1.2.1.1                                    include
layer1             1.3.6.1.2.1.2.2.1.7                              include

8 out of 8 Total entries displayed
--------------------------------------------------------------------------------
TOKYO:5#
```

Creating a community

To create a community on the Passport 8000 Series switch, enter the following command:

```
config snmp-v3 community create <Comm Idx> <name> <security>
[tag <value>]
```

The **config snmp-v3 community create** command includes the following options:

config snmp-v3 community create followed by:	
Comm Idx	The unique index value of a row in this table. The range is 1-32 characters.
name	The community string for which a row in this table represents a configuration
security	Maps community string to the security name in the VACM Group Member Table.
tag <*value*> (optional)	The transport tag name in the table. The range is 1-32 characters.

Other community commands

The following are additional **config snmp-v3 community** commands:

config snmp-v3 community followed by:	
info	Displays the community table, including the index, name, and security name.
delete <*Comm Idx*>	Deletes an entry from the community table.
commname <*Comm Idx*> new-commname <*value*>	Changes the name for an entry in the community table.
secname <*Comm Idx*> new-secname <*value*>	Changes the security name for an entry in the community table.

config snmp-v3 community followed by:	
`tag <Comm Idx> new-tag <value>`	Changes the transport tag for an entry in the community table.
`rmtag <Comm Idx>`	Removes the transport tag for an entry in the community table.

Changing the default community strings

If you're using the default public/private access through SNMPv1, SNMPv2, or SNMPv3 and want to change them, use the following command:

```
config snmp-v3 community commname <Comm Idx> new-commname
<value>
```

where:
Comm Idx is unique index value of a row in this table. The range is 1-32 characters.
value is the new community name.

In the following example, you change the default public name, first, to new_public and the default private name, second, to new_private:

```
config snmp-v3 community commname first new-commname
new_public

config snmp-v3 community commname second new-commname
new_private
```

To view the Community Table, use the following command:

```
config snmp-v3 community info
```

Figure 24 shows the output from this command.

Figure 24 config snmp-v3 community info output

```
TOKYO>:5# config snmp-v3 community info

================================================================================
                                      Community Table
================================================================================
INDEX           NAME            SECURITYNAME    TRANSPORT TAG
--------------------------------------------------------------------------------
first           ********        readview
second          ********        initialview

2 out of 2 Total entries displayed
--------------------------------------------------------------------------------

TOKYO>:5#
```

Configuration example: community

The following configuration example uses the commands described above to:

- Create a community using third as the index, using public as the name, and v1v2only as security.
- View the community information.
- Change the name to private.
- View the community information.
- Change the security to v1v3only.
- View the community information.

Figure 25 shows sample output using these commands.

Figure 25 Community commands sample output

```
TOKYO>:5# config snmp-v3 community create third public v1v2only
TOKYO>:5# config snmp-v3 community info

================================================================================
                                    Community Table
================================================================================
INDEX           NAME            SECURITYNAME    TRANSPORT TAG
--------------------------------------------------------------------------------
first           ********        readview
second          ********        initialview
third           ********        v1v2only

3 out of 3 Total entries displayed
--------------------------------------------------------------------------------

TOKYO>:5# config snmp-v3 community secname third new-secname private
TOKYO>:5# config snmp-v3 community info

================================================================================
                                    Community Table
================================================================================
INDEX           NAME            SECURITYNAME    TRANSPORT TAG
--------------------------------------------------------------------------------
first           ********        readview
second          ********        initialview
third           ********        private

3 out of 3 Total entries displayed
--------------------------------------------------------------------------------

TOKYO>:5# config snmp-v3 community commname third new-commname private
TOKYO>:5# config snmp-v3 community info

================================================================================
                                    Community Table
================================================================================
INDEX           NAME            SECURITYNAME    TRANSPORT TAG
--------------------------------------------------------------------------------
first           ********        readview
second          ********        initialview
third           ********        private

3 out of 3 Total entries displayed
--------------------------------------------------------------------------------
```

Configuring trap notifications

With release 3.7, you configure traps by creating SNMPv3 trap notifications, creating a target address to which you want to send the notifications, and specifying target parameters. Nortel Networks provides two default entries in the notify table: Inform and Trap. The tag values for these entries are informTag and trapTag, respectively. For more information about configuring traps using release 3.7, see *Release Notes for the Passport 8000 Series Switch Software 3.7*.

Creating a notify table

You use a notify table to select management targets that should receive notifications, as well as the type of notification that should be sent to each selected management target. Refer to RFC 3413 for detailed information on creating a notify table.

To create a new notify table on the Passport 8000 Series switch, enter the following command:

```
config snmp-v3 notify create <Notify Name> [tag <value>]
[type <value>]
```

The **`config snmp-v3 notify create`** command includes the following options:

`config snmp-v3 notify create` followed by:	
`Notify Name`	The index of the notify table.
`tag <value>`	The tag value used to select the entries in snmpTargetAddrTable.
`type <value>`	The type assigned to the community string name. The valid options are trap and inform.

Other notify commands

The following are additional **`config snmp-v3 notify`** commands:

`config snmp-v3 notify` followed by:	
`info`	Displays the notify table information.
`delete <Notify Name>`	Deletes a user group for the notify table.
`tag <Notify Name> new-tag <value>`	Specifies the new tag value that you want to use to select the entries in snmpTargetAddrTable.
`type <Notify Name> new-type <value>`	Specifies the new type value that you want assigned to the community string name. The valid options are trap and inform.

Configuration example: SNMPv3 group

The following configuration example uses the commands described above to:

- Create a new notify, notify1, type inform.
- Create a new notify, notify2, type trap.
- View the notify table information.
- Delete notify2 from notify.

Figure 26 config snmp-v3 notify commands

```
Passport-8603:3# config snmp-v3 notify create notify1 type inform
Passport-8603:3# config snmp-v3 notify create notify2 type trap
Passport-8603:3# config snmp-v3 notify info
================================================================
                                    Notify Configuration
================================================================
Notify Name                     Tag                             Type
----------------------------------------------------------------
group3                          group3                          inform
notify1                                                         inform
notify2                                                         trap
Passport-8603:3# config snmp-v3 notify delete notify2
Passport-8603:3# config snmp-v3 notify info
================================================================
                                    Notify Configuration
================================================================Notify
Name                    Tag                                 Type
----------------------------------------------------------------
group3                          group3                          inform
notify1                                                         inform
Passport-8603:3#
```

Creating a notify profile table

You use a notify profile table to associate a notification filter profile with a particular set of target parameters. Refer to RFC 3413 for detailed information on notify filter profile table.

To create a new notify profile table on the Passport 8000 Series switch, enter the following command:

`config snmp-v3 ntfy-profile create <`*`Params Name`*`> [profile <`*`value`*`>]`

where:
`profile` *`value`* is the name of the filter profile used while generating notifications in snmpTargetAddrTable.

Other ntfy-profile commands

The following are additional **`config snmp-v3 ntfy-profile`** commands:

`config snmp-v3 ntfy-profile` followed by:	
`info`	Displays the notify profile information.
`delete <Params Name>`	Deletes the specified notify profile.
`profile <Params Name> <new-profile>`	Specifies the new filter profile to be used while generating notifications in snmpTargetAddrTable.

Configuration example: SNMPv3 group

The following configuration example uses the commands described above to:

- Create a new notify profile, ntfy-profile, in tparm.
- Create a new notify profile, ntfy-profile, in tparm1
- View the notify profile information.
- Delete tparm1 from ntfy-profile

Figure 27 config snmp-v3 ntfy-profile commands

```
Passport-8603:3# config snmp-v3 ntfy-profile create tparm
Passport-8603:3# config snmp-v3 ntfy-profile create tparm1
Passport-8603:3# config snmp-v3 ntfy-profile info
=====================================================================
Notify Profile Configuration
=====================================================================
Params Name                       Profile Name
---------------------------------------------------------------------
tparm
tparm1
Passport-8603:3# config snmp-v3 ntfy-profile delete tparm1
Passport-8603:3# config snmp-v3 ntfy-profile info
=====================================================================
Notify Profile Configuration
=====================================================================
Params Name                       Profile Name
---------------------------------------------------------------------
tparm

Passport-8603:3#
```

Creating a notify filter table

A notify filter table contains a list of profiles. You use filter profiles to determine whether particular management targets should receive particular notifications. Refer to RFC 3413 for detailed information on notify filter table.

To create a new notify filter table on the Passport 8000 Series switch, enter the following command:

```
config snmp-v3 ntfy-filter create <Profile Name> <subtree
oid> [mask <value>] [type <value>]
```

where:
Profile Name is the name of the profile.
subtree oid is identifies the filter subtree object.
mask <*value*> is the bit mask in combination with snmpNotifyFilterMask, which defines a family of subtrees.
type <*value*> indicates whether the family of filter subtrees defined by this entry are included or excluded from a filter.

Other ntfy-filter commands

The following are additional **config snmp-v3 ntfy-filter** commands:

config snmp-v3 ntfy-filter followed by:	
info	Displays the notify filter information.
delete <*Profile Name*> <*subtree oid*>	Deletes the specified notify profile.
mask <*Profile Name*> <*subtree oid*> new-mask <*value*>	Specifies the new bit mask in combination with snmpNotifyFilterMask defines a family of subtrees.
type <*Profile Name*> <*subtree oid*> new-type <*value*>	Specifies the new type that you want for a profile. The valid values are included and excluded.

Configuration example: SNMPv3 group

The following configuration example uses the commands described above to:

- Create a new ntfy-filter, vrrpprofile,subtree 1.3.6.1.2.1.46.1.1.15.0
- View ntfy-filter information.

Figure 28 config snmp-v3 ntfy-filter commands

```
Passport-8603:3# config snmp-v3 ntfy-filter create vrrpprofile
1.3.6.1.2.1.46.1.1.15.0
Passport-8603:3# config snmp-v3 ntfy-filter info
================================================================
                                      Notify Filter Configuration
================================================================
Profile Name                    Subtree                Mask
   Type
----------------------------------------------------------------
vrrpprofile                      1.3.6.1.2.1.46.1.1.15.0
   include
Passport-8603:3#
```

Creating a new target address table

A target address table contains a list of transport addresses to be used in the generation of SNMP messages. Refer to RFC 3413 for detailed information on creating a target table.

To create a new target address table on the Passport 8000 Series switch, enter the following command:

```
config snmp-v3 target-addr create <Target Name> <Ip
addr:port> <Target parm> [timeout <value>] [retry <value>]
[taglist <value>] [mask <value>] [mms <value>]
```

The **`config snmp-v3 target-addr create`** command includes the following options:

`config snmp-v3 target-addr create` followed by:	
Ipaddr:port	The IP address and the host of the target and the UDP port number. **Note:** Port 162 is reserved for SNMP traps.
`mask <value>`	The mask value associated with an entry in the snmpTargetAddrTable.
`mms <value>`	The maximum message size value associated with an entry in the snmpTargetAddrTable.

config snmp-v3 target-addr create followed by:	
Target parm	The string value that identifies snmpTargetParamsTable entries.
retry <*value*>	The number of retries to be attempted when a response is not received for a generated message.
taglist <*value*>	Specifies a list of tag values. A tag value refers to a class of targets to which the messages may be sent
timeout <*value*>	The maximum round trip time required for communicating with the transport address defined by this row.

Other target-addr commands

The following are additional **config snmp-v3 target-addr** commands:

config snmp-v3 target-addr followed by:	
info	Displays the target-address information.
delete <*Target Name*>	Deletes a user group for the target-address table.
address <*Target Name*> new-addr <*value*>	Specifies a new IP address for the target.
mask <*Target Name*> new-mask <*value*>	Specifies a new mask for the target.
mms <*Target Name*> new-mms <*value*>	Specifies a new maximum message size associated with an entry in the snmpTargetAddrTable.
parms <*Target Name*> new-parms <*value*>	Specifies a new string value that identifies snmpTargetParams Table entries.
retry <*Target Name*> new-retry <*value*>	Specifies a new number of retries to be attempted when a response is not received for a generated message.
taglist <*Target Name*> new-taglist <*value*>	Specifies a new list of tag values.
timeout <*Target Name*> new-timeout <*value*>	Specifies a new maximum route trip time required for communicating with the transport address defined by this row.

Configuration example: SNMPv3 group

The following configuration example uses the commands described above to:

- Create a new target address, station 1, using 10.1.1.1 for 162.
- Create a new target address station 2, using 10.1.1.2 for 162.
- Delete target address station 2 from tparm.
- View the group member information

Figure 29 config snmp-v3 target-addr commands

```
Passport-8603:3# config snmp-v3 target-addr create station1 10.1.1.1:162
tparm timeout 10 retry 3
Passport-8603:3# config snmp-v3 target-addr create station2 10.1.1.2:162
tparm
Passport-8603:3# config snmp-v3 target-addr info
================================================================
Target Address Configuration
================================================================
Target Name                      TDomain                 TAddress
TMask
----------------------------------------------------------------
station1                  snmpCommunityIndex.1.1  10.1.1.1:162
station2                  snmpCommunityIndex.1.1  10.1.1.2:162
================================================================
Target Address Configuration
================================================================
Target Name                     Timeout Retry TagList
Params                           MMS
----------------------------------------------------------------
station1                        10      3
tparm                            484
station2                        1500    3
tparm                            484
Passport-8603:3#
Passport-8603:3# config snmp-v3 target-addr delete station2
Passport-8603:3# config snmp-v3 target-addr info
================================================================
                                        Target Address Configuration
================================================================
Target Name                      TDomain                 TAddress
TMask
----------------------------------------------------------------
station1                  snmpCommunityIndex.1.1  10.1.1.1:162
================================================================
Target Address Configuration
================================================================
Target Name                     Timeout Retry TagList
Params                           MMS
----------------------------------------------------------------
station1                        10      3
tparm                            484
Passport-8603:3#
```

Creating a new target parameter table

A target params table contains a list of SNMP target information to be used in the generation of SNMP messages. Refer to RFC 3413 for detailed information on creating a target params table.

To create a new target parameter table on the Passport 8000 Series switch, enter the following command:

```
config snmp-v3 target-param create <target param name>
mp-model <value> sec-level <value> sec-name <value>
```

The **`config snmp-v3 target-param create`** command includes the following options:

`config snmp-v3 target-param create` followed by:	
`mp-model <value>`	The SNMP version. The valid options are snmpv1, snmpv2c, and usm (SNMPv3).
`sec-level <value>`	The security level. The valid options are noAuthNoPriv, authNoPriv, and authPriv.
`sec-name <value>`	The security name, which identifies the principal to generate SNMP messages.

Other target-param commands

The following are additional **`config snmp-v3 target-param`** commands:

`config snmp-v3 target-param` followed by:	
`info`	Displays information for the target parameter table.
`delete <target param name>`	Deletes the specified target parameter table.
`mp-model <target param name> new-mpmodel <value>`	Specifies the a new SNMP version. The valid options are snmpv1, snmpv2c, and usm (SNMPv3).

config snmp-v3 target-param followed by:	
sec-level <*target param name*> new-seclevel <*value*>	Specifies a new security level. The valid options are noAuthNoPriv, authNoPriv, and authPriv.
sec-name <*target param name*> new-secname <*value*>	Specifies a new security name, which identifies the principal to generate SNMP messages.

Configuration example: SNMPv3 group

The following configuration example uses the commands described above to:

- Create a new target param, tparm, using mp model USM for sec-level.
- Create a new target param, tparm1, using mp model USM for sec-level.
- Delete group tparm from target-param.
- View the group member information

Figure 30 config snmp-v3 target-param commands

```
Passport-8603:3#  config snmp-v3 target-param create tparm1 mp-model usm sec-level
authPriv sec-name user1
Passport-8603:3# config snmp-v3 target-param info
================================================================
Target Params Configuration
================================================================
Target Name                    MP Model  User Name                    Sec Level
----------------------------------------------------------------
tparm                          usm                                    noAuthNoPriv
tparm1                          usm       user1                       authPriv
Passport-8603:3# config snmp-v3 target-param delete tparm
Passport-8603:3# config snmp-v3 target-param info
================================================================
Target Params Configuration
================================================================
Target Name                    MP Model  User Name                    Sec Level
----------------------------------------------------------------
tparm1                          usm       user1                       authPriv
Passport-8603:3#
```

SNMPv3 configuration example

The following procedure shows how to create a user for SNMPv3, create a group for that user, assign view access for that group, and create and assign a MIB view for that group.

1. Create a user (for example, rdalton).

   ```
   config snmp-v3 usm create rdalton md5 auth password
   ```

2. Create a group and assign it to the user.

   ```
   config snmp-v3 group-member create rdalton usm newgroup
   ```

3. Assign view access for the newly created group.

   ```
   config snmp-v3 group-access create newgroup "" usm
   authNoPriv
   ```

4. Create a MIB view.

   ```
   config snmp-v3 mib-view create newmibview 1.3
   ```

5. Assign a MIB view for the group.

   ```
   config snmp-v3 group-access view newgroup "" usm
   authNoPriv read newmibview write newmibview
   ```

SNMPv1/SNMPv2 configuration example

The following procedure shows how to create a user for SNMPv1 or SNMPv2, create a group for that user, and assign view access and a MIB view for that group.

1. Create a user. For this example, *index1* is the index of the entry, *newgroup* is the community string that will be used for login, and *initialview* is the security name that is associated with the group-member table (VCAM table).

   ```
   config snmp-v3 community create index1 newgroup
   initialview
   ```

2. Create a group and assign it to a user for SNMPv1 or SNMPv2. For this example, *newgroupgrp* is the group that belongs to the community *newgroup*.

```
config snmp-v3 group-member create initialview snmpv1
newgroupgrp
```
or
```
config snmp-v3 group-member create initialview snmpv2c
newgroupgrp
```

3 Assign view access for the newly created group.

```
config snmp-v3 group-access create newgroupgrp "" snmpv1
noAuthNoPriv
```
or
```
config snmp-v3 group-access create newgroupgrp "" snmpv2c
noAuthNoPriv
```

4 Assign a MIB view for the group. For this example, use the *root* MIB view; if this does not exist, use *org*.

```
config snmp-v3 group-access view newgroupgrp "" snmpv1
noAuthNoPriv read root write root
```
or
```
config snmp-v3 group-access view newgroupgrp "" snmpv2c
noAuthNoPriv read root write root
```

Note: You can also create your own MIB view by using the command `config snmp-v3 mib-view create <View Name> <subtree oid> [mask <value>] [<type <value>]` (see "Creating a new entry for the MIB in the View table" on page 107 for instructions). After you create a MIB view, you can then assign it to a group.

Displaying SNMP system information

To display SNMP system information on the Passport 8000 Series switch, enter the following command:

```
show config module sys
```

Configuration example: show SNMP system information

Figure 31, Figure 32, and Figure 33 show sample output for the **`show config module sys`** command to display SNMP system information.

Figure 31 show config module sys command sample output

```
TOKYO>:5# show config module sys
Preparing to Display Configuration...
#
# TUE MAY 11 18:46:06 2004 UTC
# box type             : Passport-8006
# software version     : REL3.7.0.0_B085
# monitor version      : 3.7.0.0/085
#

#
# Asic Info :
# SlotNum|Name   |CardType    |MdaType |Parts Description
#
# Slot   1 8681XLR   0x22334101 0x00000000    IOM: TENGMAC=0   BFM: OP=3 TMUX=2 RARU
=4 CPLD=5
# Slot   2 8672ATME 0x20550108 0x00000001   0x20550201   BFM: OP=255 TMUX=2 RARU=0
CPLD=5
# Slot   3 8608SX    0x20320108 0x00000000    IOM: GMAC=5   BFM: OP=2 TMUX=2 RARU=2
CPLD=4
# Slot   4 8632TXE   0x20210120 0x00000000    IOM: PLRO=3   GMAC=5   BFM: OP=3 TMUX=2
 RARU=4 CPLD=5
# Slot   5 8690SF    0x200e0100 0x00000000   CPU: CPLD=14 SFM: OP=2 TMUX=2 SWIP=2 F
AD=1 CF=11
# Slot   6 8690SF    0x200e0100 0x00000000   CPU: CPLD=14 SFM: OP=2 TMUX=2 SWIP=2 F
AD=1 CF=11
config

# LICENSE CONFIGURATION
mac-flap-time-limit 500

#

# SYSTEM CONFIGURATION
#
#
# LOG CONFIGURATION
#
#
# LINK-FLAP-DETECT CONFIGURATION
#
#
# IEEE VLAN AGING CONFIGURATION
```

Figure 32 show config module sys command sample output continued

```
#
# ACCESS-POLICY CONFIGURATION
#

sys access-policy enable true
sys access-policy policy 2 create
sys access-policy policy 2 name ""
sys access-policy policy 2 username ""
#
# SSH CONFIGURATION
#
sys set ssh enable true

#
# MCAST SOFTWARE FORWARDING CONFIGURATION
#

#
# SNMP V3 GROUP MEMBERSHIP CONFIGURATION
#
snmp-v3 group-member create usmuser usm usmusergrp

#
# SNMP V3 GROUP ACCESS CONFIGURATION
#

snmp-v3 group-access create usmusergrp "" usm noAuthNoPriv
snmp-v3 group-access view usmusergrp "" usm noAuthNoPriv read "" write "" notify
 ""

#
# SNMP V3 MIB VIEW CONFIGURATION
#

#
# SNMP V3 NOTIFY CONFIGURATION
#

snmp-v3 notify create DefNotify tag defTag type trap

#
# SNMP V3 TARGET ADDRESS CONFIGURATION
#
#
```

Figure 33 show config module sys command sample output concluded

```
#
# SNMP V3 TARGET PARAMS CONFIGURATION
#

snmp-v3 target-param create TparamV1 mp-model snmpv1 sec-level noAuthNoPriv sec-name
readview
snmp-v3 target-param create TparamV2 mp-model snmpv2c sec-level noAuthNoPriv sec-name
readview

#
# SNMP V3 NOTIFY FILTER CONFIGURATION
#

#
# SNMP V3 NOTIFY FILTER PROFILE CONFIGURATION
#

#
# DNS CONFIGURATION
#

sys dns primary-create 47.81.2.10

sys dns secondary-create 47.82.2.10

#
# SLOT CONFIGURATION
#

#
# GLOBAL EAP CONFIGURATION
#

back
TOKYO>:5#
```

Note: To maintain security, the USM table is not displayed. This prevents viewing of the USM auth and priv passwords. When you chose **`save config`**, the usm table is saved in an encrypted file called `snmp_usm.txt` without the default entries.

Blocking SNMP

You disable SNMP access to the Passport 8600 by entering the following commands:

```
Passport-8610:5#config bootconfig flags block-snmp true
Passport-8610:5#save boot
Passport-8610:5#boot -y
```

By default, SNMP access is enabled. To reenable SNMP access, enter the following command:

```
Passport-8610:5#config bootconfig flags block-snmp false
```

Chapter 7
Configuring SNMPv3 using Device Manager

An SNMPv3 engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one-to-one association between an SNMP engine and the SNMP entity, which contains it.

This chapter includes the following topics:

Loading the encryption module

Before you can access the switch using SNMPv3 with DES encryption, you must load the encryption module, p80c3700.des, which allows you to use the Privacy protocol.

Note: You must install the p80c3700.des encryption module only when encryption is required (that is, communication between a network management application and the Passport 8600). The SNMPv3 protocol can work successfully without this module.

1. Open a browser and enter the following URL:

   `www.nortelnetworks.com`

2. Select “Software Downloads” under the Support heading.
3. Select “Passport” under Product family.
4. Find “Passport 8600 Routing Switch.”
5. Click on the “Software” link.
6. Click on the “Passport 8600 SNMPv3/DES” link.
7. Log in.
8. Answer the questions on the questionnaire.
9. Click submit.
10. Right mouse click on file download link and enter a file location in which to copy the DES encryption module.
11. Click OK.
12. The file is downloaded.

Note: Note the location of this file. You will need to load the file on the switch before you can use the protocol.

13. Now, FTP this file to the switch. Open the DOS window.
14. FTP to the Passport 8000 Series switch. Figure 34 shows sample output from an FTP session.

Figure 34 FTP sample output from DOS window

```
c:\ftp <10.10.10.10>
Connected to <10.10.10.10>
220 Passport FTP server ready
User (<10.10.10.10>:(none)): rwa
331 Password required
Password: ***
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put <path to file on the PC>
```

15 Go back to the Passport 8000 Series switch and load the module.

