Part No. 314724-B Rev 00
May 2003

4655 Great America Parkway
Santa Clara, CA 95054

# Configuring and Managing Security

## Passport 8600 Software Release 3.5

NORTEL NETWORKS™

## Copyright © 2003 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 security features for the 8000 Series switch and what you do to start and customize security services on a Nortel Networks* switch. It provides information about using both the Device Manager graphical user interface (GUI) and 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 graphical user interfaces (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 with the Management Software* for more information).

Make sure that you are running the latest version of Nortel Networks* 8000 Series and Device Manager software. For information about upgrading the 8000 Series and Device Manager, see the upgrading guide for your version of the 8000 Series.

# 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.<br>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.<br>Example: Use the **`dinfo`** command.<br>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.<br>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.<br>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.<br>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.<br>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.<br>Example: `Set Trap Monitor Filters` |
| separator ( > ) | Shows menu paths.<br>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.<br>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 | BaySecure 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 Distribution Unit |
| RADIUS | Remote Access Dial-in User Services |

| | |
|---|---|
| RFC | Request for Comment |
| 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.

**Note:** The 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 one of the following Nortel Networks Technical Solutions Centers:

| Technical Solutions Center | Telephone |
|---|---|
| Europe, Middle East, and Africa | (33) (4) 92-966-968 |
| North America | (800) 4NORTEL or (800) 466-7835 |
| Asia Pacific | (61) (2) 9927-8800 |
| China | (800) 810-5000 |

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

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 Concepts

The security features 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, SSH, SCP, SNMPv3)
- MD5, which protects routing updates (for example, OSPF and BGP)

You protect the data path using:

- MAC address filtering
- 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 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 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 Network Management* |
| IGAP | *Configuring IGMP for User Authentication (IGAP)* |

This chapter includes the following topics:

# CLI passwords

The switch is shipped with default passwords set for access to the CLI through a console or Telnet session. If you have read/write/all access authority, and you are using SNMPv3, you can change passwords that are in encrypted format. If you're using the Device Manager, you can also specify the number of allowed Telnet sessions and rlogin sessions.

**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.

For instructions on changing the CLI passwords, see:

- "Setting security features using Device Manager" on page 55
- "Setting security features using the CLI" on page 99

# 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 configuring the port lock feature, see "Locking a port" on page 58.

## 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 services, such as Telnet, SNMP, HTTP, RSH, and Rlogin. You can enable or disable access services by setting flags, either from the Boot Monitor CLI or from the Run-Time CLI.

You can define network stations that are explicitly allowed to access the switch or 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.

For instructions on configuring access policies using the Device Manager, go to Chapter 3. For instructions on configuring access policies using the CLI, go to Chapter 4.

## SNMP version 3

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.

SNMP version 3 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.SNMP version 3 (SNMPv3) provides a means of security to the SNMP framework by supporting the following:

- Security for Messages

- Access Control, and
- 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 an encryption Protocol for privacy. Only the data portion of a message was encrypted, the header and the security parameters are not. The privacy protocol supported using 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

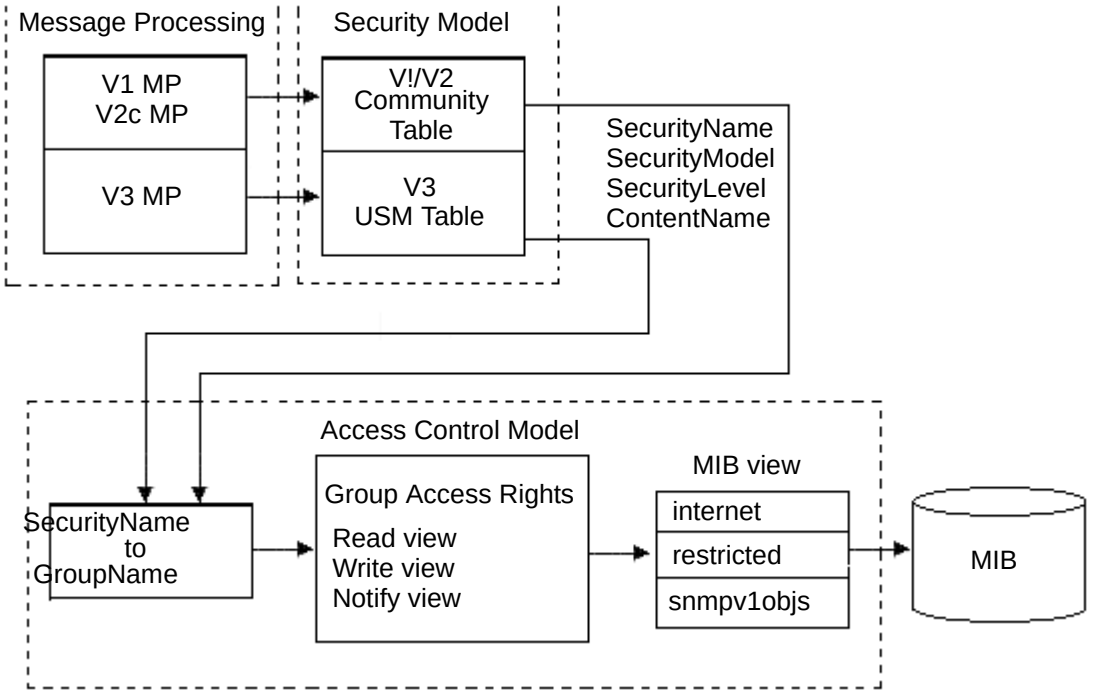
  Communication with authentication and without privacy