```
config load-module DES /flash/p80c3700.des
```

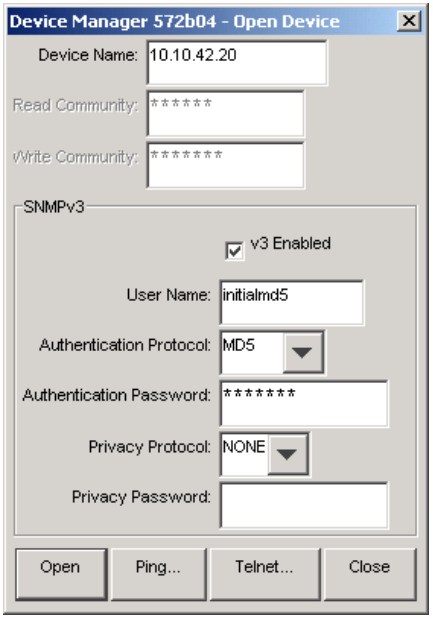
Logging on using SNMPv3

To log on using SNMPv3, you must configure SNMPv3. See "Creating a user security model process" on page 137.

1 In the Device Manager, click Open.

The Open Device dialog box appears. (Figure 35)

Figure 35 Open Device dialog box



A description of the Open Device dialog box fields is shown in Table 10.

2 Enter the device IP address in the Device Name field.

3 Select the v3 Enabled check box.

4 Enter a user name in the User Name field.

5 Select MD5 in the Authentication Protocol field.

6 Enter the Authentication password.

7 Select NONE in the Privacy Protocol field.

8 Click Open.

Device Manager opens.

Table 10 Open Device box fields

Field	Description
User Name	Indicates the name of the user in usmUser.
Authentication Protocol	Identifies the Authentication protocol used.
Authentication Password	A password that is used for authentication purposes. If no value is entered, assume the entry has no authentication capability.
Privacy Protocol	Identifies the privacy protocol used.
Privacy Password	A password that is used for privacy purposes. If no value is entered, assume the entry has no privacy capability. (**Note:** Privacy has to be set with authentication.)

Creating a user security model process

This section covers the process for creating a user Security model (USM).

- "Creating a USM" on page 137
- "Creating membership for a group" on page 141
- "Creating access for a group" on page 143

Creating a USM

Note: You must configure a valid SNMPv3 user through the CLI before you can access the SNMPv3 USM table, VACM table, and Community table.

To create a user security model (USM):

1 From the Device Manager menu bar, click Edit > SnmpV3 > USM Table.

The USM dialog box opens. (Figure 36)

Figure 36 USM dialog box

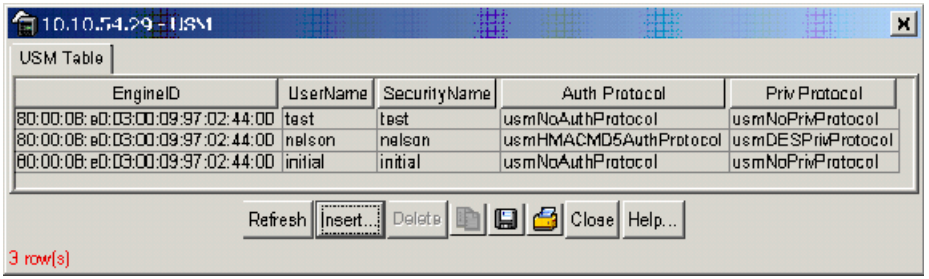


Table 11 describes the USM tab fields.

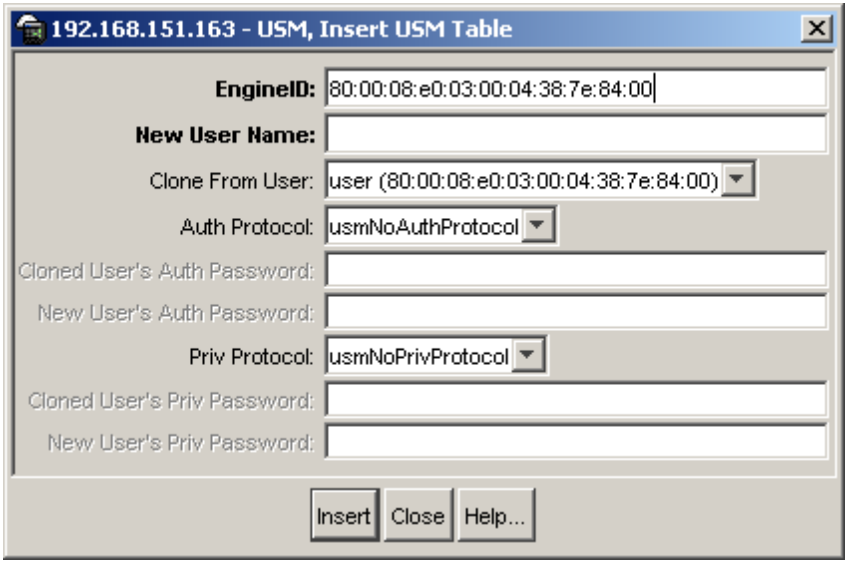
Table 11 USM dialog box fields

Field	Description
EngineID	Indicates the SNMP engine's administratively-unique Identifier.
UserName	The name of the user in usmUser.
SecurityName	Creates the name used as an index to the table. The range is 1 to 32 characters.
Auth Protocol	Identifies the Authentication protocol used.
Priv Protocol	Identifies the privacy protocol used.

2 Click Insert.

The USM, Insert USM Table dialog box opens. (Figure 37)

Figure 37 USM—Insert USM Table dialog box



3. Update the EngineID, if required. This is the value of the Engine-Id associated with the entry in USM table. By default, this is the engine-id used by the switch.
4. Enter a new user name.
5. In the CloneFrom field, select a security name from which the new entry copies authentication data and private data.
6. Select an authentication protocol.
7. Enter the cloned user's authentication password.
8. Enter the new user's authentication password.
9. Select a privacy protocol.
10. Enter the cloned user's privacy password (if one exists).
11. Enter the new user's privacy password (if desired).
12. Click Insert.

The USM dialog opens. The new user model is shown in the list.

Caution: To ensure security, change the GroupAccess table default views after you have set up new users in USM table. This prevents unauthorized people from accessing the switch using the default user login. Also, change Community table defaults, since the community name is used as a community string in SNMPv1/v2 PDU.

Table 12 describes the USM, Insert USM Table dialog box fields.

Table 12 USM—Insert USM Table dialog box fields

Field	Description
EngineID	Read-only field that indicates the SNMP engine's administratively-unique identifier.
New User Name	Creates the new entry with this security name. The name is used as an index to the table. The range is 1 to 32 characters.
Clone From User	Specifies the security name from which the new entry must copy privacy and authentication parameters. The range is 1 to 32 characters.
Auth Protocol (Optional)	Assigns an authentication protocol (or no authentication) from a pulldown menu. If you select this, you must enter the Cloned User's Auth Password and a New User's Auth Password.
Cloned User's Auth Password	Specifies the cloned user's authentication password.
New User's Auth Password	Specifies the new user's authentication password.
Priv Protocol (Optional)	Assigns a privacy protocol (or no privacy) from a pulldown menu. If you select this, you must enter the Cloned User's Priv Password and the New User's Priv Password.
Cloned User's Priv Password (Optional)	Specifies the cloned user's privacy password.
New User's Priv Password (Optional)	Specifies the new user's privacy password.

Creating membership for a group

To add membership for a group in the view-based access control model (VACM):

1 From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

The VACM dialog box opens with the Group Membership tab displayed. (Figure 38)

Figure 38 VACM dialog box

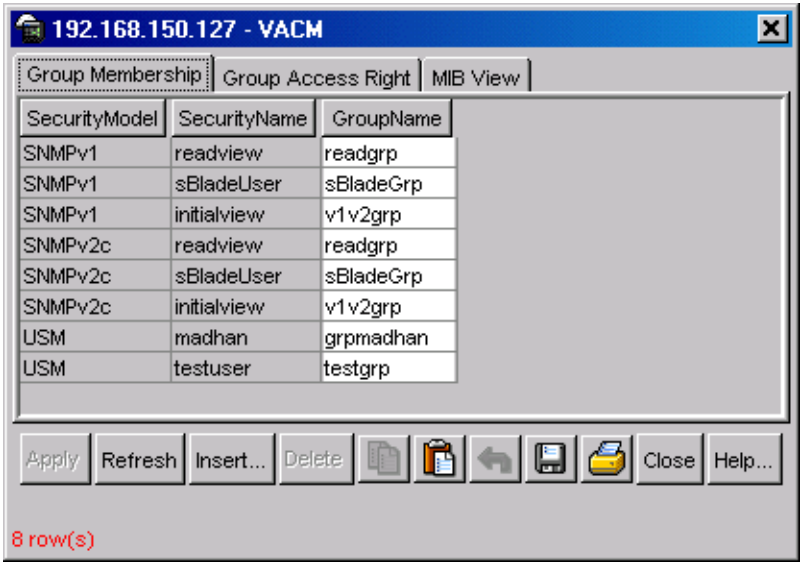


Table 13 describes the VACM tab fields.

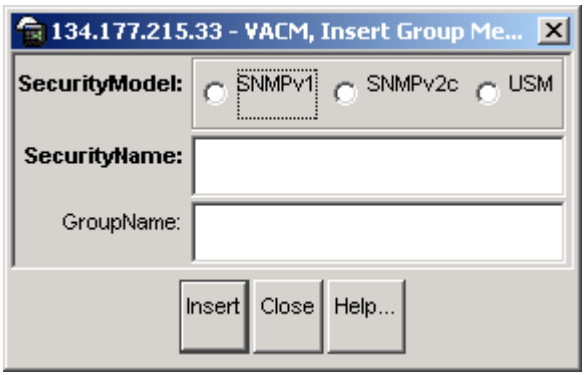
Table 13 VACM dialog box tab fields

Field	Description
SecurityModel	The security model currently in use.
SecurityName	The name representing the user in USM user. The range is 1 to 32 characters.
GroupName	The name of the group to which this entry (combination of securityModel and securityName) belongs.

2 Click Insert.

The VACM, Insert Group Membership dialog box opens. (Figure 39)

Figure 39 VACM—Insert Group Membership dialog box



3 Select a SecurityModel (choose SNMPv1, SNMPv2c, or USM).

4 Enter a SecurityName.

5 Enter a GroupName.

6 Click Insert.

The VACM dialog box updates with the new group membership added to the list.

Table 14 describes the Insert Group Membership tab fields.

Table 14 VACM dialog box—Insert Group Membership tab fields

Field	Description
SecurityModel	The authentication checking to communicate to the switch. Choose an option either SNMPv1, SNMPv2c, or USM.
SecurityName	The security name assigned to this entry in the VACM table. The range is 1 to 32 characters.
GroupName	The name assigned to this group in the VACM table. The range is 1 to 32 characters.

Creating access for a group

To create new access for a group:

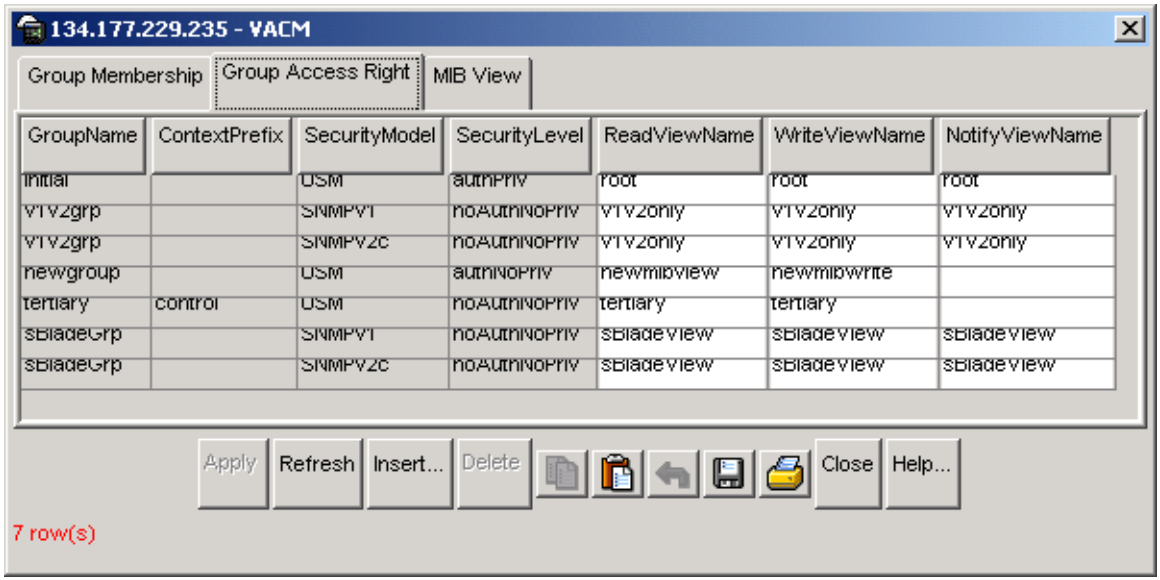
1 From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

The VACM dialog box opens with the Group Membership tab displayed. (Figure 38)

2 Click the Group Access Right tab.

The Group Access Right tab displays. (Figure 40)

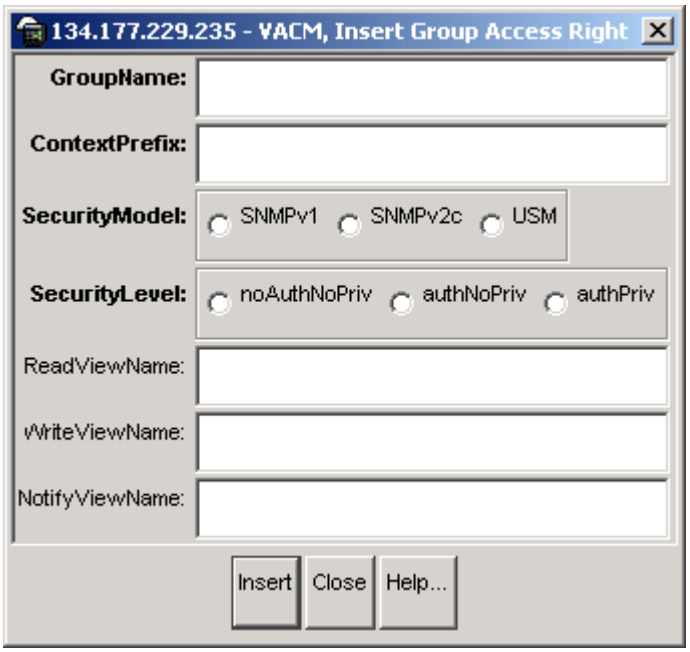
Figure 40 VACM dialog box—Group Access Right tab



3 Click Insert.

The VACM, Insert Group Access Right dialog box opens. (Figure 41)

Figure 41 VACM dialog box—Insert Group Access Right dialog box



4 Enter a GroupName.

5 Enter a ContextPrefix. The only supported prefix is the empty string (““).

6 Select a SecurtyModel (choose SNMPv1, SNMPv2c, or USM).

7 Select a SecurityLevel (choose noAuthNoPriv, authNoPriv, or authPriv).

8 If desired, select a ContextMatch (choose exact or prefix).

9 In the ReadViewName field, enter the name of the MIB view authorized for read access.

10 In the WriteViewName field, enter the name of the MIB view authorized for write access.

11 In the NotifyViewName field, enter the name of the MIB view authorized for notification access.

12 Click Insert.

The VACM Group Access Right dialog box updates with the new group access shown in the list.

Table 15 describes the Insert Group Access tab fields.

Table 15 VACM dialog box—Insert Group Access Right tab fields

Field	Description
GroupName	The name of the new group name in the VACM table. The name is a numeral. The range is 1 to 32 characters.
ContextPrefix	The contextPrefix name must match exactly or partially to the value of the instance of this object. The range is an SnmpAdminString, 1 to 32 characters. Currently, only the empty string prefix is supported.
SecurityModel	The authentication checking to communicate to the switch. The security models are: • SNMPv1 • SNMPv2c • USM
SecurityLevel	The minimum level of security required to gain the access rights allowed. The security levels are: • noAuthNoPriv • authNoPriv • authPriv
ReadViewName	The name of the MIB view authorized for read access.
WriteViewName	The name of the MIB view authorized for write access.
NotifyViewName	The name of the MIB view authorized for notification access

Assigning MIB view access for an object

To assign MIB view access for an object:

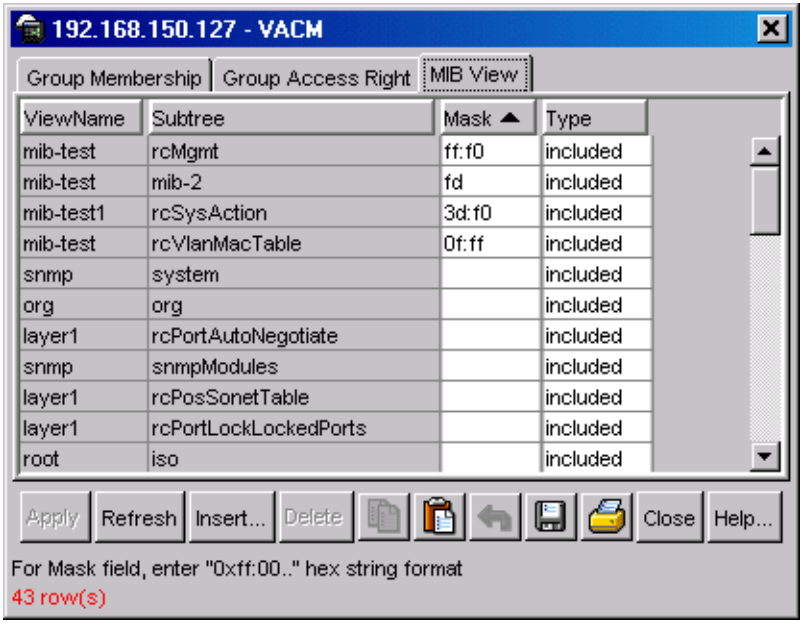
1. From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

   The VACM dialog box opens. (Figure 38)

2. Select the MIB View tab.

   The MIB View tab opens. (Figure 42)

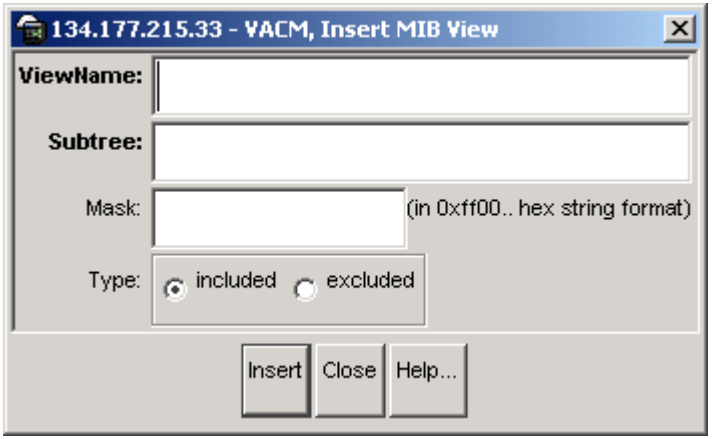
Figure 42 VACM dialog box—MIB View tab



3 Click Insert.

The VACM, Insert MIB View dialog box opens. (Figure 43)

Figure 43 VACM—Insert MIB View dialog box



4 Enter a ViewName.

5 Enter a Subtree.

6 Enter a Mask.

7 Select a Type (choose included or excluded).

8 Click Insert.

The VACM MIB View dialog box updates with the new MIB view shown in the list.

Table 16 describes the MIB View tab fields.

Table 16 VACM dialog box—MIB View tab fields

Field	Description
ViewName	Creates a new entry with this MIB view name. The range is 1 to 32 characters.
Subtree	Any valid object identifier that defines the set of MIB objects accessible by this SNMP entity, for example, 1.3.6.1.1.5
Mask (Optional)	Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.
Type	Determines whether access to a mib object is granted (Included) or denied (Excluded). Included is the default.

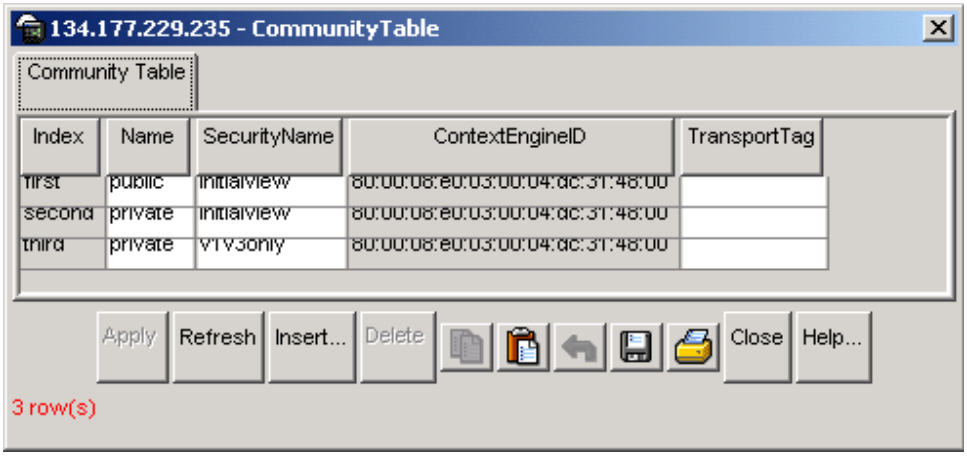
Creating a community

A community table contains objects for mapping between community strings and the security name created in VACM Group Member. To create a community:

1 From the Device Manager menu bar, click Edit > SnmpV3 > Community Table.

The Community Table dialog box opens. (Figure 44)

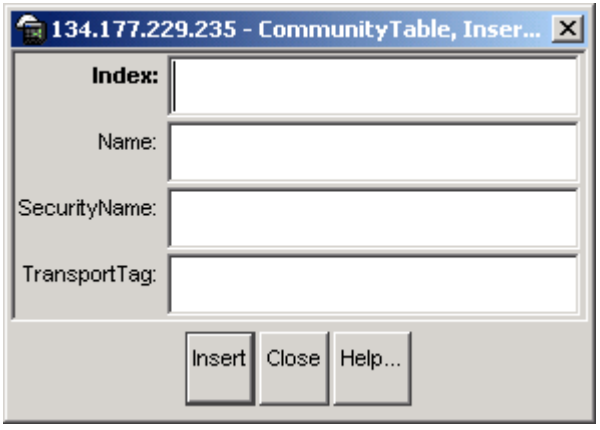
Figure 44 Community Table dialog box



2 Click Insert.

The Community Table, Insert Community Table dialog box opens. (Figure 45)

Figure 45 Community Table—Insert Community Table dialog box



3 Enter an Index.

4 Enter name that is a community string.

5 Enter a SecurityName.

6 Enter a TransportTag.

7 Click Insert.

The Community Table dialog box updates with the new community name shown in the list.

Table 17 describes the Community Table dialog box fields.

Table 17 Community Table dialog box fields

Field	Description
Index	The unique index value of a row in this table. SnmpAdminString 1-32 characters.
Name	The community string for which a row in this table represents a configuration.
SecurityName	The security name assigned to this entry in the Community table. The range is 1 to 32 characters.
ContextEngineID	The context engine ID indicates the location of the context for management information in community string.
TransportTag	The transport tag specifies a set of transport endpoints for a command responder application to accept management requests.

Creating a target table

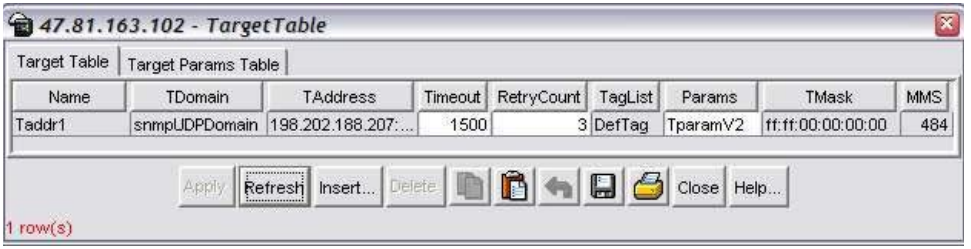
A target table contains a list of transport addresses to be used in the generation of SNMP messages. Refer to RFC 3413 for detailed information on creating a target table.

To create a target table:

1 From the Device Manager menu bar, click Edit > SnmpV3 > Target Table.

The Target Table dialog box opens. (Figure 44)

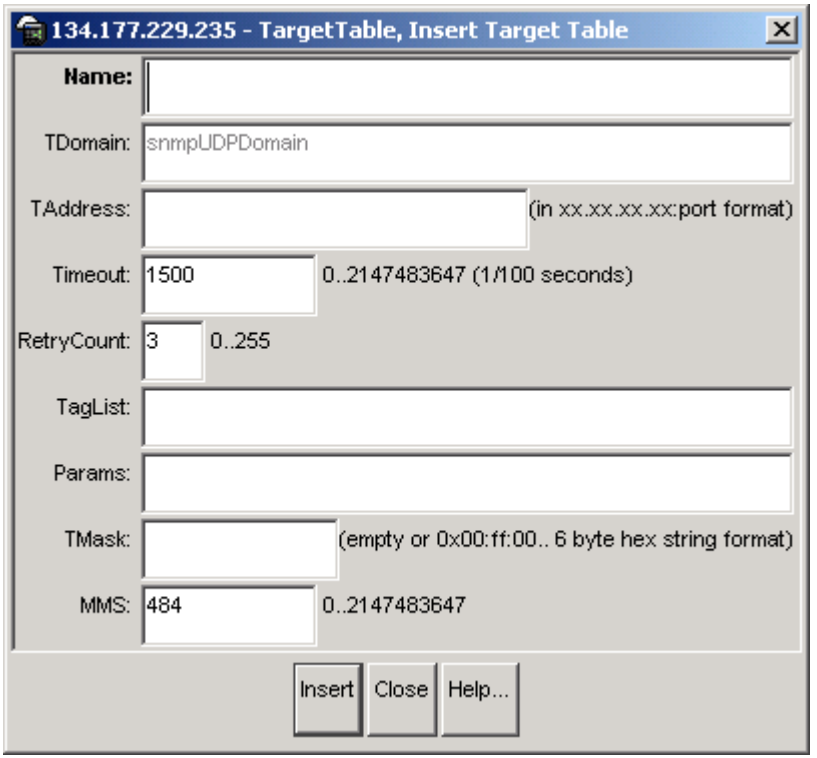
Figure 46 Target Table dialog box



2 Click Insert.

The Target Table, Insert Target Table dialog box opens. (Figure 45)

Figure 47 Target Table—Insert Target Table dialog box



3 Enter name that is a community string.

4 Enter a TAddress in xx.xx.xx.xx:port format.

5 Enter a Timeout value. Value is in 1/100 seconds.

6 Enter a RetryCount value. Value can be from 0 to 255.

7 Enter a TagList.

8 Enter a Params.

9 Enter a TMask. Value can be empty or in 6 byte hex string format.

10 Enter a MMS. Value can be from 0 to 2147483647.

11 Click Insert.

The Target Table dialog box updates with the new community name shown in the list.

Table 18 describes the Target Table dialog box fields.

Table 18 Target Table dialog box fields

Field	Description
Name	The unique identifier to index this table.
TDomain	The transport type of the address in the snmpTargetAddrTAddressobject.
TAddress	The transport address whose format depends on the value of the snmpTargetAddrTAddressobject.
Timeout	The maximum round trip time required for communicating with the transport address defined by this row.
RetryCount	The number of retries to be attempted when a response is not received for a generated message.
TagList	Specifies a list of tag values. A tag value refers to a class of targets to which the messages may be sent .
Params	The value of SnmpAdminString identifies snmpTargetParamsTable entries.
TMask	The mask value associated with an entry in the snmpTargetAddrTable.
MMS	The maximum message size value associated with an entry in the snmpTargetAddrTable.

Creating a target params table

A target params table contains a list of SNMP target information to be used in the generation of SNMP messages. Refer to RFC 3413 for detailed information on creating a target params table.

To create a target params table:

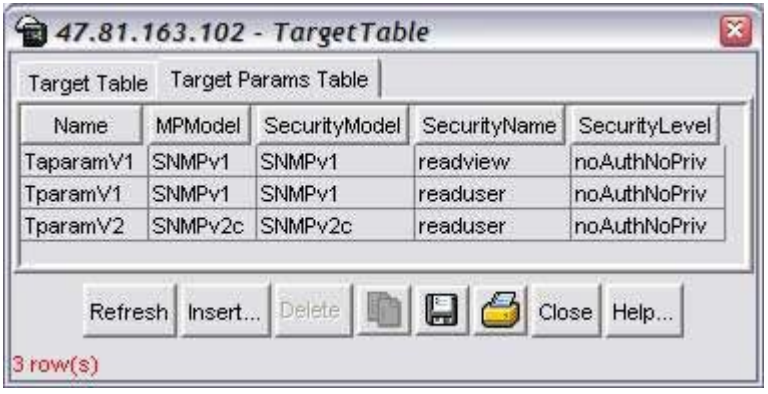
1 From the Device Manager menu bar, click Edit > SnmpV3 > Target Table.

The Target Table dialog box opens. (Figure 44)

2 Click the Target Params Table tab.

The Target Params Table dialog box opens. (Figure 48)

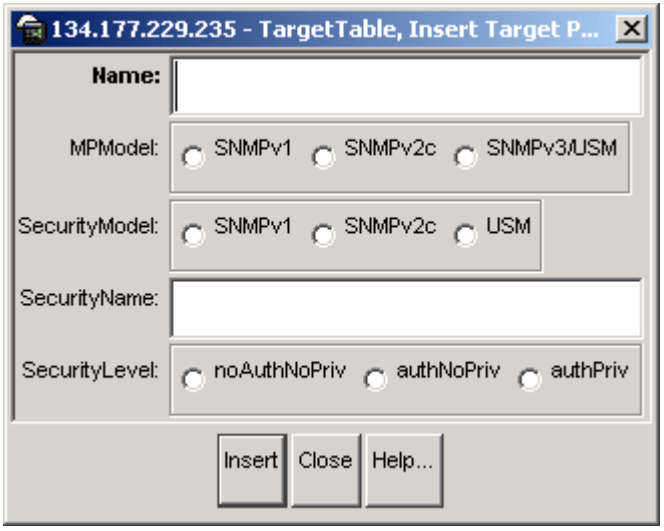
Figure 48 Target Params Table dialog box



3 Click Insert.

The Target Table, Insert Target Params Table dialog box opens. (Figure 49)

Figure 49 Target Table—Insert Target Params Table dialog box



4 Enter name that is a community string.

5 Select a MPModel. Choose from SNMPv1, SNMPv2c, or SNMPv3/USM.

6 Select a SecurityModel. Choose from SNMPv1, SNMPv2c, or USM.

7 Enter a SecurityName.

8 Select a SecurityLevel. Choose from noAuthNoPriv, authNoPriv, or authPriv.

9 Click Insert.

The Target Params Table dialog box updates with the new community name shown in the list.

Table 19 describes the Target Params Table dialog box fields.

Table 19 Target Params Table dialog box fields

Field	Description
Name	The community string for which a row in this table represents a configuration.
MPModel	• SNMPv1 • SNMPv2c • SNMPv3/USM

Table 19 Target Params Table dialog box fields (continued)

Field	Description
SecurityModel	• SNMPv1 • SNMPv2c • USM
SecurityName	The security name identifies the principal to generate SNMP messages using security name entry.
SecurityLevel	• noAuthNoPriv • authNoPriv • authPriv

Creating a notify table

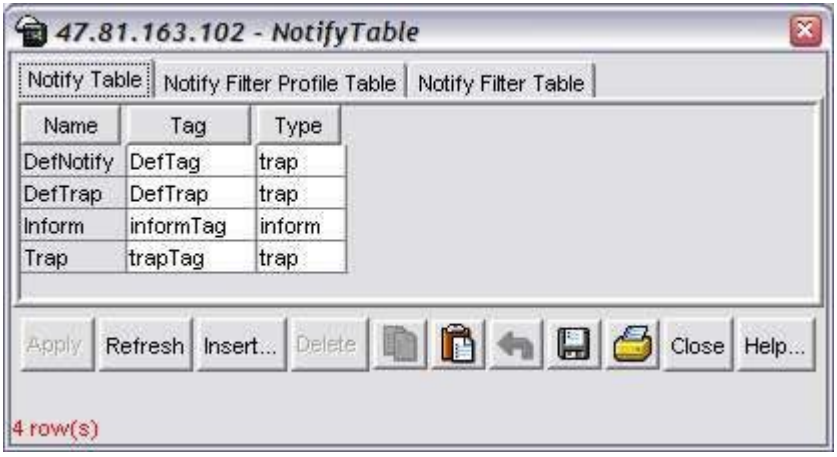
You use a notify table to select management targets that should receive notifications, as well as the type of notification that should be sent to each selected management target. Refer to RFC 3413 for detailed information on creating a notify table.

To create a notify tag for a user:

1 From the Device Manager menu bar, click Edit > SnmpV3 > Notify Table.

The Notify Table dialog box opens. (Figure 50)

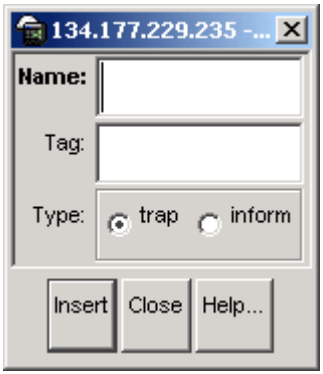
Figure 50 Notify Table dialog box



2 Click Insert.

The Notify Table, Insert Notify Table dialog box opens. (Figure 51)

Figure 51 Notify Table—Insert Notify Table dialog box



3 Enter name that is a community string.

4 Enter a Tag.

5 Select a type (choose either trap or inform).

6 Click Insert.

The Notify Table dialog box updates with the new community name shown in the list.

Table 20 describes the Notify Table dialog box fields.

Table 20 Notify Table dialog box fields

Field	Description
Name	The community string for which a row in this table represents a configuration.
Tag	The tag value used to select the entries in snmpTargetAddrTable.
Type	The type assigned to the community string name. Choices are: • trap • inform

Creating a notify filter profile table

You use a notify filter profile table to associate a notification filter profile with a particular set of target parameters. Refer to RFC 3413 for detailed information on notify filter profile table.

To create a notify filter profile for a user:

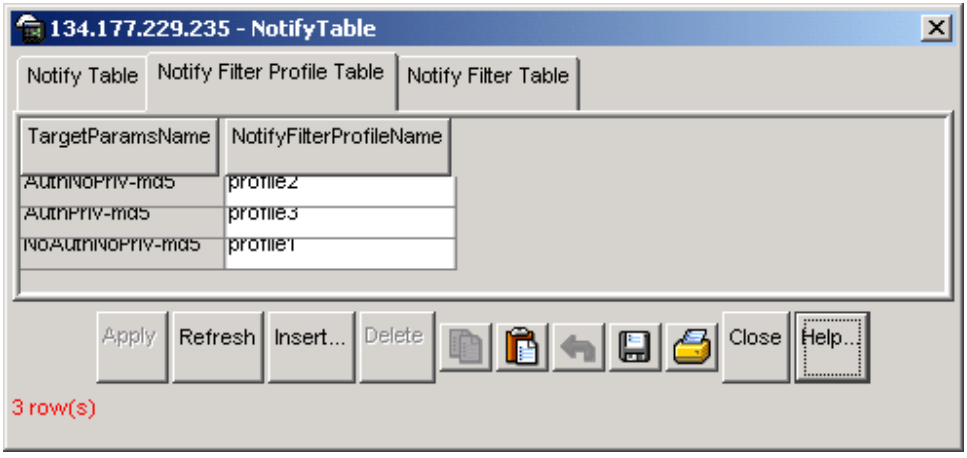
1 From the Device Manager menu bar, click Edit > SnmpV3 > Notify Table.

The Notify Table dialog box opens. (Figure 50)

2 Click the Notify Filter Profile Table.

The Notify Filter Profile Table dialog box opens. (Figure 52)

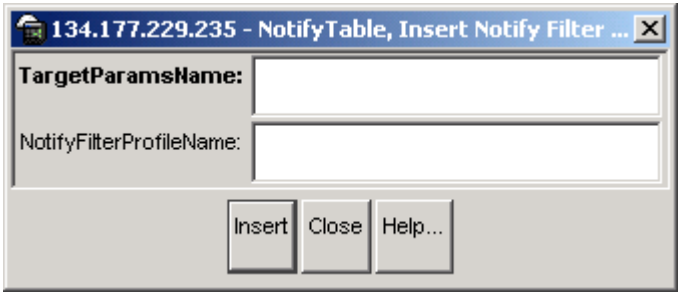
Figure 52 Notify Filter Profile Table dialog box



3 Click Insert.

The Notify Table, Insert Notify Filter Profile Table dialog box opens. (Figure 53)

Figure 53 Notify Table—Insert Notify Filter Profile Table dialog box



4 Enter name that is a TargetParamsName.

5 Enter a NotifyFilterProfileName.

6 Click Insert.

The Notify Filter Profile Table dialog box updates with the new Target Parameter name shown in the list.

Table 21 describes the Notify Filter Profile Table dialog box fields.

Table 21 Notify Filter Profile Table dialog box fields

Field	Description
TargetParamsName	The unique indentifier associated with this entry. SnmpAdminString1-32 characters
NotifyFilterProfile Name	The name of the filter profile used while generating notifications in snmpTargetAddrTable.

Creating a notify filter table

A notify filter table contains a list of profiles. You use filter profiles to determine whether particular management targets should receive particular notifications. Refer to RFC 3413 for detailed information on notify filter table.

To create a notify filter for a user:

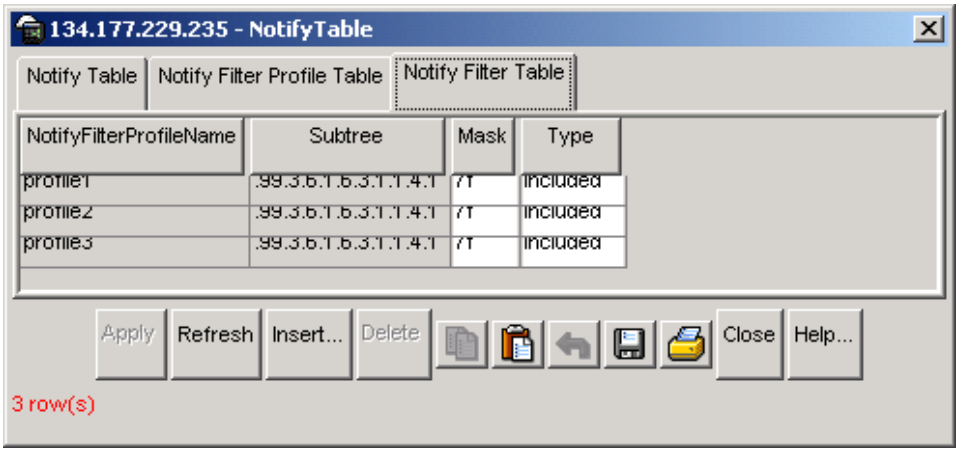
1 From the Device Manager menu bar, click Edit > SnmpV3 > Notify Table.

The Notify Table dialog box opens. (Figure 50)

2 Click the Notify Filter Table.

The Notify Filter Table dialog box opens. (Figure 54)

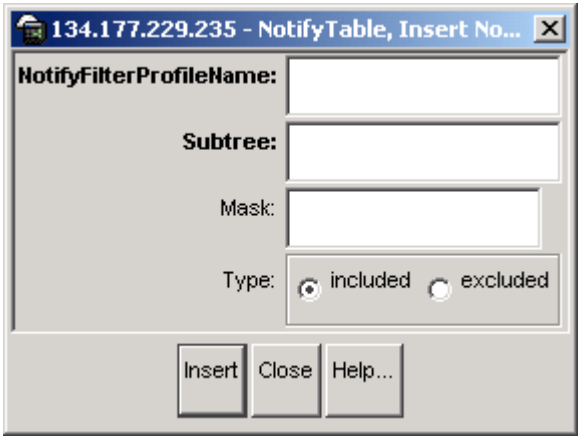
Figure 54 Notify Filter Table dialog box



3 Click Insert.

The Notify Table, Insert Notify Filter Table dialog box opens. (Figure 55)

Figure 55 Notify Table—Insert Notify Filter Table dialog box



4 Enter name that is a NotifyFilterProfileName.

5 Enter a Subtree.

6 Enter a Mask.

7 Enter a Type. (Choose either included or excluded)

8 Click Insert.

The Notify Filter Table dialog box updates with the new Notify name shown in the list.

Table 22 describes the Notify Filter Table dialog box fields.

Table 22 Notify Filter Table dialog box fields

Field	Description
NotifyFilterProfile Name	The name of the filter profile used while generating notifications in snmpTargetAddrTable
Subtree	MIB subtree with the corresponding instance of snmpNotifyFilterMask defines a family of subtrees.
Mask	Bit mask in combination with snmpNotifyFilterMask defines a family of subtrees.
Type	Indicates whether the family of filter subtrees defined by this entry are included or excluded from a filter. The valid options are included and excluded.

Chapter 8
Configuring SSH using the CLI

This chapter includes the following topics:

Roadmap of CLI Secure Shell commands

The following roadmap lists the CLI Secure Shell commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config sys set ssh`	`info`
	`action <action choice> [<integer>]`
	`dsa-auth <true|false>`
	`enable <true|false|secure>`
	`max-sessions <integer>`
	`pass-auth <true|false>`
	`port <integer>`
	`rsa-auth <true|false>`

Command	Parameter
	timeout <integer>
	version <both|v2only>
show sys ssh	global
	session

Configuration prerequisites

Before beginning configuration of the SSH server, make sure the following prerequisites are satisfied:

- The sshd daemon is disabled. All SSH commands except `enable`, require that the sshd daemon be disabled.
- User access level is set to read/write/all community strings.
- All insecure services are disabled. Nortel Networks recommends disabling the following services: SNMP, TFTP, FTP, Telnet, and rlogin.

  To disable the SNMP protocol use the following **`flags`** command:

  `config bootconfig flags block-snmp true`

Nortel Networks recommends using the console port to configure the SSH parameters.

Downloading the 3DES encryption image

Due to export restrictions, the encryption capability has been separated from the main software image. The SSH server will not function properly without the use of this image.

You must load the encryption module, 3DES, which allows you to use SSH.

1. Open a browser and enter the following URL:

   `www.nortelnetworks.com`

2. Select “Software Downloads” under the Support heading.

3. Log in.
4. Select “Passport” under Product family.
5. Find “Passport 8600 Routing Switch”.
6. Click on the “Software” link.
7. Click on the “Passport 8600 SSH/3DES” link.
8. Answer the questions on the questionnaire.
9. Click submit.
10. Right mouse click on file download link and enter a file location in which to copy the 3DES encryption module.
11. Click OK.
12. The file is downloaded.
13. The file needs to be copied from your computer to the switch using FTP. The file should be saved as `/flash/p80c3700.img`. Figure 56 shows sample output from DOS command prompt window.

Figure 56 DOS command prompt output

```
C:\ftp <switch IP address>
Connected to <switch IP address>
220 Passport FTP server ready
User (switch IP address:(none)): rwa
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put (path to file from your computer)\filename.des
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp>
```

14. Go back to the Passport 8000 Series switch and load the module.

```
config load-encryption-module 3DES
```

Enabling the SSH server

Use the **config bootconfig flags** command to enable and disable SNMP sessions to provide secure management traffic and enable and disable the SSH server.

To enable the SSH server on the switch, complete the following steps:

1. Enter the following command:

   config bootconfig flags sshd

2. Save the boot.cfg file using the following **save** command.

   save bootconfig

3. Reboot the switch using the **boot** command.

   boot

The general **config bootconfig flags** command includes the following options.

config bootconfig flags followed by:	
info	Displays the current flag settings for boot configuration.
8100-mode <true|false>	Enables (true) or disables (false) Passport 8100 mode.
alt-led-enable <true|false>	Enables (true) or disables (false) alternate LED behavior.
autoboot <true|false>	Enables (true) or disables (false) autoboot on power-up.
block-warmstandby-switchover <true|false>	Stops (true) secondary CPU in warm standby mode from switching over to primary CPU.
control-record-optimization <true-false>	Enables (true) or disables (false) adding a hardware record for receiving Level 3 protocol control traffic that uses a multicast address.
daylight-saving-time <true|false>	Enables (true) or disables (false) daylight savings time.

config bootconfig flags followed by:	
`debugmode <true|false>`	Enables (true) or disables (false) runtime debug mode.
`debug-config <true|false|file>`	Enables (true) or disables (false) runtime debug of the configuration file.
`egress-mirror <true|false>`	Enables (true) or disables (false) egress mirror capability.
`factorydefaults <true|false>`	Sets (true) runtime switch configuration back to factory settings.
`ftpd <true|false>`	Enables (true) or disables (false) FTP server.
`ha-cpu <true|false>`	Enables (true) or disables (false) high availability for a CPU.
`hsecure <true|false>`	Enables (true) or disables (false) high secure mode.
`logging <true|false>`	Enables (true) or disables (false) system logging to pc card file.
`reboot <true|false>`	Enables (true) or disables (false) reboot on fatal error.
`rlogind <true|false>`	Enables (true) or disables (false) rlogin/rsh server.
`savetostandby <true|false>`	Enables (true) or disables (false) saving to config/ bootconfig automatically to standby CPU.
`block-snmp <true|false>`	Blocks (true) SNMP access.
`sshd <true|false>`	Enables (true) or disables (false) the SSH services on the switch.
`telnetd <true|false>`	Enables (true) or disables (false) the telnet server.
`tftpd <true|false>`	Enables (true) or disables (false) TFTP server.
`trace-logging <true|false>`	Enables (true) or disables (false) system tracing to a pc card file.
`verify-config <true|false>`	Enables (true) or disables (false) syntax check of a configuration file.
`wdt <true|false>`	Enables (true) or disables (false) a hardware watchdog timer.

Configuration example: flags

The following configuration example uses the commands described above to:

- Set 8100-mode to false
- Set alt-led-enable to false
- Set autoboot to false
- Set block-warmstandby-switchover to false
- Set control-record-optimization to false
- Set daylight-saving-time to false
- Set debugmode to false
- Set debug-config to false
- Set egress-mirror to true
- Set factorydefaults to false
- Set ftpd to true
- Set ha-cpu to false
- Set hsecure to false
- Set logging to true
- Set reboot to true
- Set rlogind to false
- Set savetostandby to false
- Set block-snmp to false
- Set sshd to false
- Set telnetd to true
- Set tftpd to true
- Set trace-logging to false
- Set verify-config to false

Figure 57 shows sample output using these commands.

Figure 57 config bootconfig flags sample output

```
Passport-8603:3# config bootconfig flags 8100-mode false
Passport-8603:3# config bootconfig flags alt-led-enable false
Passport-8603:3# config bootconfig flags autoboot false
Passport-8603:3# config bootconfig flags block-warmstandby-switchover false
Passport-8603:3# config bootconfig flags control-record-optimization false
Passport-8603:3# config bootconfig flags daylight-saving-time false
Passport-8603:3# config bootconfig flags debugmode false
Passport-8603:3# config bootconfig flags debug-config false
Passport-8603:3# config bootconfig flags egress-mirror true
Passport-8603:3# config bootconfig flags factorydefaults false
Passport-8603:3# config bootconfig flags ftpd true
Passport-8603:3# config bootconfig flags ha-cpu false
Passport-8603:3# config bootconfig flags hsecure false
Passport-8603:3# config bootconfig flags logging true
Passport-8603:3# config bootconfig flags reboot true
Passport-8603:3# config bootconfig flags rlogind false
Passport-8603:3# config bootconfig flags savetostandby false
Passport-8603:3# config bootconfig flags block-snmp false
Passport-8603:3# config bootconfig flags sshd false
Passport-8603:3# config bootconfig flags telnetd true
Passport-8603:3# config bootconfig flags tftpd true
Passport-8603:3# config bootconfig flags trace-logging false
Passport-8603:3# config bootconfig flags verify-config false
Passport-8603:3# config bootconfig flags wdt true
Passport-8603:3# config bootconfig info
flags 8100-mode false
flags alt-led-enable false
flags autoboot false
flags block-warmstandby-switchover false
flags control-record-optimization false
flags daylight-saving-time false
flags debugmode false
flags debug-config false
flags egress-mirror true
flags factorydefaults false
flags ftpd true
flags ha-cpu false
flags hsecure false
flags logging true
flags reboot true
flags rlogind false
flags savetostandby false
flags block-snmp false
flags sshd false
flags telnetd true
flags tftpd true
flags trace-logging false
flags verify-config false
flags wdt true
Passport-8603:3#
```

Setting SSH configuration parameters

To set SSH configuration parameters on a Passport 8000 Series switch, use the following command:

```
config sys set ssh
```

The general **`config sys set ssh`** command includes the following options.

`config sys set ssh` followed by:	
`info`	Displays the current configuration parameters of SSH services.
`action <action choice> [<integer>]`	Sets the SSH key action. • *`<action choice>`* choose one of the following actions: - rsa-keygen - rsa-keydel - dsa-keygen - dsa-keydel • *`[<integer>]`* the SSH host key size. Can be a value from 512 to 1024. Default is 1024.
`dsa-auth <true|false>`	Enables or disables the DSA authentication. • <true|false> true enables the authentication and false disables the authentication. Default is true.
`enable <true|false|secure>`	Sets SSH. • *`true`* enables SSH. • *`false`* disables SSH. • *`secure`* securely enables SSH by turning off other daemon flags.
`max-sessions <integer>`	The maximum number of SSH sessions allowed. • <integer> a value from 0 to 8. Default is 4.
`pass-auth <true|false>`	Enables or disables password authentication. • `<true|false>` set to true to enable authentication and false to disable authentication. Default is true.
`port <integer>`	Sets the SSH connection port. • *`<integer>`* port number. Default is 22.

config sys set ssh followed by:	
rsa-auth <*true*|*false*>	Enables or disables RSA authentication. • <true|false> set to true to enable authentication and false to disable authentication. Default is true.
timeout <*integer*>	The SSH connection authentication timeout in seconds. • <*integer*> number of seconds. Default is 60 seconds.
version <*both*|*v2only*>	Sets the SSH version. • <both|v2only> both|v2only. Default is v2only. **Note:** Nortel Networks recommends setting the version to v2only.

Configuration example: SSH

The following configuration example uses the commands described above to:

- Set action rsa-keygen to 1021.
- Set action dsa-keygen to 1022.
- Enable DSA authentication.
- Set the maximum of SSH sessions to 5.
- Enable password authentication.
- Set the connection port to 21.
- Enable RSA authentication.
- Set connection authentication timeout to 50 seconds.
- Set the version to v2only.
- Enable the SSH daemon.
- View the information for SSH.

Figure 58 shows sample output using these commands.

Figure 58 config sys set ssh commands sample output

```
TOKYO>:5# config sys set ssh action rsa-keygen 1021
TOKYO>:5# config sys set ssh action dsa-keygen 1022
TOKYO>:5# config sys set ssh dsa-auth true
TOKYO>:5# config sys set ssh max-sessions 5
TOKYO>:5# config sys set ssh pass-auth true
TOKYO>:5# config sys set ssh port 21
TOKYO>:5# config sys set ssh rsa-auth true
TOKYO>:5# config sys set ssh timeout 50
TOKYO>:5# config sys set ssh version v2only
TOKYO>:5# config sys set ssh enable true
TOKYO>:5# config sys set ssh info

Total Active Sessions  : 0
        version            : v2only
        port               : 21
        max-sessions       : 5
        timeout            : 50
        action rsa-keygen  : rsa-keysize 1021
        action dsa-keygen  : dsa-keysize 1022
        rsa-auth           : true
        dsa-auth           : true
        pass-auth          : true
        enable             : true

TOKYO>:5#
```

Verifying and displaying SSH configuration information

To verify that SSH services are enabled on the Passport 8000 Series switch and to display SSH configuration information, use the following command:

```
show sys ssh
```

The general **show sys ssh** commands include the following options.

show sys ssh followed by:	
global	Displays global system SSH information.
session	Displays current session SSH information.

Figure 59 shows sample output for the **show ssh global** and **show ssh session** commands.

Figure 59 show sys ssh global and show sys ssh session commands

```
TOKYO>:5# show sys ssh global

Total Active Sessions  : 1
        version             : v2only
        port                : 21
        max-sessions        : 5
        timeout             : 50
        action rsa-keygen   : rsa-keysize 1021
        action dsa-keygen   : dsa-keysize 1022
        rsa-auth            : true
        dsa-auth            : true
        pass-auth           : true
        enable              : true

Passport-8306:5(config)# show sys ssh session

        SSH Session Id : 0
        User Name      : rwa
        Host           : 10.10.40.233

TOKYO>:5#
```

Chapter 9
Configuring SSH using Device Manager

This chapter includes the following topics:

Changing Secure Shell (SSH) configuration parameters

You can use Device Manager (DM) to change the SSH configuration parameters. However, Nortel Networks recommends using the CLI.

Note: If the SSH service is enabled, all fields will be grayed out until the SSH service is disabled. The SSH service must be disabled before setting the SSH service parameters.

Before you can make modifications to the SSH service parameters using DM the following conditions must apply:

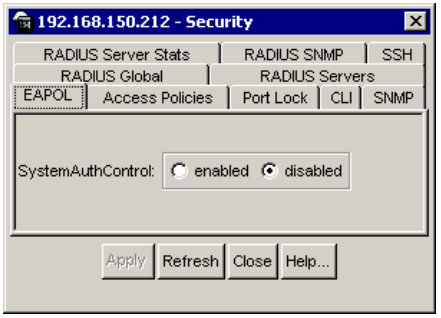
- The user Access Level is set to read/write/all community strings.
- The SNMP protocol is enabled.

To change SSH parameters:

1 From the Device Manager menu bar, choose Edit > Security.

The Security dialog box opens with the EAPOL tab displayed. (Figure 60)

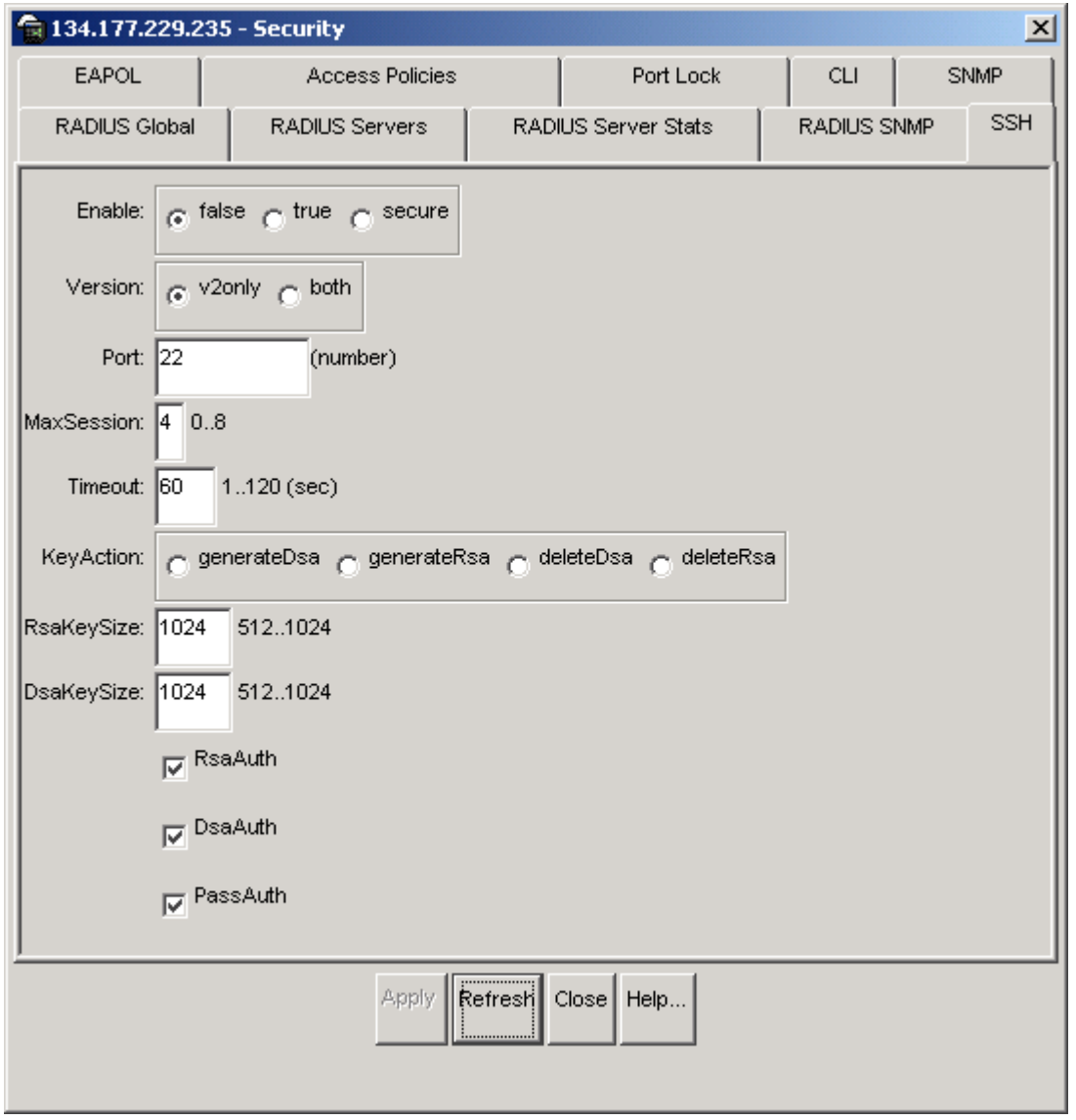
Figure 60 Security dialog box—EAPOL tab



2 Click SSH.

The SSH tab is displayed. (Figure 61)

Figure 61 Security dialog box—SSH tab



3 Enter information.

4 Click Apply.

Table 23 describes the SSH tab fields.

Table 23 Security dialog box—SSH tab fields

Field	Description
Enable	Enable or disable SSH. Set to **false** to disable SSH services. Set to **true** to enable SSH services. Set to **secure** to enable SSH and disable insecure services SNMP, TFTP, and Telnet. The **secure** mode will take effect after reboot. Default is false.
Version	Set the SSH version. Set to **both** or **v2only**. Default is v2only.
Port	Sets the SSH connection port number. Default is 22.
MaxSession	Sets the maximum number of SSH sessions allowed. The value can be from 0 to 8. Default is 4.
Timeout	Set the SSH authentication connection timeout in seconds. Default is 60 seconds.
KeyAction	Set the SSH key action.
RsaKeySize	RSA key size. Value can be from 512 to 1024. Default is 1024.
DsaKeySize	DSA key size. Value can be from 512 to 1024. Default is 1024.
RsaAuth	Enable or disable RSA authentication. Default is enabled.
DsaAuth	Enable or disable DSA authentication. Default is enabled.
PassAuth	Enable or disable password authentication. Default is enabled.

Supported SSH and SCP clients

Table 24 describes the third party SSH and SCP client software that have been tested but are not included with this release.

Table 24 Third party SSH and SCP client software

SSH Client	Secure Shell (SSH)	Secure Copy (SCP)
Tera Term Pro with TTSSH extension Windows 2000	• Supports SSH-1 client only. • Authentication: - RSA - Password • Does not include a keygen tool. • A separate key generation tool such as PuTTYgen must be used to generate an RSA key in SSHv1 format. • **Note:** The 8600 does not generate a log message when a RSA key is manually generated.	• Client distribution does not include SCP client. • Tested on the 8600 with the following applications: - Pageant (authentication agent holding private keys in memory) - PSCP (secure copy client)

Table 24 Third party SSH and SCP client software (continued)

SSH Client	Secure Shell (SSH)	Secure Copy (SCP)
Secure Shell Client Window 2000	• Supports SSH-2 client. • Authentication: - DSA - Password • Provides a keygen tool. • It creates a DSA key in SSHv2 format. • **Note:** The 8600 generates a log message stating that a DSA key has been generated.	• Client distribution includes a SCP client which is not compatible with the 8600.
OpenSSH Unix Solaris 2.5 / 2.6	• Supports SSH-1 and SSH-2 clients. • Authentication: - RSA - DSA - Password • Provides a keygen tool. • It creates both RSA and DSA keys in SSH v1 format.	• Client distribution includes a SCP client which is supported on the 8600.

After you have installed one of the SSH clients described in Table 24, you must generate a client and server key using the RSA or DSA algorithms.

Note: Authentication keys are not saved to a backup SSF if one is present. You can use TFTP or FTP to copy the keys to a backup SSF.

The Passport 8600 generates a DSA public and private server key pair. The public part of the key for DSA is stored `in/flash/.ssh/dsa_pub.key`. If a DSA key pair does not exist, the Passport 8600 will automatically generate one, once the SSH server is enabled. To authenticate a client using DSA, the administrator has to copy the public part of the client DSA key to the Passport 8600.

Table 25 describes access levels and file names used for storing the SSH client authentication information using DSA.

Table 25 DSA authentication access level and file name

Client key format or WSM	Access Level	File name
Client key in IETF format (SSHv2)	RWA	*/flash/.ssh/dsa_key_rwa_ietf*
	RW	*/flash/.ssh/dsa_key_rw_ietf*
	RO	*/flash/.ssh/dsa_key_ro_ietf*
	L3	*/flash/.ssh/dsa_key_rwl3_ietf*
	L2	*/flash/.ssh/dsa_key_rwl2_ietf*
	L1	*/flash/.ssh/dsa_key_rwl1_ietf*
Client key in non IETF format	RWA	*/flash/.ssh/dsa_key_rwa*
	RW	*/flash/.ssh/dsa_key_rw*
	RO	*/flash/.ssh/dsa_key_ro*
	L3	*/flash/.ssh/dsa_key_rwl3*
	L2	*/flash/.ssh/dsa_key_rwl2*
	L1	*/flash/.ssh/dsa_key_rwl1*
WSM	14admin	*/flash/.ssh/dsa_key_14admin*
	slbadmin	*/flash/.ssh/dsa_key_slbadmin*
	oper	*/flash/.ssh/dsa_key_oper*
	14oper	*/flash/.ssh/dsa_key_14_oper*
	slboper	*/flash/.ssh/dsa_key_slboper*
	ssladmin	*/flash/.ssh/dsa_key_ssladmin*

The Passport 8600 generates an RSA public and private server key pair. The public part of the key for RSA is stored in `/flash/.ssh/ssh_key_rsa_pub.key`. If an RSA key pair does not exist, the Passport 8600 will automatically generate one, once the SSH server is enabled. To authenticate a client using RSA, the administrator has to copy the public part of the client RSA key to the Passport 8600.

Table 26 describes the access level and file name used for storing the SSH client authentication information using RSA.

Table 26 RSA authentication access level and file name

Client key format or WSM	Access level	File name
Client key in IETF format	RWA	*/flash/.ssh/rsa_key_rwa*
	RW	*/flash/.ssh/rsa_key_rw*
	RO	*/flash/.ssh/rsa_key_ro*
	L3	*/flash/.ssh/rsa_key_rwl3*
	L2	*/flash/.ssh/rsa_key_rwl2*
	L1	*/flash/.ssh/rsa_key_rwl1*
WSM	14admin	*/flash/.ssh/rsa_key_14admin*
	slbadmin	*/flash/.ssh/rsa_key_slbadmin*
	oper	*/flash/.ssh/rsa_key_oper*
	14oper	*/flash/.ssh/rsa_key_14_oper*
	slboper	*/flash/.ssh/rsa_key_slboper*
	ssladmin	*/flash/.ssh/rsa_key_ssladmin*

Chapter 10
Setting up RADIUS servers

Before you enable RADIUS accounting on the switch, you must create at least one RADIUS server. Nortel Networks recommends that you configure at least two RADIUS servers in the network to provide redundancy. You can configure a maximum of 10 RADIUS servers in a single network.

The Passport 8600 software supports BaySecure Access Control (BSAC*), Merit Network, and freeRadius servers. For instructions on installing the BSAC, Merit Network, or freeRadius server software on the server that you will use, see the installation manual that came with your software.

After the software is installed, you must make changes to one or more files for these servers. For information about the changes that must be made for the BSAC server, see “Updating files for the BSAC RADIUS server.” For information about the changes that must be made for the Merit Network server, see “Updating the dictionary file for a Merit Network server.” For information about changes that must be made for the freeRadius server, see “Updating files for the freeRadius server.”

For detailed instructions on configuring a RADIUS server, including adding clients and adding users and access priorities, refer to the documentation that came with the server software.

This chapter describes how to update four files for the BSAC RADIUS server, one file for the Merit Network server, and three files for the freeRadius server. It also describes the vendor-specific attribute format for CLI commands if you're using a third-party RADIUS server and need to modify the dictionary files. Specifically, this chapter includes the following topics:

Updating files for the BSAC RADIUS server

After you have installed the BSAC server software on either a UNIX or Windows NT server, you must update four files for BSAC to successfully authenticate a user:

- The main dictionary (radius.dct). This file must be edited to contain an entry of parameters from the newly created Passport dictionary.
- A private dictionary (pprt8600.dct). This file, which is specific to the Passport 8600 switch, must be generated. It will be sourced and used by dictiona.dcm and vendor.ini.
- The vendor.ini file. This file must contain an entry for the Passport 8600 in order for the file to acknowledge the model/type during the client configuration.
- The account.ini file. This file must contain the CLI-Command= entry.

Specifically, you must make the following configuration changes for the BSAC server:

1 Add the following lines in files radius.dct and pprt8600.dct:

```
ATTRIBUTE   Access-Priority     26    [vid=1584
type1=192 len1=+2 data=integer]R
VALUE       Access-Priority     None-Access             0
VALUE       Access-Priority     Read-Only-Access        1
VALUE       Access-Priority     L1-Read-Write-Access    2
VALUE       Access-Priority     L2-Read-Write-Access    3
VALUE       Access-Priority     L3-Read-Write-Access    4
VALUE       Access-Priority     Read-Write-Access       5
VALUE       Access-Priority     Read-Write-All-Access   6

ATTRIBUTE Cli-Command 26 [vid=1584 type1=193 len1=+2
data=string]
```

Note: The value in the type1 field must match the vendor-specific authentication attribute value.

2 Add the following lines in vendor.ini:

```
vendor-product = Nortel Passport 8600
dictionary = pprt8600
ignore-ports = no
port-number-usage = per-port-type
help-id = 0
```

3 Add the following entry to the account.ini file:

```
Cli-Command=
```

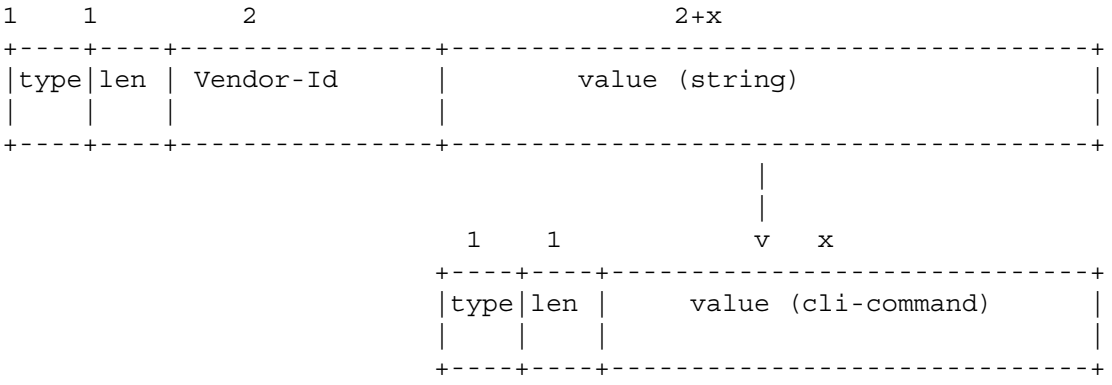
4 In the account.ini file, make sure that the following lines are present:

```
User-Name=
Acct-Input-Octets=
Acct-Output-Octets=
Acct-Session-Id=
Acct-Session-Time=
Acct-Input-Packets=
Acct-Output-Packets=
```

5 Restart the server to activate the changes.

Using a third-party RADIUS server

If you're using a third-party RADIUS server and need to modify the dictionary files, you must use the following vendor-specific attribute format for CLI commands:



Updating the dictionary file for a Merit Network server

You must add the following lines in the dictionary file for the Merit Network server:

```
VENDOR          Nortel  1584

ATTRIBUTE       Access-Priority 192 integer  Nortel

VALUE   Access-Priority         None-Access             0
VALUE   Access-Priority         Read-Only-Access        1
VALUE   Access-Priority         L1-Read-Write-Access    2
VALUE   Access-Priority         L2-Read-Write-Access    3
VALUE   Access-Priority         L3-Read-Write-Access    4
VALUE   Access-Priority         Read-Write-Access       5
VALUE   Access-Priority         Read-Write-All-Access   6

ATTRIBUTE       Cli-Command     192 string  Nortel
```

You must restart the server to activate the changes.

Updating files for the freeRadius server

After you have installed the freeRadius server software on either a UNIX or Windows NT server, you must update three files for freeRadius to successfully authenticate a user:

- A private dictionary (dictionary.nortel).
- clients.conf
- users

Specifically, you must make the following configuration changes for the freeRadius server:

1 Add the following lines in the dictionary file:

```
VENDOR          Nortel  1584

BEGIN-VENDOR Nortel

ATTRIBUTE       Access-Priority 192 integer

VALUE   Access-Priority         None-Access             0
VALUE   Access-Priority         Read-Only-Access        1
VALUE   Access-Priority         L1-Read-Write-Access    2
VALUE   Access-Priority         L2-Read-Write-Access    3
VALUE   Access-Priority         L3-Read-Write-Access    4
VALUE   Access-Priority         Read-Write-Access       5
VALUE   Access-Priority         Read-Write-All-Access   6

#CLI profile
ATTRIBUTE       Command-Access 194 integer

#CLI Commands
ATTRIBUTE       Cli-Commands 193 string

#CLI Commands
ATTRIBUTE       Commands 195 string

VALUE Command-Access FALSE 0
VALUE Command-Access True 1

#802 priority (value: 0-7)
ATTRIBUTE Dot1x-Port-Priority 1 integer
```

2 Add the following lines in clients.conf. You must enter these lines for the freeRadius server to work. The secret is not encrypted, so be careful when giving permissions to the directories.

```
client 130.128.254.5/32 {
secret = test
shortname = R5
nastype = other
}
```

3 Add the following lines in users.

```
# EAPoL users, using Microsoft Windows Domain convention
DOMAIN2\\user_n       Auth-Type := EAP, User-Password == "password"
        Reply-Message = "You're authenticated, %u !!",

DOMAIN2\\eap_user     Auth-Type := EAP, User-Password == "eap_password"
        Reply-Message = "You're authenticated, %u !!",

# Console/Telnet access via regular RADIUS
# the following will prohibit user "administrator" from issuing commands
"config ip" tree
administrator   Auth-Type := Local, User-Password == "dimension"
                Access-Priority = "Read-Write-All-Access",
                Command-Access = "FALSE",
                Commands = "config ip"
```

You must restart the server to activate the changes.

Changing user access

As a network administrator, you can override a user's access to specific CLI commands by configuring the RADIUS server for user authentication. You must still give access based on the existing six access levels in the Passport 8600, but you can customize user access by permitting and preventing access to specific CLI commands.

Note: For the NNCLI, the ability to customize access to specific commands using the CLI-Command attribute is not currently supported. Also, the ability to log commands and statistics in accounting packets is not currently supported.

Subscriber and/or administrative interaction

You must configure the following three returnable attributes for each user:

- Access priority (single instance) - the access levels currently available on Passport 8600: ro, l1, l2, l3, rw, rwa.
- Command access (single instance) - indicates whether the NNCLI or CLI commands configured on the RADIUS server are allowed or disallowed for the user.
- NNCLI or CLI commands (multiple instances) - the list of commands that the user can/cannot use. The user cannot include allow and deny commands in the list of multiple commands; the commands must be either all allow or all deny.

Configuring the BSAC or Merit Network server

To change the configuration of a BSAC or Merit Network server:

1 Create a new file (for example, pprtl2l3.dct) and update the following information:

```
##############################################################################
# passaprt.dct - RADLINX PASSaPORT dictionary
#
# (See README.DCT for more details on the format of this file)
##############################################################################
#
# Use the Radius specification attributes in lieu of the RADLINX PASSaPORT  ones
#
@radius.dct
#
# Define additional RADLINX PASSaPORT  parameters
# (add RADLINX PASSaPORT  specific attributes below)

ATTRIBUTE   Radlinx-Vendor-Specific  26  [vid=648 data=string]  R

##############################################################################
# pprtl2l3.dct - RADLINX PASSaPORT dictionary
##############################################################################
#Define Nortel Passport 1000 & 8000 Layer 2 & Layer 3 dictionary
#@radius.dct
@pprtL2L3.dct
ATTRIBUTE       Access-Priority         26 [vid=1584 type1=192 len1=+2 data=integer] r
    VALUE       Access-Priority         None-Access             0
    VALUE       Access-Priority         Read-Only-Access        1
    VALUE       Access-Priority         L1-Read-Write-Access    2
    VALUE       Access-Priority         L2-Read-Write-Access    3
    VALUE       Access-Priority         L3-Read-Write-Access    4
    VALUE       Access-Priority         Read-Write-Access       5
    VALUE       Access-Priority         Read-Write-All-Access   6
    VALUE       Access-Priority         CommReadOnly            1
    VALUE       Access-Priority         CommReadWriteLayer1     2
    VALUE       Access-Priority         CommReadWriteLayer2     4
    VALUE       Access-Priority         CommReadWriteLayer3     8
    VALUE       Access-Priority         CommReadWrite           16
    VALUE       Access-Priority         CommReadWriteAll        32

ATTRIBUTE       Acct-Status-Type        26 [vid=1584 type1=193 len1=+2 data=integer] r
    VALUE       Acct-Status-Type        Start                   1
    VALUE       Acct-Status-Type        Stop                    2
    VALUE       Acct-Status-Type        Interim-Update          3
    VALUE       Acct-Status-Type        Accounting-On           7
    VALUE       Acct-Status-Type        Accounting-Off          8

ATTRIBUTE       Command-Access          26 [vid=1584 type1=194 len1=+2 data=integer] r
    VALUE       Command-Access          TRUE                    1
    VALUE       Command-Access          FALSE                   0

ATTRIBUTE       Cli-Commands            26 [vid=1584 type1=195 len1=+2 data=string]R
##############################################################################
```

192,194,195 are the default values. If you change these values on the Passport 8600 switch, you must change them in the file.

Assign one of the following access levels to a user:

```
VENDOR          Nortel  1584

ATTRIBUTE       Access-Priority 192 integer  Nortel

VALUE   Access-Priority         None-Access             0
VALUE   Access-Priority         Read-Only-Access        1
VALUE   Access-Priority         L1-Read-Write-Access    2
VALUE   Access-Priority         L2-Read-Write-Access    3
VALUE   Access-Priority         L3-Read-Write-Access    4
VALUE   Access-Priority         Read-Write-Access       5
VALUE   Access-Priority         Read-Write-All-Access   6

ATTRIBUTE       Cli-Command     192 string  Nortel
```

The following are the values that are valid for the Command-Access Attribute:

```
VALUE Command-Access TRUE 1
VALUE Command-Access FALSE 0
```

2 In the file dictiona.dcm, reference the new file pprtl2l2.dct:

```
@pprtl2l3.dct
```

3 Update the file vendor.ini as follows:

```
vendor-product = Nortel Passport 8600
Switches
dictionary = pprtl2l3
ignore-ports = no
help-id = 0
```

Configuring the freeRadius server

To change the configuration of a freeRADIUS server:

1. Create a new file dictionary.passport and include it in the dictionary file.
2. Add the following to the dictionary.passport file:

```
VENDOR Passport 1584
ATTRIBUTE Access-Priority-Attribute 192 integer Passport
ATTRIBUTE Cli-Commands-Attribute 195 string Passport
ATTRIBUTE Command-Access 194 integer Passport
```

192,193 are the default values. If you change these values on the Passport 8600 switch, you must change them in the file.

Assign one of the following access levels to a user:

```
VENDOR          Nortel  1584

ATTRIBUTE       Access-Priority 192 integer  Nortel

VALUE   Access-Priority        None-Access            0
VALUE   Access-Priority        Read-Only-Access       1
VALUE   Access-Priority        L1-Read-Write-Access   2
VALUE   Access-Priority        L2-Read-Write-Access   3
VALUE   Access-Priority        L3-Read-Write-Access   4
VALUE   Access-Priority        Read-Write-Access      5
VALUE   Access-Priority        Read-Write-All-Access  6

ATTRIBUTE       Cli-Command     192 string  Nortel
```

The following values are valid for the Command-Access Attribute.

```
VALUE Command-Access FALSE 0
VALUE Command-Access TRUE 1
```

3. Modify the file clients.conf to provide access to the Passport 8600 switch and to provide the secret value:

   x.x.x.x mysecret

where *x.x.x.x* is the Passport 8600 IP address.
mysecret is the secret configured while creating a RADIUS server.

Note: The secret value configured on the RADIUS server must be the same as the one configured in the Passport 8600 switch.

4 The file users must have the following access:

```
rwa Auth-Type:= Local, Password == rwa
Access-Priority = RWA-Access,
```

The user and password must be rwa and Access-Priority must be in the dictionary.passport file.

Example 1

```
User- john
Access-Priority – L2-Access
Command-Access - True
Cli-Commands - Config ip forwarding
```

Though John has only L2 access, he can use the command **config ip forwarding**, which normally requires L3 access.

Example 2

```
User- Mike
Access-Priority - RWA-Access
Command-Access – False
Cli-Commands – reset
```

Although Mike has rwa access, he is prevented from using the **reset** command to reboot the switch.

5 If a user enters the `help` command, the system displays help for only those commands to which the user has access.

Note: If you prevent access to any command, only the lowest option in the command tree cannot be accessed. For example, if you prevent access to the CLI command **`config sys set`** for a user, the user is able to display or execute **`config`** or **`config sys`**; however, the user cannot display or execute **`set`**.

Chapter 11
Configuring RADIUS authentication and accounting using the CLI

This chapter includes the following topics:

Roadmap of CLI RADIUS commands

The following roadmap lists the CLI RADIUS commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
config radius	info
	acct-attribute-value <value>
	acct-enable <true|false>
	acct-include-cli-commands <true|false>
	access-priority-attribute <value>
	clear-stat
	cli-commands-attribute <value>
	cli-profile-enable <true|false>
	command-access-attribute <value>
	enable <true|false>
	igap-passwd-attr <standard|auth-info>
	igap-timeout-log-fsize <value>
	maxserver <value>
	mcast-addr-attr-value <value>
	sourceip-flag <true|false>
config radius enable <true|false>	
config radius acct-enable <true|false>	
config radius access-priority-attribute <value>	
config radius acct-attribute-value <value>	
config radius info show radius info	
config radius info show radius info	
config radius server	info

Command	Parameter
	create <ipaddr> secret <value>
	[usedby <value>] [port <value>] [priority <value>] [retry <value>] [timeout <value>] [enable <value>] [acct-port <value>] [acct-enable <value>] [source-ip <value>]
	delete <ipaddr> usedby <value>
	set <ipaddr> usedby <value>
	[secret <value>] [port <value>] [priority <value>] [retry <value>] [timeout <value>] [enable <value>] [acct-port <value>] [acct-enable <value>] [source-ip <value>]
show radius server config	
show radius server stat	
config sys set udpsrc-by-vip <enable|disable>	

Configuring RADIUS on the switch

To configure RADIUS on the switch, use the following command:

```
config radius
```

This is a complete listing of all of the **`config radius`** commands. The next sections will provides specific details about each command.

`config radius` followed by:	
`info`	Displays global RADIUS settings.
`acct-attribute-value <value>`	Specific to RADIUS accounting. Sets the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server. This value *must* be different from the access-priority attribute value configured for authentication. The default value is 193. *value* is between 192 and 240.
`acct-enable <true|false>`	Enables (true) or disables (false) RADIUS accounting globally. RADIUS accounting cannot be enabled unless a valid server is configured. This feature is disabled by default.
`acct-include-cli-commands <true|false>`	Specifies whether you want CLI commands to be included in RADIUS accounting requests. If you set this parameter to true, the commands are included in the requests. If you set this parameter to false, the commands are not included and interim updates are not sent.
`access-priority-attribute <value>`	Specific to RADIUS accounting. Sets the vendor-specific attribute value of the Access Priority attribute to match the type value set in the dictionary file on the RADIUS server. *value* is between 192 and 240.
`auth-info-attr-value <value>`	Sets the integer value for the auth-info attribute. *value* is between 0 and 255.
`clear-stat`	Clears RADIUS statistics from the server.
`cli-commands-attribute <value>`	Sets the CLI command-attribute value. *value* is between 192 and 240.
`cli-profile-enable <true|false>`	Enables (true) or disables (false) RADIUS profiling.
`command-access-attribute <value>`	Sets the integer value of the command-access attribute. *value* is between 192 and 240.
`enable <true|false>`	Enables (true) or disables (false) the RADIUS authentication feature.

config radius followed by:	
igap-passwd-attr <standard|auth-info>	Sets the IGAP password attribute type. The valid values are standard and auth-info. For IGAP RADIUS Auth-Requests, use either the standard password attribute or Auth-Info attribute.
igap-timeout-log-fsize <*value*>	Sets the maximum size of the IGAP log file in KB. *value* is between 50 and 8192.
maxserver <*value*>	Specific to RADIUS authentication. Sets the maximum number of servers allowed for the switch. *value* is between 1 and 10.
mcast-addr-attr-value <*value*>	Sets the integer value of the multicast address attribute. *value* is between 0 and 255.
sourceip-flag <true|false>	Enables (true) or disables (false) the RADIUS packet source IP flag.

Enabling RADIUS authentication

To enable or disable RADIUS authentication globally on the switch, use the following command:

```
config radius enable <true|false>
```

where:
`true` enables RADIUS authentication globally.
`false` disables RADIUS authentication globally.

Enabling RADIUS accounting

Note: You must set up a RADIUS server and add it to the switch's configuration file before you can enable RADIUS accounting on the switch. Otherwise, the system displays an error message.

To enable or disable RADIUS accounting globally, use the following command:

```
config radius acct-enable <true|false>
```

where:
`true` enables RADIUS accounting globally.
`false` disables RADIUS accounting globally.

RADIUS accounting is disabled by default.

Configuring RADIUS authentication and RADIUS accounting attribute values

To configure the RADIUS authentication attribute value, use the following command:

```
config radius access-priority-attribute <value>
```

where:
value is a range from 192 to 240. The default value is 192.

To configure the RADIUS accounting attribute value, use the following command:

```
config radius acct-attribute-value <value>
```

where:
value is a range from 192 to 240. The default value is 193.

Configuration example: RADIUS accounting and authentication

The following configuration example uses the commands described above to:

- Enable RADIUS accounting.
- View RADIUS information.

Figure 62 shows sample output using these commands.

Figure 62 config radius command sample output

```
TOKYO>:5# config radius enable true
TOKYO>:5# config radius info

Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:

             acct-attribute-value : 193
                      acct-enable : false
        acct-include-cli-commands : false
        access-priority-attribute : 192
             auth-info-attr-value : 91
         command-access-attribute : 194
           cli-commands-attribute : 195
               cli-profile-enable : false
                           enable : true
                 igap-passwd-attr : standard
           igap-timeout-log-fsize : 512
                        maxserver : 10
            mcast-addr-attr-value : 90
                    sourceip-flag : false
TOKYO>:5#
```

Showing RADIUS information

To display the global status of RADIUS information, use one of the following commands:

```
config radius info
show radius info
```

Figure 63 shows sample output for the **`config radius info`** command. The output for the **`show radius info`** command is the same as that for **`config radius info`** command.

Figure 63 config radius info sample output

```
TOKYO>:5# config radius info

Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:

             acct-attribute-value : 193
                      acct-enable : false
        acct-include-cli-commands : false
        access-priority-attribute : 192
             auth-info-attr-value : 91
         command-access-attribute : 194
           cli-commands-attribute : 195
               cli-profile-enable : false
                           enable : true
                 igap-passwd-attr : standard
           igap-timeout-log-fsize : 512
                       maxserver : 10
            mcast-addr-attr-value : 90
                    sourceip-flag : false
TOKYO>:5#
```

Configuring a RADIUS server

To create, delete, or get information about a RADIUS server, use the following command:

```
config radius server
```

This command includes the following options:

config radius server followed by:	
`info`	Displays a list of all configured RADIUS servers.

`create <ipaddr> secret <value>`
 	
Optional parameters:
`[usedby <value>] [port <value>] [priority <value>] [retry <value>] [timeout <value>] [enable <value>] [acct-port <value>] [acct-enable <value>] [source-ip <value>]`
	Creates a server.
	• *ipaddr* is the IP address of the server you want to add.
	• `secret <value>` is the secret key of the authentication client**.**
	(optional)
	• `usedby` is used with CLI, SNMP, IGAP or EAPOL.
	• `port <value>` is the UDP ports you want to use (1..65536). The default is 1812.
	• `priority <value>` is the priority value for this server (1..10). The default is 10.
	• `retry <value>` is the number of authentication retries the server will accept (1..6). The default is 3.
	• `timeout <value>` is the number of seconds before the authentication request times out (1..10). The default is 3.
	• `enable <value>` enables (true) or disables (false) this server. The default value is true.
	• `acct-port <value>` is the UDP port of the RADIUS accounting server (1..65536). The default value is 1813.
	Note: The UDP port value set for the client must match the UDP value set for the RADIUS server.
	• `acct-enable <value>` enables (true) or disables (false) RADIUS accounting on this server. The default value is true.
	• `source-ip <value>` is the source IP address.
	Note: The source-ip that can be configured in the radius server setting need to be a circuitless-ip interface. Only if the source-ip is a CLIP, then NAS-IP, is replaced with this source-ip and sent to the radius server.

config radius server followed by:	
`delete <ipaddr> usedby <value>`	Deletes a server. • `ipaddr` is the IP address of the server you want to delete. • `usedby` is used with CLI, SNMP, IGAP or EAPOL.

`set <ipaddr> usedby <value>`
 	
Optional parameters:
`[secret <value>] [port <value>] [priority <value>] [retry <value>] [timeout <value>] [enable <value>] [acct-port <value>] [acct-enable <value>] [source-ip <value>]`
	Changes specified server values without having to delete the server and re-create it again. Creates and configures a server:
	• *ipaddr* is the IP address of the server you want to add.
	• `usedby` is used with CLI, SNMP, IGAP or EAPOL.
	• (optional)
	• `secret <value>` is the secret key of the authentication client**.**
	• `port <value>` is the UDP ports you want to use (1..65536). The default is 1812.
	• `priority <value>` is the priority value for this server (1..10). The default is 10.
	• `retry <value>` is the number of authentication retries the server will accept (1..6). The default is 3.
	• `timeout <value>` is the number of seconds before the authentication request times out (1..10). The default is 3.
	• `enable <value>` enables (true) or disables (false) this server. The default value is true.
	• `acct-port <value>` is the UDP port of the RADIUS accounting server (1..65536). The default value is 1813.
	Note: The UDP port value set for the client must match the UDP value set for the RADIUS server.
	• `acct-enable <value>` enables (true) or disables (false) RADIUS accounting on this server. The default value is true.
	• `source-ip <value>` is the source IP address.

Configuration example: Adding a RADIUS server

The following configuration example uses the commands described above to:

- Add a RADIUS server with IP address 12.12.12.12, a key of 9, and usedby CLI.
- View RADIUS server information.

Figure 64 shows sample output using these commands.

Figure 64 config radius server command sample output

```
TOKYO>:5# config radius server create 12.12.12.12 secret 9 usedby cli
TOKYO>:5# config radius server info

Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:

                     create :

Name            Usedby Secret           Port    Prio  Retry Timeout Enabled
Acct-port Acct-enabled source-ip
12.12.12.12     cli    9             1812    10    1     3       true    1813
true          0.0.0.0

                     delete : N/A
                        set : N/A

TOKYO>:5#
```

Showing RADIUS server configurations and server statistics

The **`show radius server config`** command displays current RADIUS server configurations. The command uses the syntax:

```
show radius server config
```

Figure 65 shows sample output for the **`show radius server config`** command.

Figure 65 show radius server config sample command output

```
TOKYO>:5# show radius server config

Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:

                      create :

Name             Usedby Secret            Port     Prio  Retry Timeout Enabled
Acct-port Acct-enabled source-ip
12.12.12.12     cli    9              1812    10    1     3       true    1813
true          0.0.0.0

                      delete : N/A
                         set : N/A

TOKYO>:5#
```

The **`show radius server stat`** command displays statistics for the current RADIUS servers. The command uses the syntax:

```
show radius server stat
```

Note: You cannot collect the following network statistics from a console port: the number of input and output packets, and the number of input and output bytes. All other statistics from console ports are available to assist with debugging.

Figure 66 shows sample output for the **`show radius server stat`** command.

Figure 66 show radius server stat command sample output

```
TOKYO>:5# show radius server stat

Responses with invalid server address: 0

   Radius Server(UsedBy) : 12.12.12.12(cli)
-----------------------------------------------------------
         Access Requests : 0
          Access Accepts : 0
          Access Rejects : 0
           Bad Responses : 0
          Client Retries : 0
        Pending Requests : 0
        Acct On Requests : 0
       Acct Off Requests : 0
     Acct Start Requests : 0
      Acct Stop Requests : 0
   Acct Interim Requests : 0
      Acct Bad Responses : 0
   Acct Pending Requests : 0
     Acct Client Retries : 0
       Access Challanges : 0
          Round-trip Time : unknown
           Nas Ip Address : 0.0.0.0
 TOKYO>:5#
```

Table 27 describes the statistics from this command.

Table 27 show radius server stat command statistics

Item	Description
RADIUS Server	The IP address of the RADIUS server.
Access Requests	Number of access-response packets sent to the server; does not include retransmissions.
Access Accepts	Number of access-accept packets, valid or invalid, received from the server.
Access Rejects	Number of access-reject packets, valid or invalid, received from the server.
Bad Responses	Number of invalid access-response packets received from the server.

Table 27 show radius server stat command statistics (continued)

Item	Description
Client Retries	Number of authentication retransmissions to the server.
Pending Requests	Access-request packets sent to the server that have not yet received a response, or have timed out.
Acct On Requests	Number of accounting On requests sent to the server.
Acct Off Requests	Number of accounting Off requests sent to the server.
Acct Start Requests	Number of accounting Start requests sent to the server.
Acct Stop Requests	Number of accounting Stop requests sent to the server.
Acct Interim Requests	Number of accounting Interim Requests sent to the server. **Note:** The AcctInterimRequests counter will increment only if the parameter acct-include-cli-commands is set to true.
Acct Bad Responses	Number of Invalid Responses from the server that are discarded.
Acct Pending Requests	Number of requests waiting to be sent to the server.
Acct Client Retries	Number of retries made to this server.
Access Challenges	Number of Access-Challenge packets received from the RADIUS server.
Round-trip Time	The time difference between the instant when a RADIUS Request is sent to the server and the instant when the RADIUS Response is received from the server.
Nas Ip Address	The NAS IP address used in the RADIUS requests sent to this server.

Note: To clear server statistics, use the **`config radius clear-stat`** command.

Configuring RADIUS Accounting for SNMP

You can authenticate the users logging into the Passport 8000 Series switch through SNMP. The authentication request is forwarded to a RADIUS server only if the `enable` parameter under `config/radius/snmp#` is set to `true`.

You can enable accounting, which records the duration of the SNMP session and the number of packets/octets received during the session. Accounting is enabled by setting the `acct-enable` parameter under `config/radius/snmp#` is set to `true`.

Note: You must configure a RADIUS SNMP server before you can enable reauthentication and accounting. Be sure to enter snmp as the value for the usedby option.

Radius server configuration

The following changes are required to configure a RADIUS SNMP server.

1. Create a new file say “pprtl2l3.dct” and update the following info:

```
ATTRIBUTE Radlinx-Vendor-Specific 26[vid=648 data=string]R
ATTRIBUTE Acct-Status-Type 26 [vid=1584 type1=193 len1=+2 data=integer]r
ATTRIBUTE Access-Priority 26 [vid=1584 type1=192 len1=+2 data=integer]r
```

192,193 are the default values. If you change these values on the Passport 8000 Series switch, you must change them in this file.

You can give the following access levels to a user.

VALUE	Access-Priority	CommReadWriteAll	32
VALUE	Access-Priority	CommReadWrite	16
VALUE	Access-Priority	CommReadWriteLayer3	8
VALUE	Access-Priority	CommReadWriteLayer2	4
VALUE	Access-Priority	CommReadWriteLayer1	2
VALUE	Access-Priority	CommReadOnly	1

2. In the file `dictiona.ini` add the new file `pprtl2l3.dc` as shown below.

```
@pprtl2l3.dct
```

3. Update the file `vendor.ini` as shown below.

```
vendor-product = Nortel Passport 1000 and 8000 L2L3
Switches
dictionary = pprtl2l3
ignore-ports = no
help-id = 0
```

4 Add the following line in the file account.ini file.

```
Acct-Status-Type =
```

Configuring a freeRadius server

To configure a freeRadius server, do the following:

1 Create a new file, `dictionary.passport`, containing the following information:

```
VENDOR Passport 1584
ATTRIBUTE Access-Priority 192 integer Passport
ATTRIBUTE Acct-Status-Type 193 integer Passport
```

192,193 are the default values. If you change these values on the Passport 8000 Series switch, you must change them in this file.

You can give the following access levels to a user.

VALUE	Access-Priority	CommReadWriteAll	16
VALUE	Access-Priority	CommReadWrite	16
VALUE	Access-Priority	CommReadWriteLayer3	8
VALUE	Access-Priority	CommReadWriteLayer2	4
VALUE	Access-Priority	CommReadWriteLayer1	2
VALUE	Access-Priority	CommReadOnly	1

2 Modify the file clients to provide access to the Passport 8000 Series switch and also to provide the secret value.

```
x.x.x.x mysecret
```

where x.x.x.x is the 8600 IP address.

Note: The secret value configured on the radius server must be same as the one configured in Passport 8000 Series switch for that particular server using the command `config radius server create`.

3 Enter the following in the users file:

```
snmp_user Auth-Type := Local, Password == "public"

Access-Priority = CommReadWriteAll
```

Here user must be `snmp_user`, the password can be any string value, and the Access-Priority has to be among the above mentioned values in the `dictionary.passport` file.

Configuration example: RADIUS server

The following configuration example uses the commands described above to:

- Add a RADIUS server with IP address 11.11.11.11, a secret of tokyo, and is usedby SNMP.
- View RADIUS server information.

Figure 67 shows sample output using these commands.

Figure 67 config radius server command sample output

```
Passport-8603:3# config radius server create 11.11.11.11 secret tokyo usedby
snmp
Passport-8603:3# config radius server info

Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:

                     create :

Name           Usedby Secret          Port    Prio  Retry Timeout Enabled Acct
-port Acct-enabled source-ip
12.12.12.12     cli    tokyo           1812    10    1     3       true    1813
      true          0.0.0.0
11.11.11.11     snmp   tokyo           1812    10    1     3       true    1813
      true          0.0.0.0

                     delete : N/A
                        set : N/A

Passport-8603:3#
```

After you have created a RADIUS SNMP server, you have the following command options available to you.

config radius server snmp followed by:	
`info`	Displays information about the RADIUS server.
`abort-session-timer`	Specifies time before aborting the session.
`acct-enable <false/true>`	Enables server accounting (true) or disables accounting (false).
`enable <false/true>`	Enables the server (true) or disables the server (false).
`re-auth-timer <value>`	Specifies time before reauthorization of the server.
`user <string>`	Specifies the user name for SNMP access. The valid range is 0 to 20 characters.

RADIUS/SNMP header network address modifications

A new flag has been introduced, `udpsrc-by-vip`. When enabled, this flag directs the IP header to have the same source address as the management virtual IP address for self-generated UDP packets. The syntax of the command is:

`config sys set udpsrc-by-vip <enable|disable>`

If a management virtual IP address is configured and the `udpsrc-by-vip` flag is set, the network address in the SNMP header is always the management virtual IP address. This is true for all traps routed out on the I/O ports or on the out-of-band management ethernet port.

If the `udpsrc-by-vip` flag is disabled or the management virtual IP address is not configured, you can determine the source address using the following steps:

1. Verify that the trap receiver is a locally attached station on the management port.

   If this is true, the management port's IP address is used as the source address in the SNMP header.

2. If the trap receiver is not a locally attached station, check the list of configured management routes.

   If you locate a route, the management IP address is used as the source address in the SNMP header.

Caution: Nortel strongly recommends that you do not configure a less specific route on the management port than on an overlapping route on a local interface (VLAN or brouter port) the SNMP header of the packets generated by the Passport 8600 are set to the management IP address and the source IP address is the local interface's IP address. In this case, the addresses do not match.

3. If step 2 does not yield a route to the trap receiver, search the IP forwarding table for a route.
4. If you locate a route, use the outgoing interface's IP address as the source address in the SNMP header.

5 If the previous steps do not return a route to the receiver, verify that there is a default route specified for the debug port (only possible on the Passport 8100).

   It is assumed that the receiver can be reached from the gateway. The management IP address is used as the source address in the SNMP header.

If you do not find a route using the above steps, the trap receiver is not reachable, and the SNMP trap is not sent out. In the case of the RADIUS header, the NAS IP address is set to 0.0.0.0.

When this happens, an NMS application still receives the trap correctly but does not associate it with the correct IP address. As a consequence, the status of the device (icon) in the NMS application does not reflect the trap (that is, change the icon to red).

To prevent this:

1 When a trap is being sent out to a receiver, check the phase 2 routing table to determine a route to the receiver.

2 Determine if the receiver is a locally attached station on the management port.

3 If you have a default route in the routing table, use the next hop of the static route as the source (SRC) network address in the trap PDU.

4 If the IP header source address field is that of the management port IP address, there is a mismatch between the fields.

Chapter 12
Configuring RADIUS authentication and accounting using Device Manager

This chapter includes the following topics:

Enabling RADIUS authentication

To enable RADIUS authentication globally:

1 From the Device Manager menu bar, choose Edit > Security.

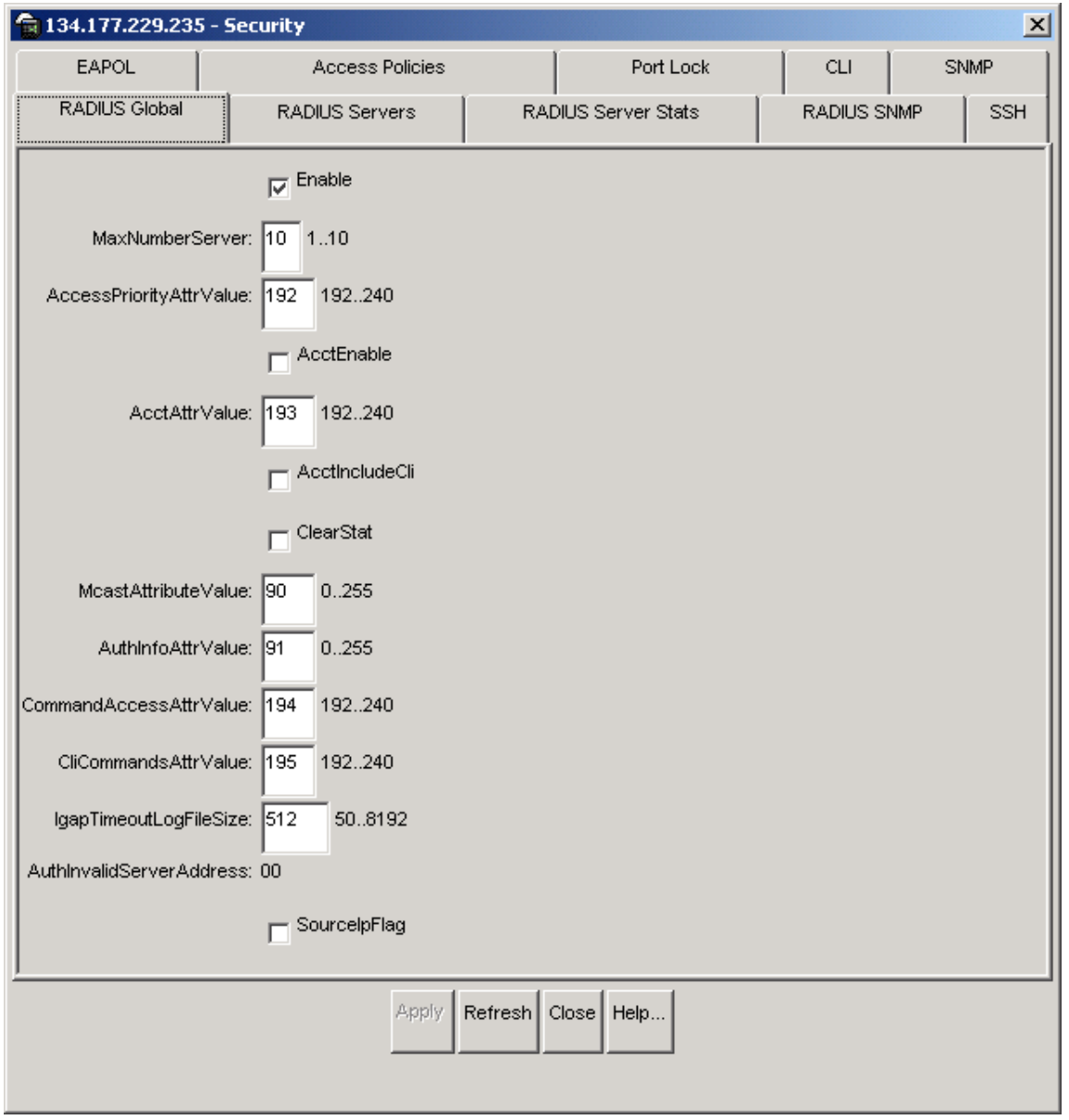
The EAPOL tab opens. (Figure 68)

Figure 68 Security tab

2 Click the RADIUS Global tab.

The RADIUS Global tab opens. (Figure 69)

Figure 69 Security dialog box—RADIUS Global tab



3 Click Enable.

4 Enter a value for the maximum number of servers in the MaxNumberServer field.

5 Enter an access policy value in the AccessPriorityAttrValue field (by default, this value is 192).

6 Click Apply.

Table 28 describes the RADIUS Global tab fields.

Table 28 Security dialog box—RADIUS Global tab fields

Fields	Description
Enable	Enables the RADIUS authentication feature globally.
MaxNumberServer	Specifies the maximum number of servers to be used, between 1 and 10, inclusive.
AccessPriorityAttrValue	Specific to RADIUS authentication. Sets the vendor-specific attribute value of the Access-Priority attribute to match the type value set in the dictionary file on the RADIUS server. The valid values are 192 through 240. Nortel Networks recommends the default setting of 192 for the Passport 8600 switch.
AcctEnable	Enables RADIUS accounting.
AcctAttrValue	Specific to RADIUS accounting. Sets the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server. This value *must* be different from the Access-priority attribute value configured for authentication. The valid values are 192 through 240. The default value is 193.
AcctIncludeCli	Specifies whether you want CLI commands included in RADIUS accounting requests.
ClearStat	Clears RADIUS statistics from the switch.
McastAttributeValue	Sets the value of the multicast address attribute.
AuthInfoAttrValue	Sets the value for the auth-info attribute.
CommandAccessAttrValue	Specifies the value of the command access attribute. The valid values are 192 through 240. The default value is 194.
CliCommandsAttrValue	Specifies the value of the CLI command attribute. The valid values are 192 through 240. The default value is 195.
IgapTimeoutLogFileSize	Sets the maximum size of the IGAP log file in KB.
AuthInvalidServerAddress	Invalid server address authentication.
SourceIpFlag	Enables, if selected, or disables the RADIUS packet source IP flag.

Enabling RADIUS accounting

Note: You must set up a RADIUS server and add it to the switch's configuration file before you can enable RADIUS accounting on the switch. Otherwise, the system displays an error message.

To enable RADIUS accounting:

1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the EAPOL tab displayed. (Figure 68)

2. Click the RADIUS Global tab.

   The RADIUS Global tab opens. (Figure 69)

3. Click AcctEnable.
4. Enter an access policy value in the AcctAttributeValue field (by default, this value is 193).
5. Click Apply.
6. Close the dialog box.

Note: To disable RADIUS accounting, you deselect AcctEnable. You cannot globally disable RADIUS accounting unless a server entry exists.

Adding a RADIUS server

To add a RADIUS server:

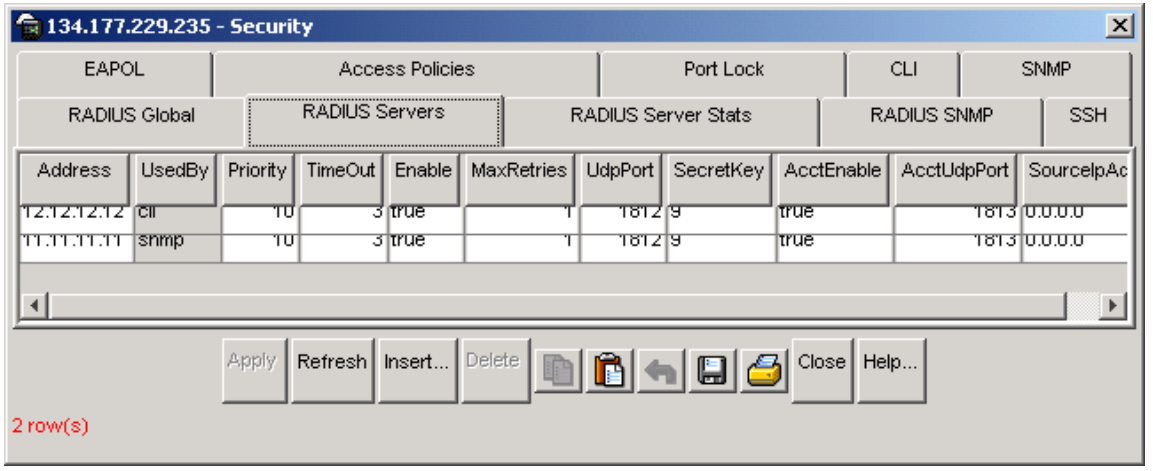
1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the EAPOL tab displayed. (Figure 68)

2. Click the RADIUS Servers tab.

   The RADIUS Servers tab opens. (Figure 70)

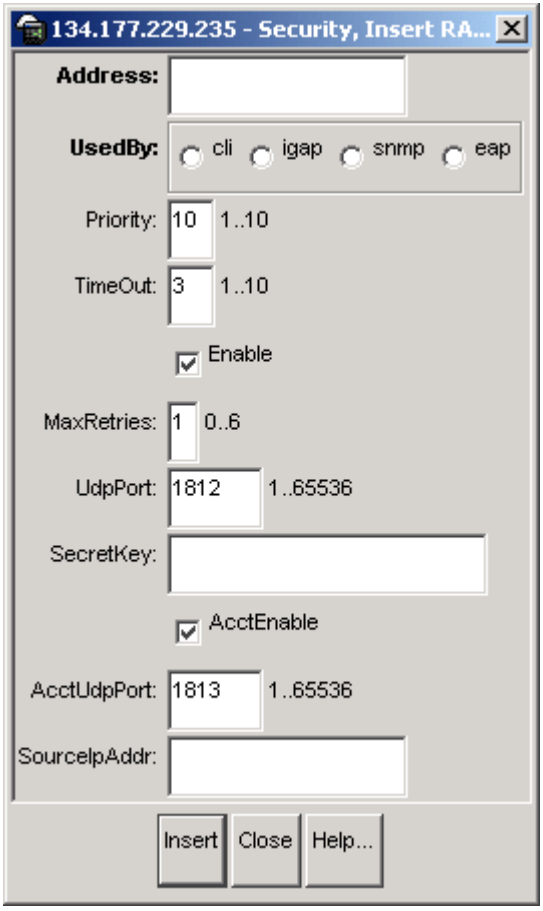
Figure 70 Security dialog box—RADIUS Servers tab



3 Click Insert.

The Security, Insert RADIUS Servers dialog box opens. (Figure 71)

Figure 71 Insert RADIUS Servers dialog RADIUS Servers tab



4 Enter the IP address of the RADIUS server that you want to add in the Address field.

5 Select a service for the Usedby field. Choose from either CLI, IGAP, SNMP, or EAP.

6 Enter a secret key.

7 Click Insert.

The information for the configured RADIUS server appears in the RADIUS Servers tab of the Security dialog box.

Table 29 describes the Security, Insert RADIUS Servers tab fields.

Table 29 Security dialog box—RADIUS Servers tab fields

Fields	Description
Address	The IP address of the RADIUS server.
UsedBy	Specifies the that service that this device will be used by. Choices are CLI, IGAP, SNMP, or EAP.
Priority	Specifies the priority of each server, or the order of servers to send authentication (1 to 10). The default is 10.
TimeOut	Specifies the time interval in seconds before the client retransmits the packet (1 to 6). The default is 3 seconds.
Enable	Enables or disables authentication on the server. The default is true.
MaxRetries	Specifies the maximum number of retransmissions allowed (1 to 6). The default is 3.
UdpPort	Specifies the UDP port that the client uses to send requests to the server (1 to 65536). The default value is 1812. **Note:** The UDP port value set for the client must match the UDP value set for the RADIUS server.
SecretKey	Specifies the RADIUS server secret key, which is the password used by the client to be validated by the server.
AcctEnable	Enables or disable RADIUS accounting. The default is true.
AcctUdpPort	Specifies the UDP port of the RADIUS accounting server (1to65536). The default value is 1813. **Note:** The UDP port value set for the client must match the UDP value set for the RADIUS server.
SourceIpAddr	Specifies the IP address of the source.

Reauthenticating the RADIUS SNMP server session

To reauthenticate the RADIUS SNMP server session:

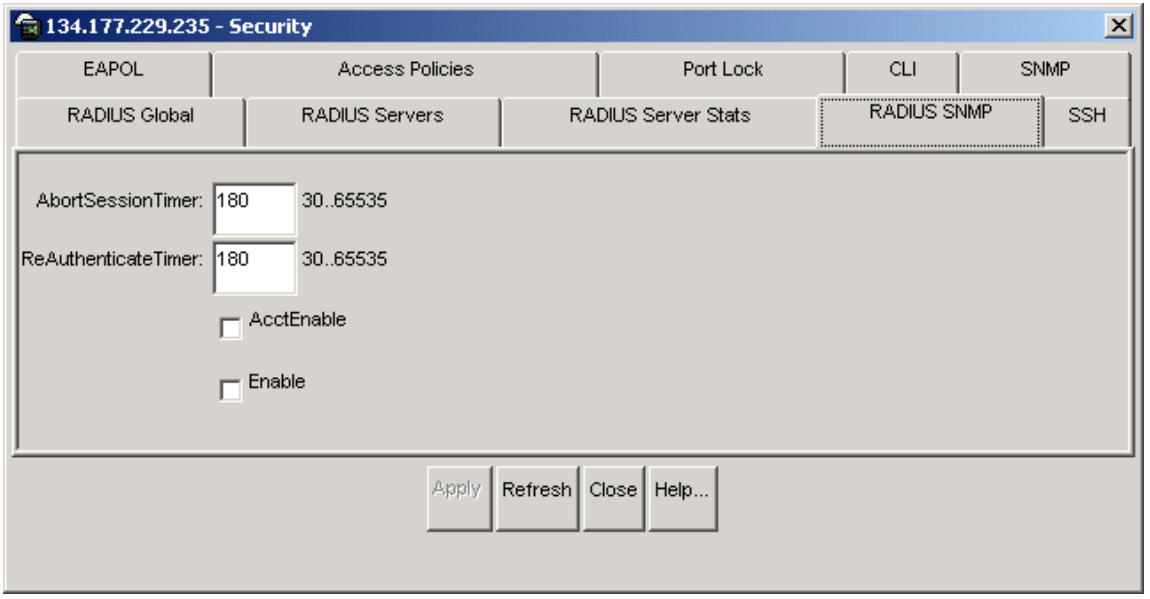
1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the EAPOL tab displayed. (Figure 68)

2. Click the RADIUS SNMP tab.

The RADIUS SNMP tab opens. (Figure 72)

Figure 72 Security dialog box—RADIUS SNMP tab



3 In the ReAuthenticateTimer field, enter a value (30 to 65535 seconds) to specify the interval between RADIUS SNMP server reauthentications.

4 Click Enable.

The timer for reauthentication of the RADIUS SNMP server session is enabled.

Note: To abort the RADIUS SNMP server session, enter a value for the AbortSessionTimer, and then click Enable.

5 To enable accounting and record the number of packets/octets received during the SNMP session, click AcctEnable.

Table 30 describes the Security, RADIUS SNMP tab fields.

Table 30 Security dialog box—RADIUS SNMP tab fields

Fields	Description
AbortSessionTImer	Specifies the allowable time, in seconds, before aborting the RADIUS SNMP server session (30 to 65535). The default is 180.
ReAuthenticateTimer	Specifies the time, in seconds, between reauthentications of the RADIUS SNMP server (30 to 65535). The default is 180.
AcctEnable	Enables or disables the RADIUS SNMP session timer. The default is true.
Enable	Enables or disables timer authentication on the server. The default is true.

Showing RADIUS server statistics

Note: You cannot access the Radius Server statistics from the CLI.

To show RADIUS server statistics on the switch:

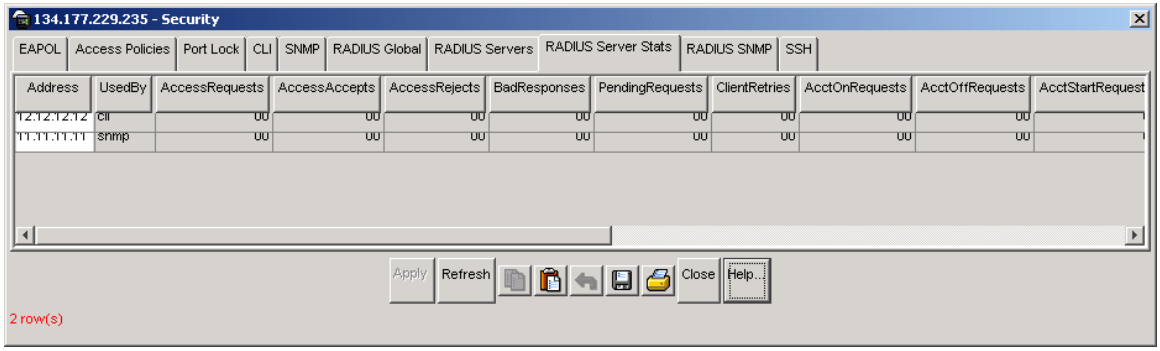
1 From the Device Manager menu bar, choose Edit > Security.

The Security dialog box opens with the EAPOL tab displayed. (Figure 68)

2 Click the RADIUS Servers Stats tab.

The RADIUS Servers Stats tab opens. (Figure 73)

Figure 73 Security dialog box—RADIUS Servers Stats tab



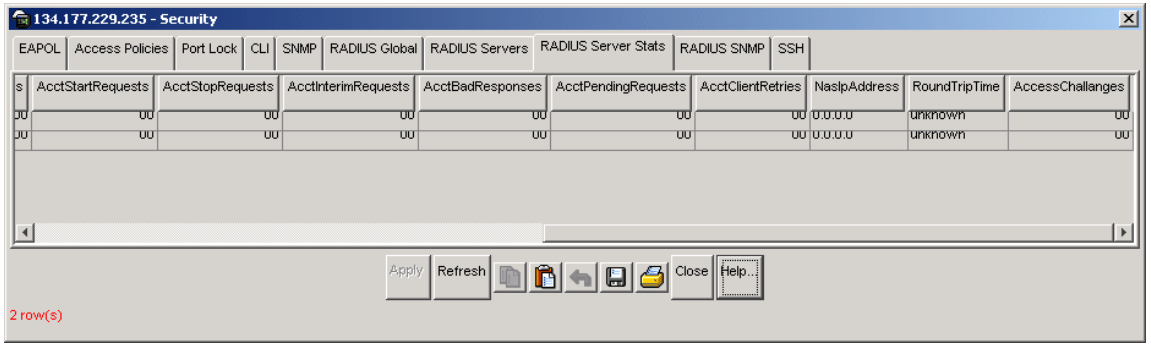


Table 31 describes the RADIUS Servers Stats tab fields.

Table 31 Security dialog box—RADIUS Server Stats tab fields

Item	Description
Address	The IP address of the RADIUS server.
UsedBy	The service that the RADIUS is being used by.
AccessRequests	Number of RADIUS access-response packets sent to this server. This does not include retransmissions.
AccessAccepts	Number of RADIUS access-accept packets, valid or invalid, received from this server.
AccessRejects	Number of RADIUS access-reject packets, valid or invalid, received from this server.
BadResponses	Number of RADIUS invalid access-response packets received from this server.

Table 31 Security dialog box—RADIUS Server Stats tab fields (continued)

Item	Description
PendingRequests	Number of RADIUS access-request packets sent to this server that have not yet received a response, or have timed out. This variable is increased when an access-request is sent and decreased due to receipt of an access-request, access-reject, a timeout, or retransmission.
ClientRetries	Number of authentication retransmissions to the server.
AcctOnRequests	Number of RADIUS accounting On requests sent to this server. This does not include retransmissions.
AcctOffRequests	Number of RADIUS accounting Off requests sent to this server. This does not include retransmissions.
AcctStartRequests	Number of RADIUS accounting Start requests sent to this server. This does not include retransmissions.
AcctStopRequests	Number of RADIUS accounting Stop requests sent to this server. This does not include retransmissions.
AcctInterimRequests	Number of RADIUS Accounting Interim requests sent to this server. This does not include retransmissions. Note: The AcctInterimRequests counter will increment only if you select AcctIncludeCli from the RADIUS Global tab. (Figure 69 on page 217)
AcctBadResponses	Number of Invalid Responses received from this server.
AcctPendingRequests	Number of RADIUS accounting requests waiting to be sent to the server. This variable is increased whenever any accounting request is sent to this server and decreased when an acknowledgement is received or timeout occurs.
AcctClientRetries	Number of RADIUS accounting requests retransmitted to this server.
NaslpAdress	The RADIUS client NAS identifier for this server.
RoundTripTime	The time difference between the instance when a RADIUS request is sent and the corresponding response is received.
AccessChallenges	Number of RADIUS access-challenges requests sent to this server. This does not include retransmissions.

Note: To clear server statistics, select ClearStat from the RADIUS Global tab (Figure 69) and click Apply.

Modifying a RADIUS configuration

To modify an existing RADIUS configuration:

1. From the Device Manager menu bar, choose Edit > Security.
   The Security dialog box opens with the EAPOL tab displayed. (Figure 68)
2. Click the RADIUS Servers tab.
   The RADIUS Servers tab opens. (Figure 70)
3. In the row to modify, type the information, or use the lists to make a selection.
   Access lists by left-clicking in a field.
4. Click Apply.

Deleting a RADIUS configuration

To delete an existing RADIUS configuration:

1. From the Device Manager menu bar, choose Edit > Security.
   The Security dialog box opens with the EAPOL tab displayed. (Figure 68)
2. Click the RADIUS Servers tab.
   The RADIUS Servers tab opens. (Figure 70)
3. Identify the configuration to delete by clicking anywhere in the row.
4. Click Delete.
5. Click Apply.

Chapter 13
CLI command logging

The CLI command logging feature provides the functionality of logging and encrypting the CLI and remote sessions (for example, Telnet and SSH). This provides a secured logging mechanism within the switch. The commands which are executed in the switch after booting up are stored in an encrypted format in a PCMCIA file accessible only to the rwa user.

When you execute a command from a session, the command is encrypted and stored in the clilog.txt file in the PCMCIA. The following attributes of the command are captured while logging:

- Sequence Number: Identifies a specific command.
- CPU Slot Number: Indicates the CPU slot from which the command is logged.
- Date & Time: The switch time at which the command is executed.
- Context: The type of the session used to connect to the switch. This includes Console, Modem, Telnet, SSH, Rlogin, FTP, TFTP. If it is a remote session, the remote IP address is identified.
- User name: This is the username used to login to the switch.
- Commands: The commands typed on the session as such.

Anything typed on the session will be logged as soon as the return key (enter key) is pressed. The commands logged can be decrypted and viewed by using the show commands provided by the feature. The decrypted commands can then be stored in the secondary storage devices or remote server by using the save command of the feature. All the above commands are accessible only to the RWA user. If the clilog.txt file in PCMCIA exceeds the maximum file size settings, then the file is automatically wrapped from the top.

This chapter includes the following topics:

Roadmap of CLI logging commands

The following roadmap lists the CLI logging commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config cli clilog enable <true/ false>`	
`config cli clilog maxfilesize <value>`	
`config cli clilog info`	
`show cli clilog info`	
`show clilog file [tail] [grep <value>]`	
`save clilog file <value>`	

Enabling CLI logging

To enable CLI logging on the switch, enter the following command:

```
config cli clilog enable <true/false>
```

where:
`true` enabled CLI command logging.
`false` disables CLI command logging.

Figure 74 shows sample output for the **`config cli clilog enable`** command.

Figure 74 config cli clilog enable <true/false> command output

```
Passport-8610:5/config/cli/clilog# enable true
Passport-8610:5/config/cli/clilog# info

Sub-Context:
Current Context:

                     enable : TRUE
                maxfilesize : 500
```

Setting the maximum allowable file size for the clilog.txt file in PCMCIA

To configure the maximum allowable file size for the clilog.txt file, enter the following command:

```
config cli clilog maxfilesize <value>
```

This command includes the following options:

config cli clilog maxfilesize followed by:	
<value>	The maximum allowable file size in KBs for the clilog.txt file in the PCMCIA. The minimum configurable value is 64KB and the maximum configurable value is 256MB. The default value is 256KB. **Note:** You can configure maxFileSize value of the clilog.txt file below the previously configured value. In this situation, if the file size has already become bigger than the newly configured value, the clilog.txt file will start wrapping at the present size. Similar behavior can be observed on failover scenarios, if the clilog.txt file exceeds the configured maxFileSize while failing over.

Figure 75 shows sample output for the **config cli clilog maxfilesize** command.

Figure 75 config cli clilog maxfilesize command output

```
Passport-8610:5/config/cli/clilog# maxfilesize 500
Passport-8610:5/config/cli/clilog# info

Sub-Context:
Current Context:

                     enable : TRUE
                maxfilesize : 500
```

Note: If a secondary CPU is present in the chassis, the configuration commands take effect in the secondary CPU as well when they are executed from the primary. While inserting a secondary CPU, the status of the clilog feature is checked and if the feature is enabled in the primary, the secondary takes the values of the global parameters from the primary CPU. However, the primary CPU and the secondary CPU work as separate CLI logging mechanisms, logging the commands independently on the primary and secondary PCMCIAs.

Viewing the clilog settings

To view the clilog command settings, enter the following command:

```
config cli clilog info
```

Figure 76 shows sample output for the **config cli clilog info** command.

Figure 76 config cli clilog info command output

```
Passport-8610:5/config/cli/clilog# info

Sub-Context:
Current Context:

                     enable : TRUE
                maxfilesize : 500
```

Displaying the status of clilog global parameters

To display status of the clilog global parameters, enter the following command:

```
show cli clilog info
```

Figure 77 shows sample output for the **show cli clilog info** command.

Figure 77 show cli clilog info command output

```
Passport-8610:5# show cli clilog info

================================================================================
                       CLILog Info
================================================================================

        CLI Logging Enable    :  TRUE

        CLI Log Max File Size :  500
--------------------------------------------------------------------------------
```

Viewing the decrypted log

To decrypt the clilog.txt file in the PCMCIA and display the log in a user readable form, enter the following command:

```
show clilog file [tail] [grep <value>]
```

This command includes the following options:

show clilog file followed by:	
`tail`	Displays the log file from the bottom.
`grep <value>`	Enables you to grep on the text specified and displays only the logs matching the text.

Figure 78 shows sample output for the **`show clilog file <tail> grep <text to be grepped>`** command.

Figure 78 show clilog file command output

```
Passport-8610:5# sho clilog file
Slot5    1 [01/27/04 17:15:53] TELNET:198.202.188.174 rwa maxfilesize 500
Slot5    2 [01/27/04 17:15:55] TELNET:198.202.188.174 rwa info
Slot5    3 [01/27/04 17:17:03] TELNET:198.202.188.174 rwa ?
Slot5    4 [01/27/04 17:17:18] TELNET:198.202.188.174 rwa maxfile ?
Slot5    5 [01/27/04 17:17:31] TELNET:198.202.188.174 rwa ena ?
Slot5    6 [01/27/04 17:18:39] TELNET:198.202.188.174 rwa sho clilog file
Slot5    7 [01/27/04 17:18:51] TELNET:198.202.188.174 rwa sho clilog file
tail
Slot5    8 [01/27/04 17:19:10] TELNET:198.202.188.174 rwa ena f

Passport-8610:5# sho clilog file tail
Slot5   21 [01/27/04 17:33:39] TELNET:198.202.188.174 rwa sho clilog file
tail
Slot5   20 [01/27/04 17:33:21] TELNET:198.202.188.174 rwa sho clilog file
Slot5   19 [01/27/04 17:33:00] TELNET:198.202.188.174 rwa sho clilog file ?
Slot5   18 [01/27/04 17:32:33] TELNET:198.202.188.174 rwa sho cli clilog info
Slot5   17 [01/27/04 17:32:27] TELNET:198.202.188.174 rwa sho clilog info
Slot5   16 [01/27/04 17:32:24] TELNET:198.202.188.174 rwa box
```

Saving the clilog file

To save the decrypted log file into a device (PCMCIA, Flash or tftp server), enter the following command:

```
save clilog file <value>
```

This command includes the following options:

save clilog file followed by:	
<value>	Specifies the destination file. The destination can be flash, PCMCIA or a remote tftp server.

Figure 79 shows sample output for the **save clilog file** command.

Figure 79 save clilog file command output

```
Passport-8610:5# save clilog file /flash/clilog.txt
```

Chapter 14
Preventing denial of service (DOS) attacks

You can use either directed broadcasts or the **high-secure** flag to prevent possible DOS attacks.

Directed broadcasts

A directed broadcast is a frame sent to the subnet broadcast address on a remote IP subnet. By disabling (or suppressing) directed broadcasts on an interface, you cause all frames sent to the subnet broadcast address for a local router interface to be dropped. Disabling directed broadcasts protects hosts from possible denial of service (DOS) attacks. By default, this feature is enabled on the switch.

To configure the switch to forward directed broadcasts for a VLAN, use the following command:

```
config vlan <vid> ip directed-broadcast
```

where:
vid is a VLAN ID.

This command includes the following options:

config vlan <*vid*> ip directed-broadcast followed by:	
`info`	Displays information about the directed broadcast suppression settings.
`disable`	Prevents the switch from forwarding directed broadcast frames to the specified VLAN.
`enable`	Allows the switch to forward directed broadcast frames to the specified VLAN. The default setting for this feature is enabled.

Note: When directed broadcast suppression is enabled (the default setting), the CPU does not receive a copy of the directed broadcast. As a result, the switch does not respond to a subnet broadcast ping sent from a remote subnet.

high-secure flag

To protect the Passport 8000 Series switch against IP packets with illegal source address of 255.255.255.255 from being routed (per RFC 1812 Section 4.2.2.11 and RFC 971 Section 3.2) [or IP addresses such as loopback or a Src IP address of all ones, or Class D or Class E addresses from being routed], the Passport 8000 Series switch now supports a configurable flag, called **`high-secure`**.

This flag is disabled by default. Note that when you enable this flag, the desired behavior (not routing source packets with an IP address of 255.255.255.255) is applied on all ports belonging to the same OctaPID.

This configurable flag is used in the following CLI command:

`config ethernet <`*`slot`*`|`*`port`*`> high-secure <true|false>`

where:
`true` enables the high secure feature for the specified port or ports. This feature blocks packets with illegal IP addresses.
`false` disabled the high secure feature for the specified port of ports. This feature is disabled by default.

Note: When you enable this flag, the desired behavior (not routing source packets with an IP address of 255.255.255.255) is applied on all ports belonging to the same component. DHCP and BootP are suppressed.

Chapter 15
Configuring EAPOL using CLI

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access control protocol. EAPoL provides security to your network by preventing users from accessing network resources before they are authenticated.

EAPoL allows you to set up network access control on internal LANs and to exchange authentication information between any end station or server connected to the Passport 8000 Series switch and an authentication server (such as a RADIUS server). This security feature extends the benefits of remote authentication to internal LAN clients. For example, if a new client PC fails the authentication process, EAPoL prevents it from accessing the network.

This chapter includes the following topics:

Roadmap of CLI EAPoL commands

The following roadmap lists the CLI EAPoL commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
config radius server create <ipaddr> secret <value> usedby eapol	
config radius server delete <ipaddr> usedby eapol	
config radius server set <ipaddr> usedby eapol	
config ethernet <portlist> eapol admin-status force-unauthorized	
config ethernet <portlist> eapol admin-status force	
config sys set eapol enable	
config sys set eapol disable	
config sys set eapol info	
config ethernet <portlist> eapol	info
	admin-status <auto|force-unauthorized|force-authorized>
	admin-traffic-control <incoming-and-outgoing|incoming-only>
	initialize
	max-req <1...10>
	quiet-period <1...65535>
	reauthentication <true|false>
	reauthenticate-now <true|false>
	reauthentication-period <1...2147483647>
	server-timeout <1...65535>

Command	Parameter
	sess-manage-mode <true|false>
	sess-manage-open-immediate <true|false>
	supplicant-timeout <1...65535>
	transmit-period <1...65535>
show sys eapol	
show ports info eapol auth-stats [<portlist>]	
show ports info eapol auth-diags [<portlist>]	
show ports info eapol session-stats [<portlist>]	
show ports info eapol config [<portlist>]	
show ports info eapol oper-stats [<portlist>]	

Configuration prerequisites

Use the following configuration rules when using EAPoL:

- Before configuring your switch, you must configure at least one EAPoL RADIUS Server and Shared Secret fields.
- You cannot configure EAPoL on ports that are currently configured for:
  - Shared segments
  - MultiLink Trunking
  - Port mirroring
- Change the `status` to *auto* for each port that you want to be controlled (see "Changing a port's authentication status" on page 244). The *auto* setting automatically authenticates the port according to the results of the RADIUS server. The default authentication setting for each port is *force-authorized*.
- You can connect only a single client on each port that is configured for EAPoL. (If you attempt to add additional clients on the EAPoL authorized port, the port goes to force-unauthorized mode).

EAPoL uses RADIUS protocol for EAPoL-authorized logins.

Configuring an EAPoL-enabled RADIUS server

The Passport 8000 Series switch uses RADIUS servers for authentication and accounting services. To add an EAPoL-enabled RADIUS server, use the following command:

```
config radius server create <ipaddr> secret <value> usedby
eapol
```

where:
ipaddr indicates the IP address of the selected server and
value specifies the secret key, which is a string of up to 20 characters.

The RADIUS server uses this password to validate users.

Note: The `usedby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`eapol` - configures the server for EAPoL authentication.
`snmp` - configures the server for SNMP authentication.
`igap` - configures the server for IGAP authentication.

The other parameters that you can use with this command are:

```
[port <value>] [priority <value>] [retry <value>]
[timeout <value>] [enable <value>] [acct-port <value>]
[acct-enable <value>] [source-ip <value>]
```

Deleting an EAPoL-enabled RADIUS server

To delete an EAPoL-enabled RADIUS server, use the following command:

```
config radius server delete <ipaddr> usedby eapol
```

where:
ipaddr indicates the IP address of the selected server.

Note: The `usedby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`eapol` - configures the server for EAPoL authentication.
`snmp` - configures the server for SNMP authentication.
`igap` - configures the server for IGAP authentication.

Setting EAPoL-enabled RADIUS server parameters

To set EAPoL-enabled RADIUS server parameters without having to delete the server and re-create the server again, use the following command:

```
config radius server set <ipaddr> usedby eapol
```

where:
ipaddr indicates the IP address of the selected server.

Note: The `useby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`eapol` - configures the server for EAPoL authentication.
`snmp` - configures the server for SNMP authentication.
`igap` - configures the server for IGAP authentication.

The other parameters that you can use with this command are:

```
[secret <value>] [port <value>] [priority <value>]
[retry <value>] [timeout <value>] [enable <value>]
[acct-port <value>] [acct-enable <value>] [source-ip
<value>]
```

Changing a port's authentication status

Ports are **force-authorized** by default. This means that the ports are always authorized and are not authenticated by the RADIUS server.

You can change this setting so that the ports are always unauthorized (**`force-unauthorized`**). You can also make the ports *controlled* so that they are automatically authenticated when you globally enable EAPoL (**`auto`**).

To configure a port so it is always unauthorized, use the following command:

```
config ethernet <portlist> eapol admin-status
force-unauthorized
```

To configure a port so it is authenticated automatically, use the following command:

```
config ethernet <portlist> eapol admin-status force
```

Globally configuring EAPoL on the switch

The `eapol` command globally enables or disables EAPoL on the switch. (By default, EAPoL is disabled.) With this one command, you can make all the **controlled** ports on the switch EAPoL-enabled.

To perform the following tasks, enter the commands in the global configuration mode.

To enable EAPoL globally on the switch, use the following command:

```
config sys set eapol enable
```

To disable EAPoL globally on the switch, use the following command:

```
config sys set eapol disable
```

To see how the switch is currently configured, use the following command:

```
config sys set eapol info
```

Figure 80 is sample output using **`config sys set eapol info`** command.

Figure 80 config sys set eapol info command sample output

```
TOKYO>:5# config sys set eapol info
                                    eap : disabled
                              sess-manage : false
TOKYO>:5#
```

Configuring EAPoL on a port

To configure EAPoL on a specific port, use the following command:

```
config ethernet <portlist> eapol
```

where:
portlist use the convention {slot/port[-slot/port][, ...]}.

This command includes the following parameters:

config ethernet <portlist> eapol followed by:	
info	Displays information about the current EAPoL configuration on this port.
admin-status <*auto*|*force-unauthorized*|*force-authorized*>	Sets the authentication status for this port. The default is ***authorized***. *auto* - port authorization depends on the results of the EAPoL authentication by the RADIUS server. *force-unauthorized* - port is always unauthorized. *force-authorized* - port is always authorized.
admin-traffic-control <*incoming-and-outgoing*|*incoming-only*>	Sets the traffic control direction. *incoming-and-outgoing* - traffic direction is both incoming and outgoing. *incoming-only* - traffic direction is only incoming.
initialize	Initializes EAPoL authentication on this port.
max-req <1...10>	Sets the maximum number of times to retry sending packets to the Supplicant. The default is 2.
quiet-period <1...65535>	Sets the time interval (in seconds) between authentication failure and the start of a new authentication. The default is 60.
reauthentication <true|false>	When enabled (true), re-authenticates an existing Supplicant at the time interval specified in reauthentication-period <1...2147483647>. The default is false.
reauthenticate-now <true|false>	Reauthenticates the Supplicant connected to this port immediately.
reauthentication-period <1...2147483647>	Sets the time interval (in seconds) between successive re-authentications (see "reauthentication <true|false>"). The default is 3600 (1 hour).

config ethernet <portlist> eapol followed by:	
server-timeout <1...65535>	Sets the time (in seconds) to wait for a response from the RADIUS server. The default is 30.
sess-manage-mode <true|false>	Enables (true) or disables (false) the session port to be managed by an external device.
sess-manage-open-immediate <true|false>	Sets the port to be opened immediately after 8021x authentication true enables the opening of the port immediately after 802.1x authentication. false disables the opening of the port immediately after 802.1x authentication.
supplicant-timeout <1...65535>	Sets the time (in seconds) to wait for a response from a Supplicant for all EAP packets except EAP Request/Identity packets. The default is 30.
transmit-period <1...65535>	Sets the time (in seconds) to wait for a response from a Supplicant for EAP Request/ Identity packets. The default is 30.

Configuration example: EAPoL

The following configuration example uses the commands described above to perform the following tasks on port 5/5.

- Set the status so the port is automatically authenticated.
- Retry sending packets to the Supplicant up to four times maximum.
- Wait 120 seconds between an authentication failure and another attempt.
- Wait 90 seconds for the Supplicant's response to EAP Request/Identity packets.
- Wait 90 seconds for a response from the RADIUS server.
- Wait 90 seconds for the Supplicant's response to all EAP packets, except EAP Request/Identity packets.
- Wait 7200 seconds (2 hours) between successive re-authentications.
- Set re-authentication to enable so that the Supplicant will be re-authenticated every 90 seconds, as specified by the re-authentication period.

Figure 81 shows sample output for using the commands for this configuration example. The **`config ethernet <portlist> eapol info`** command shows a summary of the results.

Figure 81 eapol configuration command sample output

```
TOKYO>:5# config ethernet 1/1 eapol admin-status auto
TOKYO>:5# config ethernet 1/1 eapol max-req 4
TOKYO>:5# config ethernet 1/1 eapol quiet-period 120
TOKYO>:5# config ethernet 1/1 eapol transmit-period 90
TOKYO>:5# config ethernet 1/1 eapol server-timeout 90
TOKYO>:5# config ethernet 1/1 eapol supplicant-timeout 90
TOKYO>:5# config ethernet 1/1 eapol reauthentication-period 7200
TOKYO>:5# config ethernet 1/1 eapol info
                        admin-status : auto
                admin-traffic-control : incoming-and-outgoing
                             max-req : 4
                       quiet-period : 120
                    transmit-period : 90
                     server-timeout : 90
                   sess-manage-mode : false
                  supplicant-timeout  : 90
              reauthentication-period : 7200
                     reauthentication : false
TOKYO>:5#
```

Showing EAPoL statistics

The Passport 8000 Series switch provides the following `show` commands to help you monitor and troubleshoot your switch:

- “Showing the switch’s EAPoL status” on page 249
- “Showing EAPoL Authenticator statistics” on page 249
- “Showing EAPoL Authenticator diagnostics” on page 250
- “Showing EAPoL Authenticator session statistics” on page 253
- “Showing EAPoL configuration statistics” on page 255
- “Showing EAPoL operation statistics” on page 256

Showing the switch's EAPoL status

To display how the switch is currently configured, use the following command:

```
show sys eapol
```

Figure 82 shows sample output for this command.

Figure 82 show sys eapol command sample output

```
TOKYO>:5# show sys eapol
                                        eap : disabled
                                sess-manage : false
TOKYO>:5#
```

Showing EAPoL Authenticator statistics

To display the Authenticator statistics, use the following:

```
show ports info eapol auth-stats [<portlist>]
```

Figure 83 shows sample output for this command.

Figure 83 show ports info eapol auth-stats command sample output

```
TOKYO>:5# show ports info eapol auth-stats 1/1

================================================================================
                                    Eap Authenticator Statistics
================================================================================
PORT  TOTAL TOTAL START LOGOFF RESP_ID RESP REQ-ID REQ INVALID LENGTH FRAME LAST-SRC
      RX    TX    RCVD  RCVD   RCVD    RCVD TX     TX  FRAMES  ERROR  VER   MAC
--------------------------------------------------------------------------------
1/1   0     0     0     0      0       0    0      0   0       0      0     00:00:00:00:00:00
--------------------------------------------------------------------------------
TOKYO>:5#
```

Table 32 describes the parameters in the Eap Authenticator Statistics table.

Table 32 show ports info eapol auth-stats parameters

Field	Description
TOTAL RX	Displays the number of valid EAPoL frames of any type that have been received by this Authenticator.
TOTAL TX	Displays the number of EAPoL frame types of any type that have been transmitted by this Authenticator.
START RCVD	Displays the number of EAPoL start frames that have been received by this Authenticator.
LOGOFF RCVD	Displays the number of EAPoL logoff frames that have been received by this Authenticator.
RESP_ID RCVD	Displays the number of EAPoL Resp/Id frames that have been received by this Authenticator.
RESP RCVD	Displays the number of valid EAP Response frames (Other than Resp/Id frames) that have been received by this Authenticator.
REQ_ID TX	Displays the number of EAPoL Req/Id frames that have been transmitted by this Authenticator.
REQ TX	Displays the number of EAP Req/Id frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
INVALID FRAMES	Displays the number of EAPoL frames that have been received by this Authenticator in which the frame type is not recognized.
LENGTH ERROR	Displays the number of EAPoL frames that have been received by this Authenticator in which the packet body length field is not valid.
FRAME VER	Displays the protocol version number that was in the most recently received EAPoL frame.
LAST_SRC MAC	Displays the source MAC address that was in the most recently received EAPoL frame.

Showing EAPoL Authenticator diagnostics

To display the Authenticator diagnostics, use the following command:

```
show ports info eapol auth-diags [<portlist>]
```

Figure 84 shows sample output for this command.

Figure 84 show ports info eapol auth-diags command sample output

```
Passport-8603:3# show ports info eapol auth-diags 2/14-2/20

================================================================================
                    Eap Authenticator Diagnostics Table
================================================================================
Port                    2/14   2/15   2/16   2/17   2/18   2/19   2/20
--------------------------------------------------------------------------------
Enter Conn              3      0      0      0      0      0      0
Logoff While Conn       0      0      0      0      0      0      0
Enter Authing           2      0      0      0      0      0      0
Success While Authing   1      0      0      0      0      0      0
Timeout while Authing   0      0      0      0      0      0      0
Fail While Authing      1      0      0      0      0      0      0
Reauths While Authing   0      0      0      0      0      0      0
Starts While Authing    0      0      0      0      0      0      0
Logoffs While Authing   0      0      0      0      0      0      0
Reauths While Authed    0      0      0      0      0      0      0
Starts While Authed     0      0      0      0      0      0      0
Logoffs While Authed    0      0      0      0      0      0      0
Bkend Resps             3      0      0      0      0      0      0
Bkend Access Chall      1      0      0      0      0      0      0
Bkend Reqs ToSupp       1      0      0      0      0      0      0
Bkend NonNak From Supp  1      0      0      0      0      0      0
Bkend Auth Succ         1      0      0      0      0      0      0
Bkend Auth Fails        1      0      0      0      0      0      0
```

Table 33 describes the parameters in the Eap Authenticator Diagnostics Table.

Table 33 show ports info eapol auth-diags parameters

Field	Description
Enter Conn	Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from any other state.
Logoff While Conn	Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPoL-Logoff message.

Table 33 show ports info eapol auth-diags parameters

Field	Description
Enter Auth-ing	Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/ Identity message being received from the Supplicant.
Success While Auth-ing	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the Supplicant.
Timeout While Auth-ing	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout.
Fail While Auth-ing	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure.
Reauths While Auth-ing	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of a reauthentication request.
Starts While Auth-ing	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPoL-Start message being received from the Supplicant.
Logoffs While Auth-ing	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPoL-Logoff message being received from the Supplicant.
Reauths While Authed	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of a reauthentication request.
Starts While Authed	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of an EAPoL-Start message being received from the Supplicant.
Logoffs While Authed	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Disconnected as a result of an EAPoL-Logoff message being received from the Supplicant.
Bkend Responses	Counts the number of times that the Backend Authentication state machine sends an Initial-Access request packet to the Authentication server.

Table 33 show ports info eapol auth-diags parameters

Field	Description
Bkend Access Challenge	Counts the number of times that the Backend Authentication state machine receives an Initial-Access challenge packet from the Authentication server.
Bkend OtherReqs ToSupp	Counts the number of times that the Backend Authentication state machine sends an EAP request packet (other than an Identity, Notification, failure, or success message) to the Supplicant.
Bkend NonNak FromSupp	Counts the number of times that the Backend Authentication state machine receives a response from the Supplicant to an initial EAP request and the response is something other than EAP-NAK.
Bkend Auth Successes	Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server.
Bkend Auth Fails	Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server.

Showing EAPoL Authenticator session statistics

To display the Authenticator statistics per session, use the following command:

```
show ports info eapol session-stats [<portlist>]
```

Figure 85 shows sample output for this command.

Figure 85 show ports info eapol session-stats command sample output

```
TOKYO>:5# show ports info eapol session-stats 1/1

================================================================================
                                          Eap Authenticator Session Statistics
================================================================================
     TOTAL     TOTAL     TOTAL     TOTAL
     OCTETS    OCTETS    FRAMES    FRAMES    SESSION   AUTHENTIC SESSION             TERMINATE
USER
PORT  RCVD      TXMT      RCVD      TXMT      ID        METHOD    TIME                CAUSE
NAME
--------------------------------------------------------------------------------
1/1   0       0       0       0               none     0 day(s), 00:00:00   none
--------------------------------------------------------------------------------
TOKYO>:5#
```

Table 34 describes the parameters in the Eap Authenticator Session Statistics table.

Table 34 show ports info eapol session-stats parameters

Field	Description
TOTAL OCTETS RCVD	Displays the number of octets received in user data frames on this port during the session.
TOTAL OCTETS TXMT	Displays the number of octets transmitted in user data frames on this port during the session.
TOTAL FRAMES RCVD	Displays the number of user data frames received on this port during the session.
TOTAL FRAMES TXMT	Displays the number of user data frames transmitted on this port during the session.
SESSION ID	Displays a unique identifier for the session that is at least three characters.
AUTHENTIC METHOD	Displays the authentication method (remote or local RADIUS server) used to establish the session.
SESSION TIME	Displays the duration of the session (in seconds).

Table 34 show ports info eapol session-stats parameters

Field	Description
TERMINATE CAUSE	Displays the reason for the session being terminated. The possible reasons are: **Supplicant logoff** **Supplicant restart** **Control force unauthorized** **Port admin disabled** **Port failure** **Re-authentication failed** **Port re-initialized** **Not terminated yet**
USER NAME	Displays the user name of the Supplicant PAE.

Showing EAPoL configuration statistics

To display configuration information for the Supplicant PAE associated with each selected port, use the following command:

```
show ports info eapol config [<portlist>]
```

Figure 86 shows sample output for this command.

Figure 86 show ports info eapol config command sample output

```
TOKYO>:5# show ports info eapol config 1/1

================================================================================
                                    Eap Config
================================================================================
PORT  ADMIN              CTRL MAX QUIET      TRANSMIT   SERVER     SUPPLICANT REAUTHEN-  REAUTH
      STATUS             DIR  REQ PERIOD     PERIOD     TIMEOUT    TIMEOUT    TICATION   PERIOD
--------------------------------------------------------------------------------
1/1   auto               both 4   120        90         90         90         false    7200
1/2   force-authorized   both 2   60         30         30         30         false    3600
1/3   force-authorized   both 2   60         30         30         30         false    3600
1/4   force-authorized   both 2   60         30         30         30         false    3600
1/5   force-authorized   both 2   60         30         30         30         false    3600
1/6   force-authorized   both 2   60         30         30         30         false    3600
1/7   force-authorized   both 2   60         30         30         30         false    3600
1/8   force-authorized   both 2   60         30         30         30         false    3600
--------------------------------------------------------------------------------
TOKYO>:5#
```

Table 35 describes the parameters in the Eap Config table.

Table 35 show ports info eapol config parameters

Item	Description
ADMIN STATUS	Displays the authentication status for this port. *force-unauthorized* - port is always unauthorized. *auto* - port authorization depends on the results of the EAPoL authentication by the RADIUS server. *force-authorized* - port is always authorized.
MAX REQ	Displays the maximum number of times to retry sending packets to the Supplicant.
QUIET PERIOD	Displays the time interval (in seconds) between authentication failure and the start of a new authentication.
TRANSMIT PERIOD	Displays the time (in seconds) that the Authenticator waits for a response from a Supplicant for EAP Request/Identity packets.
SERVER TIMEOUT	Displays the time (in seconds) that the Authenticator waits for a response from the RADIUS server.
SUPPLICANT TIMEOUT	Displays the time (in seconds) that the Authenticator waits for a response from a Supplicant for all EAP packets except EAP Request/Identity packets.
REAUTHENTICATION	When set to true, the Authenticator re-authenticates a Supplicant at the time interval specified in REAUTH PERIOD.
REAUTH PERIOD	Displays the time interval (in seconds) between successive re-authentications.

Showing EAPoL operation statistics

To display statistical information about the Authenticator, use the following command:

```
show ports info eapol oper-stats [<portlist>]
```

Figure 87 shows sample output for this command.

Figure 87 show ports info eapol oper-stats command sample output

```
TOKYO>:5# show ports info eapol oper-stats

================================================================================
                                      Eap Oper Stats
================================================================================
PORT  CTRL   PORT          PAE                BKEND
      DIR    STATUS        STATUS             STATUS
--------------------------------------------------------------------------------
1/1   both   authorized force-authorized idle
1/2   both   authorized force-authorized idle
1/3   both   authorized force-authorized idle
1/4   both   authorized force-authorized idle
1/5   both   authorized force-authorized idle
1/6   both   authorized force-authorized idle
1/7   both   authorized force-authorized idle
1/8   both   authorized force-authorized idle
--------------------------------------------------------------------------------
TOKYO>:5#
```

Table 36 describes the parameters in the Eap Oper Stats table.

Table 36 show ports info eapol oper-stats parameters

Item	Description
PORT STATUS	Displays the authentication status for this port. *unauthorized* - port is always unauthorized. *auto* - port authorization depends on the results of the EAPoL authentication by the RADIUS server. *authorized* - port is always authorized.
PAE STATUS	Displays the current Authenticator PAE state. The possible states are: **initialized** **disconnected** **connecting** **authenticating** **authenticated** **aborting** **held** **force-authorized** **force-unauthorized**
BKEND STATUS	Displays the current state of Backend Authentication. The possible states are: **request** **response** **success** **fail** **timeout** **idle** **initialize**

Chapter 16
Configuring EAPoL using Device Manager

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access control protocol. EAPoL provides security to your network by preventing users from accessing network resources before they are authenticated.

EAPoL allows you to set up network access control on internal LANs and to exchange authentication information between any end station or server connected to the Passport 8000 Series switch and an authentication server (such as a RADIUS server). This security feature extends the benefits of remote authentication to internal LAN clients. For example, if a new client PC fails the authentication process, EAPoL prevents it from accessing the network.

This chapter includes the following topics:

Configuration prerequisites

Use the following configuration rules when using EAPoL:

- Before configuring your switch, you must configure at least one EAPoL RADIUS Server and Shared Secret fields.
- You cannot configure EAPoL on ports that are currently configured for:

  - — Shared segments
  - — MultiLink Trunking
  - — Port mirroring
- Change the `status` to *auto* for each port that you want to be controlled (see "Changing a port's authentication status" on page 260). The *auto* setting automatically authenticates the port according to the results of the RADIUS server. The default authentication setting for each port is *force-authorized*.
- You can connect only a single client on each port that is configured for EAPoL. (If you attempt to add additional clients on the EAPoL authorized port, the port goes to force-unauthorized mode).

EAPoL uses RADIUS protocol for EAPoL-authorized logins.

Changing a port's authentication status

Ports are forceAuthorized by default. This means that the ports are always authorized and are not authenticated by the RADIUS server.

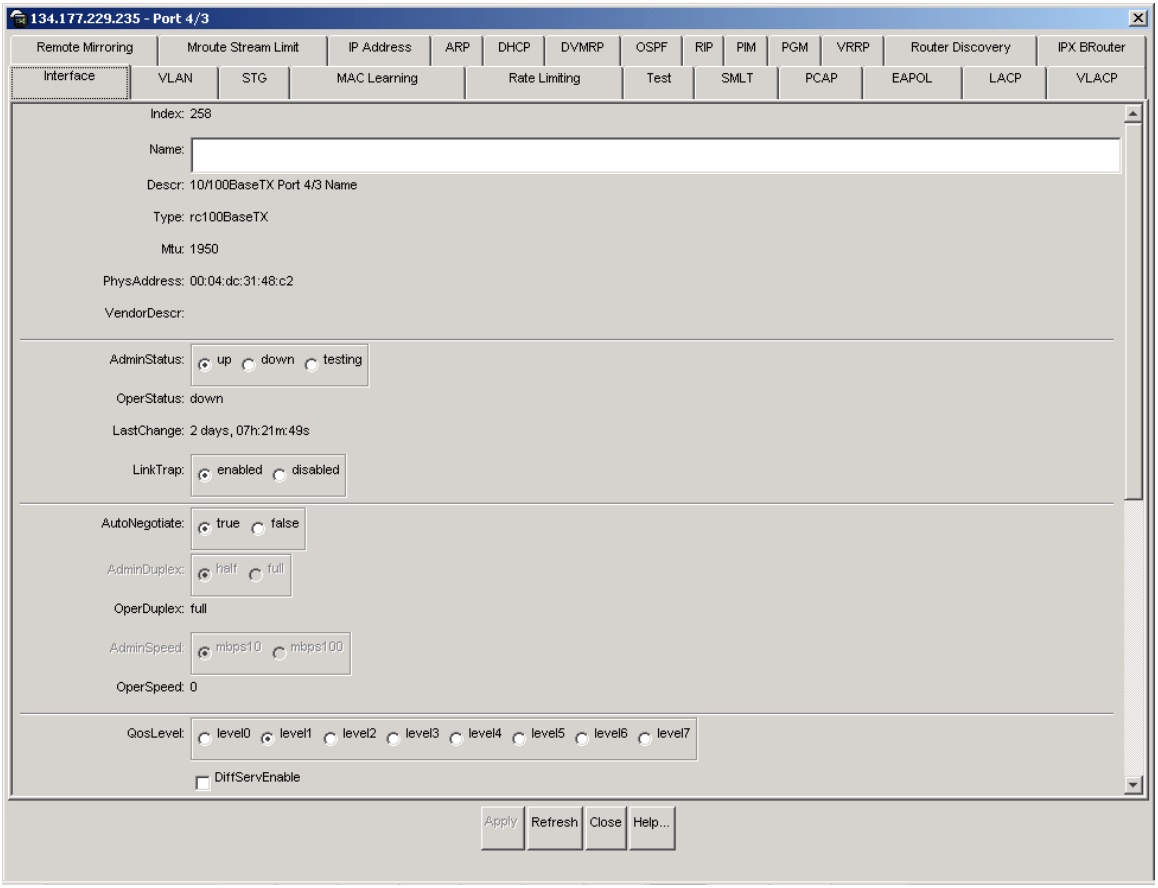
You can change this setting so that the ports are always unauthorized (**forceUnauthorized**). You can also make the ports *controlled* so that they are automatically authenticated when you globally enable EAPoL (**auto**).

To change the authentication status:

1. Select the port you want to edit.
2. Do one of the following:
   - Double-click the selected port
   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Port.
   - On the toolbar, click Edit.

   The Port dialog box for a single port opens with the Interface tab displayed. (Figure 88)

Figure 88 Port dialog box—Interface tab



3 Click EAPOL.

The EAPOL tab opens. (Figure 89)

Figure 89 Port dialog box—EAPOL tab

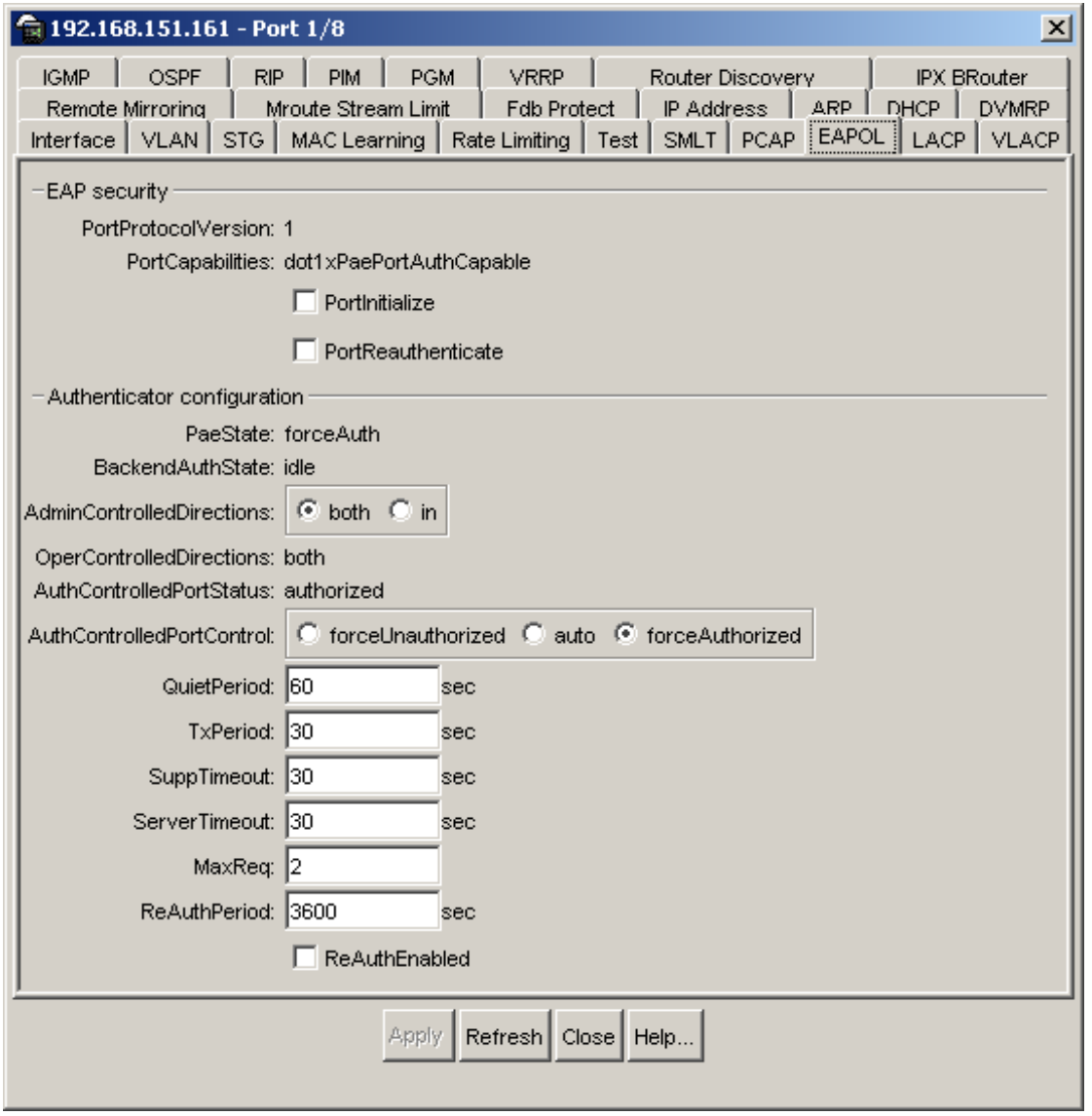


Table 37 describes the EAPOL tab fields.

Table 37 Port dialog box—EAPOL tab fields

Field	Description
portProtocolVersion	The protocol version number of the EAPOL implementation supported by the port.
portCapabilities	The capabilities of the PAE associated with the port. This parameter indicates whether Authenticator functionality, Supplicant functionality, both, or neither, is supported by the Port's PAE.
PortInitialize	When checked, initializes EAPoL authentication on this port. After the port initializes, this field reverts to its default, which is disabled.
PortReauthenticate	When checked, re-authenticates the Supplicant connected to this port immediately. The default is disabled.
PaeState	Displays the current Authenticator PAE state. The possible states are: **initialized** **disconnected** **connecting** **authenticating** **authenticated** **aborting** **held** **forceAuth** **forceUnauth**
BackendAuthState	Displays the current state of Backend Authentication. The possible states are: **request** **response** **success** **fail** **timeout** **idle** **initialize**
AdminControlDirections	Determines whether the port should exert control over communication in both directions (both incoming and outgoing) or only in incoming direction.
operControlledDirections	The current direction of control over communications exerted on the port.
AuthControlledPortStatus	Displays the port's current state: unauthorized, auto, or authorized.
AuthControlledPortControl	Sets the authentication status for this port. The default is ***forceAuthorized***. *forceUnauthorized* - port is always unauthorized. *auto* - port authorization depends on the results of the EAPoL authentication by the RADIUS server. *forceAuthorized* - port is always authorized.
QuietPeriod	Sets the time interval (in seconds) between authentication failure and the start of a new authentication. The allowed range is 1 to 65535, and the default is 60.

Table 37 Port dialog box—EAPOL tab fields (continued)

Field	Description
TxPeriod	Sets the time (in seconds) to wait for a response from a Supplicant for EAP Request/Identity packets. The allowed range is 1 to 65535, and the default is 30.
SuppTimeout	Sets the time (in seconds) to wait for a response from a Supplicant for all EAP packets except EAP Request/Identity packets. The allowed range is 1 to 65535, and the default is 30.
ServerTimeout	Sets the time (in seconds) to wait for a response from the RADIUS server. The allowed range is 1 to 65535, and the default is 30.
MaxReq	Sets the maximum number of times to retry sending packets to the Supplicant. The allowed range is 1 to 10, and the default is 2.
ReAuthPeriod	Sets the time interval (in seconds) between successive re-authentications (see "ReAuthEnabled"). The allowed range is 1 to 2147483647, and the default is 3600 (1 hour).
ReAuthEnabled	When checked, re-authenticates an existing Supplicant at the time interval specified in ReAuthPeriod.

4 In the AuthControlledPortControl field, select one of the following:

- **forceUnauthorized** - sets the port so it is always unauthorized.
- **auto** - sets the port to match the global EAPoL authentication setting.
- **forceAuthorized** - sets the port so it is always authorized (default).

Globally configuring EAPoL on the switch

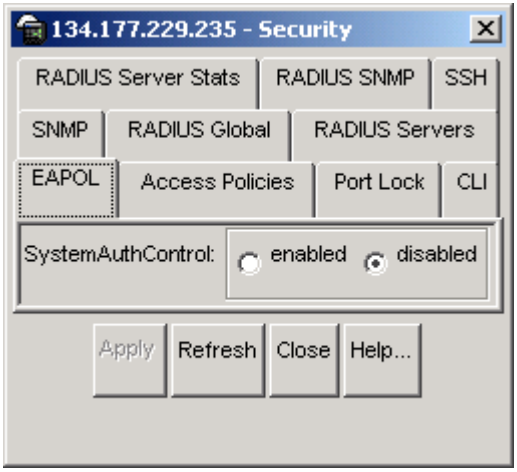
The SystemAuthControl field globally enables or disables EAPoL on the switch. (By default, EAPoL is disabled.) With this one command, you can make all the **controlled** ports on the switch EAPoL-enabled.

To enable EAPoL globally on the switch:

1 From the Device Manager main menu, choose Edit > Security.

The Security dialog box opens with the EAPOL tab displayed. (Figure 90)

Figure 90 Security dialog box—EAPOL tab



2 Click enable.

Configuring EAPoL on a port

To configure EAPoL on one or more ports:

1 Select the port you want to edit.

Note: If you want to select multiple ports, press [Ctrl] + left click the ports you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- Double-click the selected port
- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for a single port opens with the Interface tab displayed. (Figure 88)

3 Click EAPOL.

The EAPOL tab opens. (Figure 89)

Graphing EAPoL statistics

The Passport 8000 Series switch provides the following graphing tools to help you monitor and troubleshoot your switch:

- Graphing EAPoL Authenticator statistics
- Graphing EAPoL diagnostic statistics
- Graphing EAPoL session statistics

Graphing EAPoL Authenticator statistics

To display the Authenticator PAE statistics for each selected port:

1 Select the port or ports you want to graph.

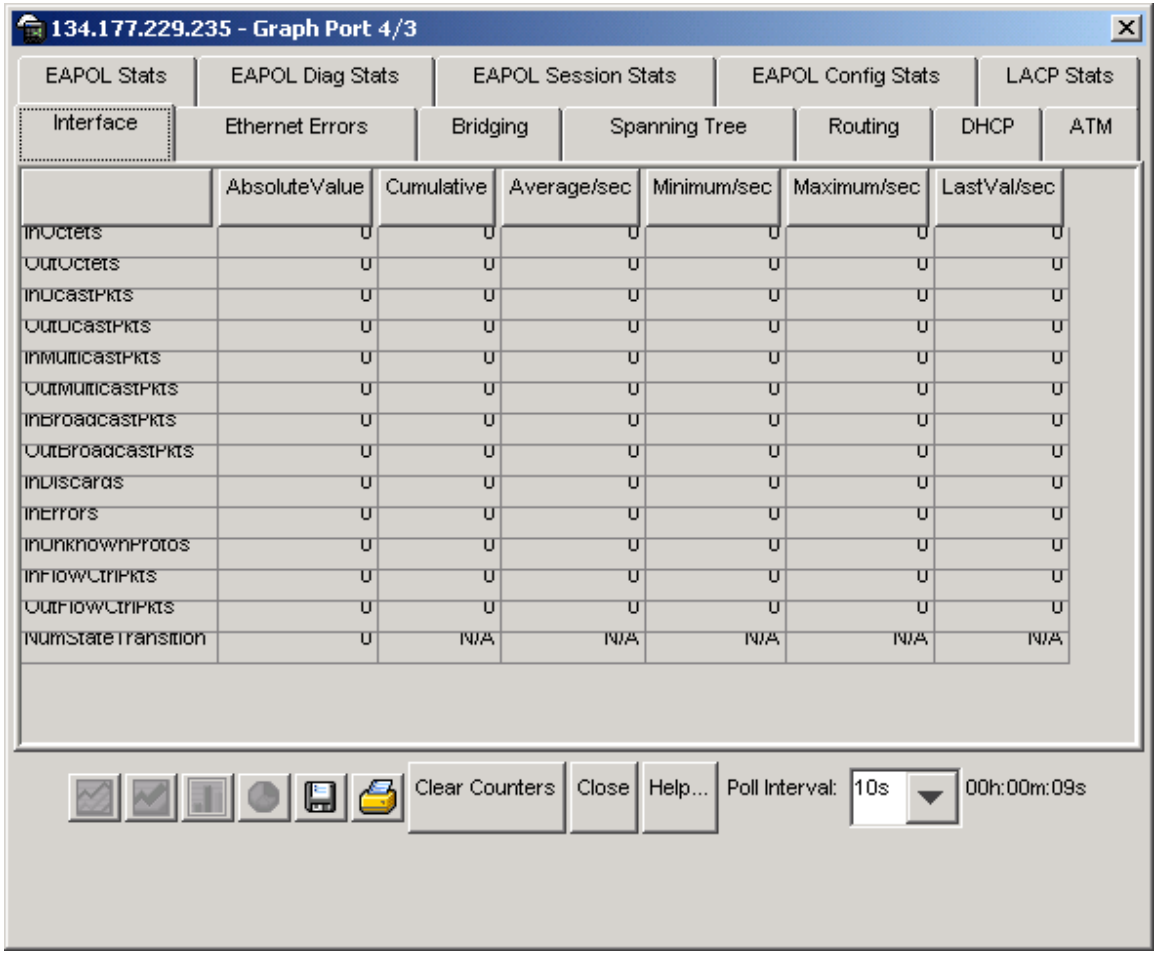
To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed. (Figure 91)

Figure 91 Graph Port dialog box—Interface tab



3 Click EAPOL Stats.

The EAPOL Stats tab for graphing multiple ports opens. (Figure 92)

Figure 92 Graph Port dialog box—EAPOL Stats tab

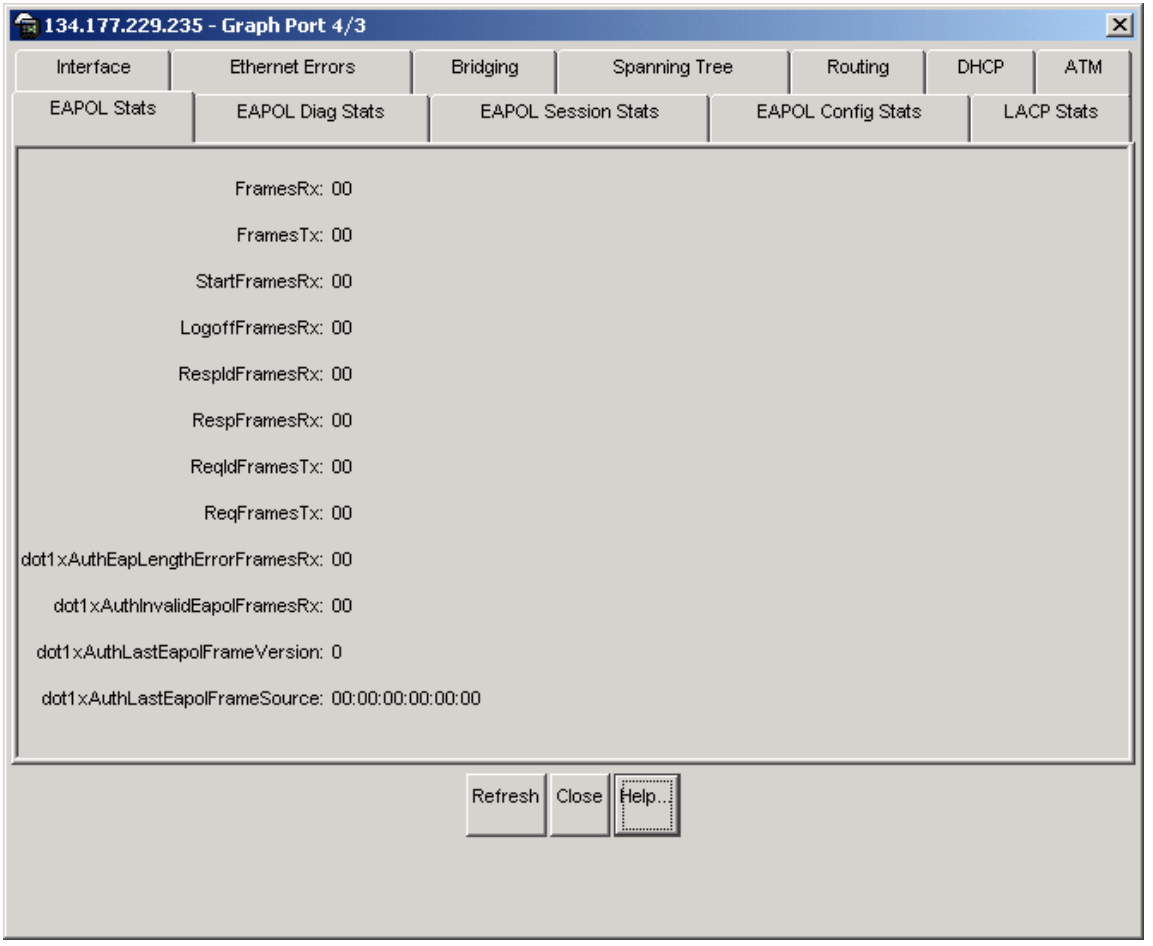


Table 38 describes the EAPOL Stats tab fields.

Table 38 Graph Port dialog box—EAPOL Stats tab fields

Field	Description
FramesRx	Displays the number of valid EAPoL frames of any type that have been received by this Authenticator.
FramesTx	Displays the number of EAPoL frame types of any type that have been transmitted by this Authenticator.

Table 38 Graph Port dialog box—EAPOL Stats tab fields (continued)

Field	Description
StartFramesRx	Displays the number of EAPoL start frames that have been received by this Authenticator.
LogoffFramesRx	Displays the number of EAPoL Logoff frames that have been received by this Authenticator.
RespIdFramesRx	Displays the number of EAPoL Resp/Id frames that have been received by this Authenticator.
RespFramesRx	Displays the number of valid EAP Response frames (Other than Resp/Id frames) that have been received by this Authenticator.
ReqIdFramesTx	Displays the number of EAPoL Req/Id frames that have been transmitted by this Authenticator.
ReqFramesTx	Displays the number of EAP Req/Id frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
AuthEapLengthErrorFramesRx	Displays the number of EAPoL frames that have been received by this Authenticator in which the packet body length field is not valid.
AuthInvalidEapolFramesRx	Displays the number of EAPoL frames that have been received by this Authenticator in which the frame type is not recognized.
AuthLastEapolFrameVersion	Displays the protocol version number that was in the most recently received EAPoL frame.
AuthLastEapolFrameSource	Displays the source MAC address that was in the most recently received EAPoL frame.

Graphing EAPoL diagnostic statistics

To display the Authenticator PAE diagnostic statistics for each selected port:

1. Select the port or ports you want to graph.

   To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2. Do one of the following:

   - From the Device Manager main menu, choose Graph > Port.
   - From the shortcut menu, choose Graph.

- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed. (Figure 91)

3 Click EAPOL DiagStats.

The EAPOL DiagStats tab for graphing multiple ports opens. (Figure 93)

Figure 93 Graph Port dialog box—EAPOL DiagStats tab

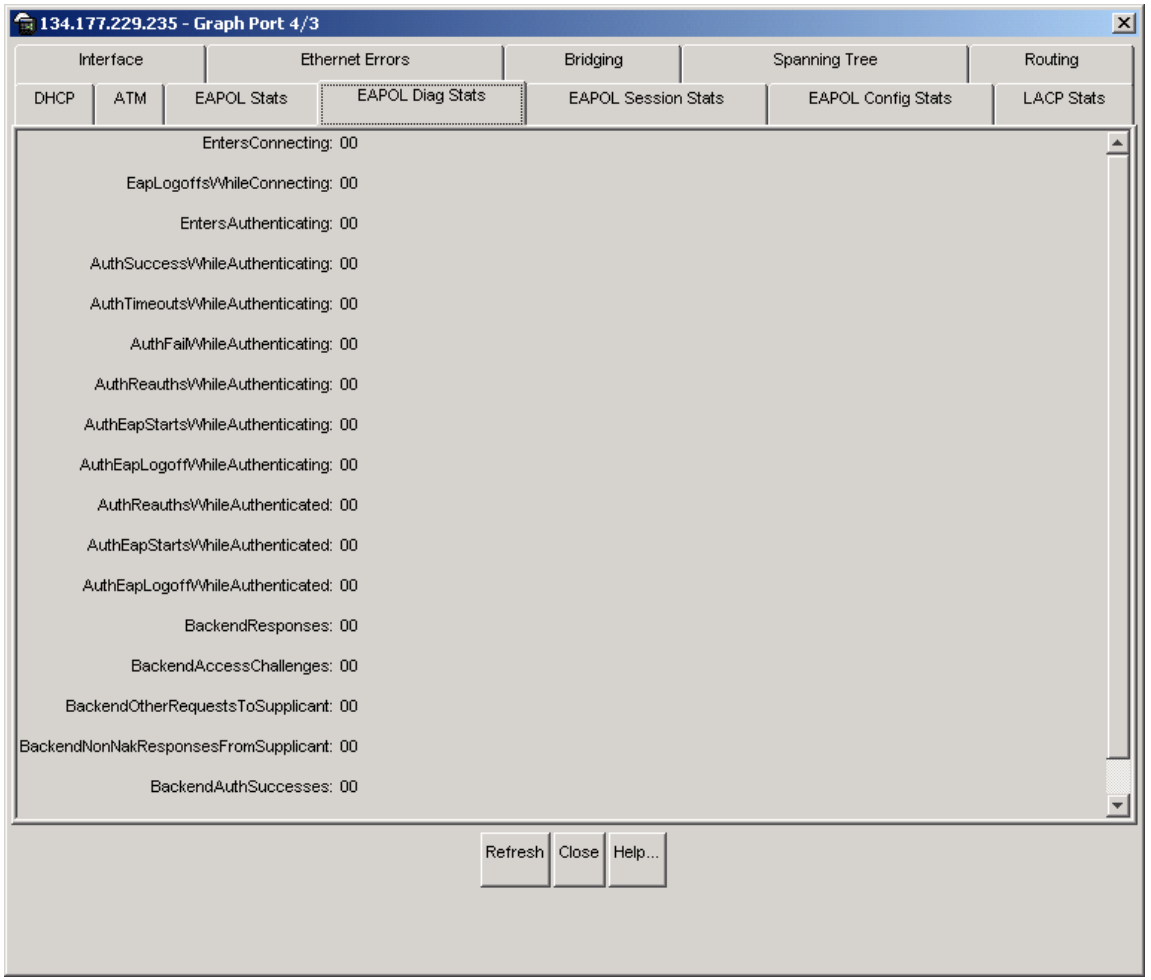


Table 39 describes the EAPOL DiagStats tab fields.

Table 39 Graph Port dialog box—EAPOL DiagStats tab fields

Field	Description
EntersConnecting	Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPoL-Logoff message.
EntersAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/Identity message being received from the Supplicant.
AuthSuccessWhile Authenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the Supplicant.
AuthTimeoutsWhile Authenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout.
AuthFailWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure.
AuthReauthsWhile Authenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPoL-Start message being received from the Supplicant.
AuthEapLogoffWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPoL-Logoff message being received from the Supplicant.
AuthReauthsWhile Authenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of a reauthentication request.

Table 39 Graph Port dialog box—EAPOL DiagStats tab fields (continued)

Field	Description
AuthEapStartsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of an EAPoL-Start message being received from the Supplicant.
AuthEapLogoffWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Disconnected as a result of an EAPoL-Logoff message being received from the Supplicant.
BackendResponses	Counts the number of times that the Backend Authentication state machine sends an Initial-Access request packet to the Authentication server.
BackendAccessChallenges	Counts the number of times that the Backend Authentication state machine receives an Initial-Access challenge packet from the Authentication server.
BackendOtherRequestsToSupplicant	Counts the number of times that the Backend Authentication state machine sends an EAP request packet (other than an Identity, Notification, failure, or success message) to the Supplicant.
BackendNonNakResponsesFromSupplicant	Counts the number of times that the Backend Authentication state machine receives a response from the Supplicant to an initial EAP request and the response is something other than EAP-NAK.
BackendAuthSuccesses	Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server.
BackendAuthFails	Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server.

Graphing EAPoL session statistics

To display the Authenticator PAE statistics for each session that is still in progress and the final values for ports where there is no currently active session:

1. Select the port or ports you want to graph.

   To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed. (Figure 91)

3 Click EAPOL SessionStats.

The EAPOL SessionStats tab for graphing multiple ports opens.

Figure 94 Graph Port dialog box—EAPOL SessionStats tab

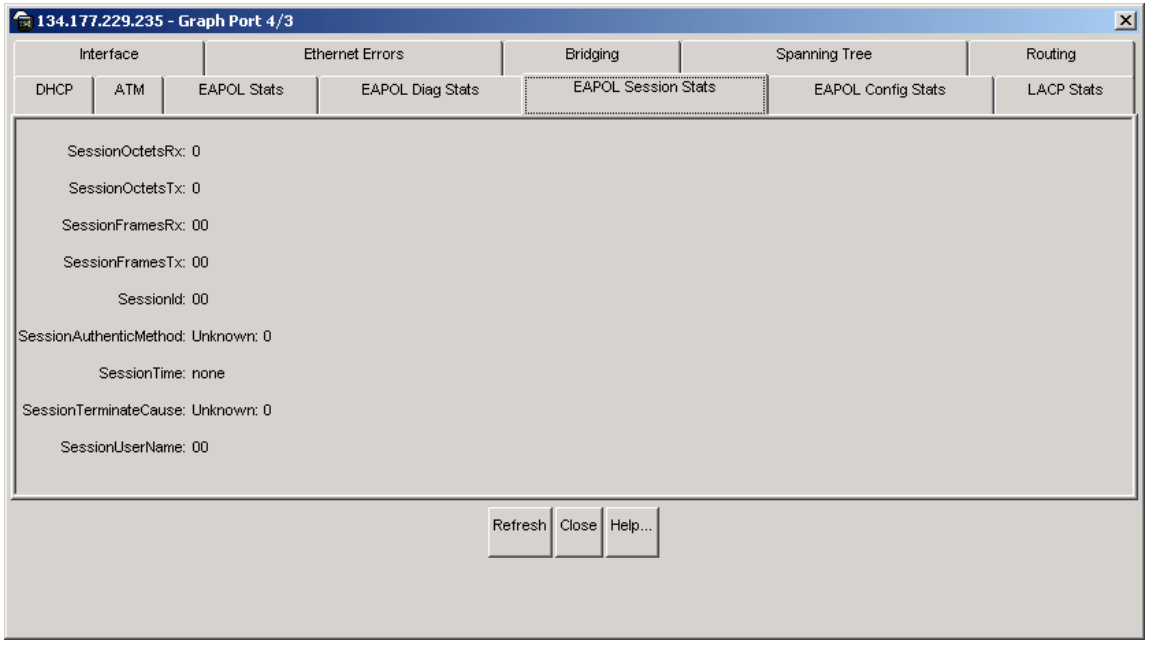


Table 40 describes the EAPOL SessionStats tab fields.

Table 40 Graph Port dialog box—EAPOL SessionStats tab fields

Field	Description
SessionOctetsRx	Displays the number of octets received in user data frames on this port during the session.
SessionOctetsTx	Displays the number of octets transmitted in user data frames on this port during the session.
SessionFramesRx	Displays the number of user data frames received on this port during the session.
SessionFramesTx	Displays the number of user data frames transmitted on this port during the session.
SessionId	Displays a unique identifier for the session that is at least three characters.
SessionAuthenticMethod	Displays the authentication method (remote or local RADIUS server) used to establish the session.
SessionTime	Displays the duration of the session (in seconds).
SessionTerminateCause	Displays the reason for the session being terminated. The possible reasons are: **Supplicant logoff** **Port failure** **Supplicant restart** **Re-authentication failed** **Control force unauthorized** **Port re-initialized** **Port admin disabled** **Not terminated yet**
SessionUserName	Displays the user name of the Supplicant PAE.

Chapter 17
CLI configuration examples

This chapter provides examples of common EAPoL and SNMPv3 configuration tasks, including the CLI commands you use to create the example configurations.

Note: For a complete description of CLI commands you can use to configure specific EAPoL and SNMPv3 tasks, including those shown in this chapter, see the appropriate CLI chapter in this guide.

This chapter includes the following topics:

Configuring EAPoL via L2

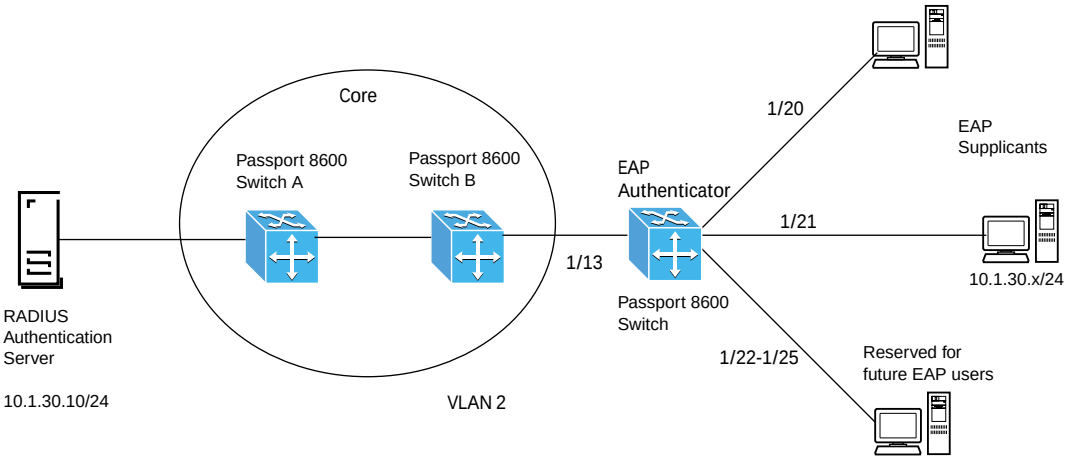
In this configuration example, you use VLAN 2 for the EAPoL Supplicants, ports 1/20-1/25. You use port 1/13 for the trunk port to the Passport 8600 core. Only ports 1/20 and 1/21 are ready for EAPoL users. The other EAPoL Supplicant ports (1/22-1/25) are reserved for future EAPoL use; configure these ports so that they cannot be accessed. Specifically, this configuration example shows how to perform the following tasks:

- Create VLAN 2 for EAPoL with port 1/13 and ports 1/20-1/25
- Use IP address of 10.1.30.2/24 on VLAN 2
- Configure ports 1/20 and 1/21 for EAPoL auto
- Configure ports 1/22-1/25 for EAPoL force-unauthorized

- Configure a RADIUS-server on the Passport 8600 switch that points to the Authentication Server

Figure 95 illustrates this configuration example.

Figure 95 EAPoL via L2



To configure the switch for this example, follow these steps:

1. Create VLAN 2 as a port-based VLAN using STG 1:

   ```
   Passport-8610:5# config vlan 2 create byport 1
   ```

2. If required, enable VLAN tagging on port 1/13:

   ```
   Passport-8610:5# config ethernet 1/13 perform-tagging
   enable
   ```

3. Add VLAN members:

   ```
   Passport-8610:5# config vlan 2 ports add 1/13,1/20-1/25
   ```

4. Remove port members from the default VLAN:

   ```
   Passport-8610:5# config vlan 1 ports remove 1/13,1/20-1/
   25
   ```

5. Add IP address to VLAN 2:

   ```
   Passport-8610:5# config vlan 2 ip create 10.1.30.2/24
   ```

6. Enable EAPoL globally:

```
Passport-8610:5# config sys set eapol enable
```

7 Enable EAPoL on ports 1/20 and 1/21:

```
Passport-8610:5# config ethernet 1/20-1/21 eapol
admin-status auto
```

8 Set ports 1/22-1/25 to EAPoL unauthorized:

```
Passport-8610:5# config ethernet 1/22-1/25 eapol
admin-status force-unauthorized
```

9 Add the RADIUS server configuration:

a Enable RADIUS globally:

```
Passport-8610:5# config radius enable true
```

b Add the RADIUS server, assuming the RADIUS key = eap8600:

```
Passport-8610:5# config radius server create
10.1.30.10 secret eap8600 usedby eap
```

Configuration files

This section shows the configuration commands and parameters used to create the topology shown in Figure 95. You can copy and paste the command outputs shown here to update your configuration files.

```
#
# PORT CONFIGURATION - PHASE I
#

ethernet 1/20 eapol admin-status auto
ethernet 1/21 eapol admin-status auto
ethernet 1/22 eapol admin-status force-unauthorized
ethernet 1/23 eapol admin-status force-unauthorized
ethernet 1/24 eapol admin-status force-unauthorized
ethernet 1/25 eapol admin-status force-unauthorized

#
#
# VLAN CONFIGURATION
#

vlan 1 ports remove 1/13,1/20-1/25 member portmember
vlan 2 create byport 1
vlan 2 ports remove 1/1-1/12,1/14-1/19,1/26-1/48,2/1-2/24,5/1-5/8
member portmember
vlan 2 ports add 1/13,1/20-1/25 member portmember
vlan 2 ip create 10.1.30.2/255.255.255.0

#
#
# RADIUS CONFIGURATION
#

radius server create 10.1.30.10 secret eap8600 usedby eapol
acct-port 1813
radius enable true


#
# GLOBAL EAP CONFIGURATION
#

sys set eapol enable

back
```

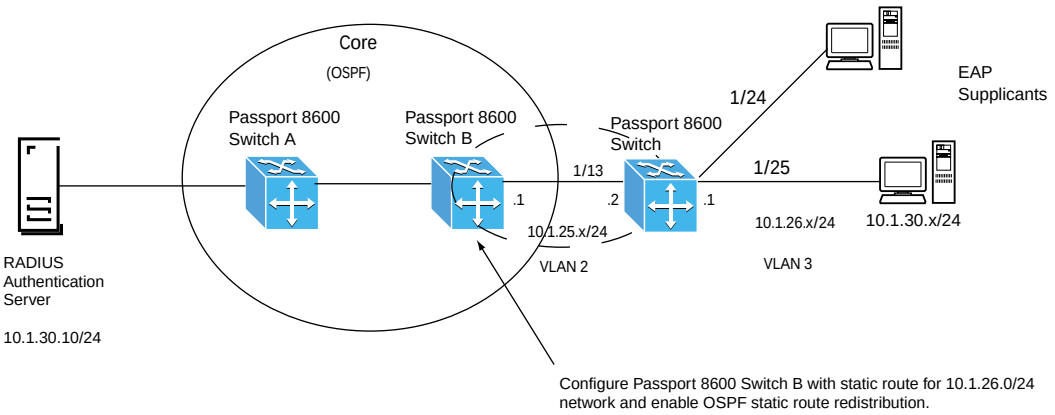
Configuring EAPoL via L3

In this configuration example, the Passport 8600 is connected to a routed core. Specifically, this configuration example shows how to perform the following tasks:

- Create VLAN 2 with port 1/13 and IP address of 10.1.25.2/24 to be used to connect to the core network.
- Create VLAN 3 with ports 1/20 and 1/21 and IP address of 10.1.26.1/24 to be used for the EAPoL Supplicants.
- Add a static default route pointing to 10.1.25.1 on Passport 8600 switch B.
- Configure RADIUS-server pointing to the authentication server.

Figure 96 illustrates this configuration example.

Figure 96 EAPoL via L3



To configure the switch for this example, follow these steps:

1. Remove ports from the default VLAN:

   ```
   Passport-8610:5# config vlan 1 ports remove 1/13,1/24-1/
   25
   ```

2. Create VLAN 2 as a port-based VLAN using STG 1:

   ```
   Passport-8610:5# config vlan 2 create byport 1
   ```

3. If required, enable VLAN tagging on port 1/13:

```
Passport-8610:5# config ethernet 1/13 perform-tagging
enable
```

4. Add VLAN members:

```
Passport-8610:5# config vlan 2 ports add 1/13
```

5. Add IP address to VLAN 2:

```
Passport-8610:5# config vlan 2 ip create 10.1.25.2/24
```

6. Create VLAN 3 as a port-based VLAN using STG 1:

```
Passport-8610:5# config vlan 3 create byport 1
```

7. Add VLAN members:

```
Passport-8610:5# config vlan 3 ports add 1/24-1/25
```

8. Add IP address to VLAN 3:

```
Passport-8610:5# config vlan 3 ip create 10.1.26.1/24
```

9. Add static route:

```
Passport-8610:5# config ip static-route create 0.0.0.0/0
next-hop 10.1.25.1 cost 1
```

10. Enable EAPoL globally:

```
Passport-8610:5# config sys set eapol enable
```

11. Enable EAPoL on ports 1/24 and 1/25:

```
Passport-8610:5# config ethernet 1/24-1/25 eapol
admin-status auto
```

12. Add the RADIUS server configuration:

    a. Enable RADIUS Globally

    ```
    Passport-8610:5# config radius enable true
    ```

    b. Add the RADIUS server, assuming the RADIUS key = eap8600

    ```
    Passport-8610:5# config radius server create
    10.1.30.10 secret eap8600 usedby eap
    ```

Configuration files

This section shows the configuration commands and parameters used to create the topology shown in Figure 96. You can copy and paste the command outputs shown here to update your configuration files.

```
#
# PORT CONFIGURATION - PHASE I
#

ethernet 1/1 eapol reauthentication true
ethernet 1/24 eapol admin-status auto
ethernet 1/25 eapol admin-status auto


#
# VLAN CONFIGURATION
#

vlan 1 ports remove 1/13,1/24-1/25 member portmember
vlan 2 create byport 1
vlan 2 ports remove 1/1-1/12,1/14-1/48,2/1-2/24,5/1-5/8 member
portmember
vlan 2 ports add 1/13 member portmember
vlan 2 ip create 10.1.25.2/255.255.255.0
vlan 3 create byport 1
vlan 3 ports remove 1/1-1/23,1/26-1/48,2/1-2/24,5/1-5/8 member
portmember
vlan 3 ports add 1/24-1/25 member portmember
vlan 3 ip create 10.1.26.1/255.255.255.0


#
ip static-route create 0.0.0.0/0.0.0.0 next-hop 10.1.25.1 cost 1

#
#
# RADIUS CONFIGURATION
#

radius server create 10.1.30.10 secret eap8600 usedby eapol
acct-port 1813
radius enable true


#
# GLOBAL EAP CONFIGURATION
```

```
#

sys set eapol enable

back
```

Configuring SNMPv3

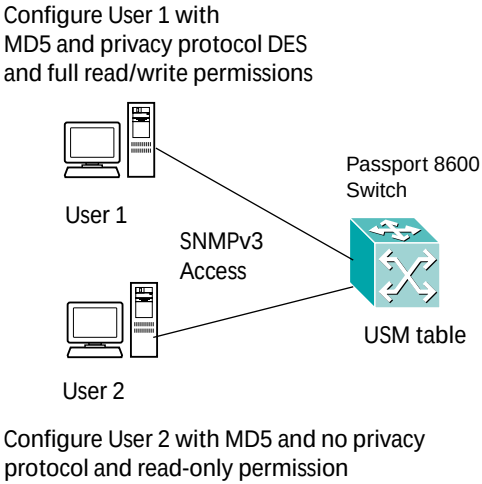
In this configuration example, you add two users to the USM table with different MIB permissions and privacy protocols to the USM table. Specifically, this configuration example shows how to perform the following tasks:

- Add User 1 to the USM table with an authentication protocol of MD5 and a privacy protocol of DES (authPriv).
- Allow User 1 full MIB views with full permission (both read and write), starting from the existing *org* level.
- Add User 2 to the USM table with an authentication protocol of MD5 and no privacy protocol (authNoPriv).
- Allow User 2 full MIB read permission, starting from the existing *org* level, but excluding write permission from all Private Enterprise MIBs.

Note: The *org* level gives users access to both the standard MIB and private tree branches; the *private* level gives users access to only MIB objects below the private branch of the MIB tree.

Figure 97 illustrates this configuration example.

Figure 97 SNMPv3 for users with different permissions/privacy protocols



To configure the switch for this example, follow these steps:

1. Load the DES module:

   After you have installed the DES module on the Passport 8600 switch, enter the following command:

   ```
   Passport-8610:5# config load-module DES /flash/
   p80c3700.des
   ```

2. Add User 1 to the USM table. For this example, specify a user name of *user1*, an MD5 password of *user1234*, and a DES privacy password of *userpriv.*

   ```
   Passport-8610:5# config snmp-v3 usm create user1 md5
   auth user1234 priv userpriv
   ```

3. Add User 1 to the USM group. For this example, add *user1* to a USM group named *group_1*.

   ```
   Passport-8610:5# config snmp-v3 group-member
   create user1 usm group_1
   ```

4. Assign access level to the USM group. For this example, assign an access level of *authPriv* to the USM group *group_1*.

   ```
   Passport-8610:5# config snmp-v3 group-access create
   group_1 "" usm authPriv
   ```

5. Assign read and write view to the USM group. For this example, assign read and write view, starting at *org*, to the USM group *group_1*.

```
Passport-8610:5# config snmp-v3 group-access view group_1
"" usm authPriv read org write org
```

6. Add User 2 to the USM table. For this example, specify a user name of *user2*, and a MD5 password of *user2abcd*.

```
Passport-8610:5# config snmp-v3 usm create user2 md5 auth
user2abcd
```

7. Add User 2 to the USM group. For this example, add User 2 to the group named *group_1* that you created in step 3.

```
Passport-8610:5# config snmp-v3 group-member create user2
usm group_1
```

8. Assign the access level to the USM group. For this example, assign an access level of *authNoPriv* to the USM group *group_1*.

```
Passport-8610:5# config snmp-v3 group-access create
group_1 "" usm authNoPriv
```

9. Create a new MIB view to exclude the private MIB for User 2. For this example, add a new MIB view named *private* to exclude access to the SNMP Private MIB.

```
Passport-8610:5# config snmp-v3 mib-view create private
1.3.6.1.4 type exclude
```

10. Assign read and write view to the USM group. For this example, assign read view only, starting at *org*, and read and write view, starting at *private*, to the USM group *group_1*.

```
Passport-8610:5# config snmp-v3 group-access view group_1
"" usm authNoPriv read org write private
```

Configuration files

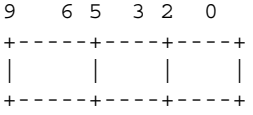
This section shows the configuration commands and parameters used to set up User 1 and User 2 for SNMPv3, as shown in Figure 97. You can copy and paste the command outputs shown here to update your configuration files.

```
#
# SNMP V3 GROUP MEMBERSHIP CONFIGURATION
#

snmp-v3 group-member create user1 usm group_1
snmp-v3 group-member create user2 usm group_1

#
# SNMP V3 GROUP ACCESS CONFIGURATION
#


snmp-v3 group-access create group_1 "" usm authNoPriv
snmp-v3 group-access view group_1 "" usm authNoPriv read "org"
write "private"
snmp-v3 group-access create group_1 "" usm authPriv
snmp-v3 group-access view group_1 "" usm authPriv read "org" write
"org"

#
# SNMP V3 MIB VIEW CONFIGURATION
#

snmp-v3 mib-view create private 1.3.6.1.4  type exclude

#
```

Appendix A
Tap and OctaPID assignment

The switch fabric in the Passport 8600 modules has nine switching taps, one for each of the eight I/O slots (1 to 4 and 7 to 10) and one for the CPU slots (5 and 6). Taps 0-7 map to the eight I/O slots and can support up to eight OctaPIDs. Each OctaPID can support up to eight ports.

In the Passport 8000 Series switch, a physical port number is 10 bits long and has the following format:



bits 9–6: Tap number (0–15)

bits 5–3: OctaPID number (0–7)

bits 2-0: MAC port number (0-7)

The Tap number bits and the OctaPID number bits combined (bits 9–3) are usually referred to as the OctaPID ID.

Table 41 lists the module types that are currently available, along with the associated OctaPID ID assignments for each module.

Table 41 Available module types and OctapPID ID assignments

Module type	Port type	OctaPID ID assignment
8608GBE and 8608GBM Modules	1000BASE-SX (GBIC)	Table 42 next
	1000BASE-LX (GBIC)	
	1000BASE-ZX (GBIC)	
	1000BASE-XD (GBIC)	
	1000BASE-TX (GBIC)	
8608GTE and 8608GTM Modules	1000BASE-T	Table 42 next
8608SXE Module	1000BASE-SX	Table 42 next
8616SXE Module	1000BASE-SX	Table 43 on page 289
8624FXE Module	100BASE-FX	Table 44 on page 290
8632TXE and 8632TXM Modules	10BASE-T/100BASE-TX	Table 45 on page 290
	1000BASE-SX (GBIC)	
	1000BASE-LX (GBIC)	
	1000BASE-ZX (GBIC)	
	1000BASE-XD (GBIC)	
	1000BASE- TX (GBIC)	
8648TXE and 8648TXM Modules	10/100 Mb/s	Table 46 on page 290
8672ATME and 8672ATMM Modules	OC-3c MDA	Table 47 on page 291
	OC-12c MDA	
	DS3	
8681XLR Module	10GBASE-LR	Table 48 on page 291
8681XLW Module	10GBASE-LW	Table 49 on page 292
8683POSM Module	OC-3c MDA	Table 50 on page 292
	OC-12c MDA	

Table 42 describes the OctaPID ID and port assignments for the 8608GBE, Passport 8608GBM, 8608GTE, 8608GTM, and 8608SXE modules.

Table 42 8608GBE/8608GBM/8608GTE/8608GTM, and 8608SXE modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	Port 2
OctaPID ID: 2	Port 3
OctaPID ID: 3	Port 4
OctaPID ID: 4	Port 5
OctaPID ID: 5	Port 6
OctaPID ID: 6	Port 7
OctaPID ID: 7	Port 8

Table 43 describes the OctaPID ID and port assignments for the 8616SXE Module.

Table 43 8616SXE module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 and 2
OctaPID ID: 1	Ports 3 and 4
OctaPID ID: 2	Ports 5 and 6
OctaPID ID: 3	Ports 7 and 8
OctaPID ID: 4	Ports 9 and 10
OctaPID ID: 5	Ports 11 and 12
OctaPID ID: 6	Ports 13 and 14
OctaPID ID: 7	Ports 15 and 16

Table 44 describes the OctaPID ID and port assignments for the 8624FXE Module.

Table 44 8624FXE module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24

Table 45 describes the OctaPID ID and port assignments for the 8632TXE and 8632TXM Modules.

Table 45 8632TXE and 8632TXM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24
-	-
-	-
OctaPID ID: 5	Ports 25 through 32
OctaPID ID: 6	Port 33 (GBIC port)
OctaPID ID: 7	Port 34 (GBIC port)

Table 46 describes the OctaPID ID and port assignments for the 8648TXE and 8648TXM Modules.

Table 46 8648TXE and 8648TXM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24
-	-
-	-

Table 46 8648TXE and 8648TXM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 5	Ports 25 through 32
OctaPID ID: 6	Port 33 through 40
OctaPID ID: 7	Port 41 through 48

Table 47 describes the OctaPID ID and port assignments for the 8672ATME and 8672ATMM Modules.

Table 47 8672ATME and 8672ATMM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	• Ports 1 through 4 (with OC-3c MDA) • Port 1 (with OC-12c MDA) • Ports 1 through 2 (with DS-3 MDA)
OctaPID ID: 1	• Ports 5 through 8 (with OC-3c MDA) • Port 5 (with OC-12c MDA) • Ports 5 through 6 (with DS-3 MDA)
OctaPID ID: 2	Not used

Table 48 describes the OctaPID ID and port assignments for the 8681XLR Module.

Table 48 8681XLR module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	
OctaPID ID: 2	
OctaPID ID: 3	
OctaPID ID: 4	
OctaPID ID: 5	
OctaPID ID: 6	
OctaPID ID: 7	

Table 49 describes the OctaPID ID and port assignments for the 8681XLW Module.

Table 49 8681XLW module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	
OctaPID ID: 2	
OctaPID ID: 3	
OctaPID ID: 4	
OctaPID ID: 5	
OctaPID ID: 6	
OctaPID ID: 7	

Table 50 describes the OctaPID ID and port assignments for the 8683POSM Module.

Table 50 8683POSM module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	• Ports 1 and 2 (with OC-3c MDA) • Port 1 (with OC-12c MDA)
OctaPID ID: 1	• Ports 3 and 4 (with OC-3c MDA) • Port 3 (with OC-12c MDA)
OctaPID ID: 2	• Ports 5 and 6 (with OC-3c MDA) • Port 5 (with OC-12c MDA)

Index

Numerics

A

B

C

D

E

S

T

U

V