- AuthPriv

  Communication with authentication and privacy.0.0

Figure 1 shows the relationship between USM and 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 for SNMPv3, and it 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

## SNMP community strings

For security reasons, the SNMP agent validates each request from an SNMP manager before responding to the request, by verifying that the manager belongs to a valid SNMP community. An *SNMP community* is a logical relationship between an SNMP agent and one or more SNMP managers (the manager software implements the protocols used to exchange data with SNMP agents). You define communities locally at the agent.

The agent establishes one community for each combination of authentication and access control characteristics that you choose. You assign each community a unique name (community string), and all members of a community have the same access privileges, either read-only or read-write:

- *Read-only*: members can view configuration and performance information.
- *Read-write*: members can view configuration and performance information, and also change the configuration.

By defining a community, an agent limits access to its MIB to a selected set of management stations. By using more than one community, the agent can provide different levels of MIB access to different management stations.

SNMP community strings are required for access to the switch using Device Manager or other SNMP-based management software. You set the SNMP community strings using the CLI. For instructions, go to Chapter 4. If you have read/write/all access authority, you can modify the SNMP community strings for access to the device through Device Manager. For instructions, go to Chapter 3.

# Web interface passwords

The 8000 switch includes a Web management interface that lets you monitor your switch through a World Wide Web browser from anywhere on your network. The Web interface provides many of the same monitoring features as the Device Manager software.

The Web management interface is protected by a security mechanism that requires you to log in to the device using a user name and password. The switch is shipped with the default user name and password both specified as ro. You can change these in the CLI using the `config sys set reset-passwd` command. In Device Manager, use the Web tab on the Edit Security dialog box. For instructions, see the publication, *Configuring Network Management*.

**Note:** For security reasons, the Web interface is disabled by default. For instructions how to enable the interface, refer to *Configuring Network Management*.

# Web server password and SNMP community string encryption

In the Passport 8000 Series switch software release 3.5, community strings are stored (as passwords have been since release 3.2.1) in encrypted format and are no longer stored in the configuration file. If a configuration file saved prior to release 3.5 is loaded, any saved passwords from the configuration file will not be recognized. If the switch is booted for the first time with the software release 3.5 image, the password is reset to default values and a log is generated indicating any changes.

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

Web-server passwords and SNMP community strings are encrypted.

- Web-Server password

The web-server passwords authenticate the user who is accessing the switch using the web interface. The passwords are encrypted using the blowfish algorithm and are stored in a hidden file. They are not visible on the switch through any `show` command and are not stored in the config file.

- SNMP community strings

  SNMP community strings are used when the user logs in to the switch over SNMP, for example, using Device manager. These strings are encrypted using the blowfish algorithm and are stored in a hidden file. They are not displayed on the switch and are not stored in the config file.

## Password recovery

You can selectively reset login username/passwords, WSM passwords, SAM passwords web-server passwords, and SNMP community strings. This command has been implemented as a hidden command in CLI and is accessible to you only if you are assigned the “rwa” access level.

## Password encryption

- When the switch boots up, the web-server passwords and community strings are restored from the hidden file.
- When the web-server username/password or SNMP community strings are modified, this information is updated to the hidden file.

## Password recovery

The following CLI commands are used for password recovery. These are hidden commands, and can only be accessed by a user who is assigned “rwa” access.

- `Passport-8603/config/sys/set/reset-passwd# login-user <l1|l2|l3|ro|rw>`

  This command resets the login usernames and passwords selectively. The following access-levels can be reset: l1, l2, l3, ro, rw.

**Note:** The “rwa” community string cannot be reset.

- `Passport-8603/config/sys/set/reset-passwd# wsm-passwd <l4admin|slbadmin|oper|l4oper|slboper>`

  This command resets the wsm usernames/passwords selectively. The following wsm access-levels can be reset: l4admin, slbadmin, oper, l4oper, slboper.

- `Passport-8603/config/sys/set/reset-passwd# sam-passwd <ssladmin>`

  This command resets the ssladmin username/password.

- `Passport-8603/config/sys/set/reset-passwd# web-server-passwd <ro>`

  This command resets the web server username/password for “ro” access.

- `Passport-8603/config/sys/set/reset-passwd# snmp-community-strings <l1|l2|l3|ro|rw>`

  This command resets the following snmp community strings: l1, l2, l3, ro, rw.

**Note:** The “rwa” community string cannot be reset.

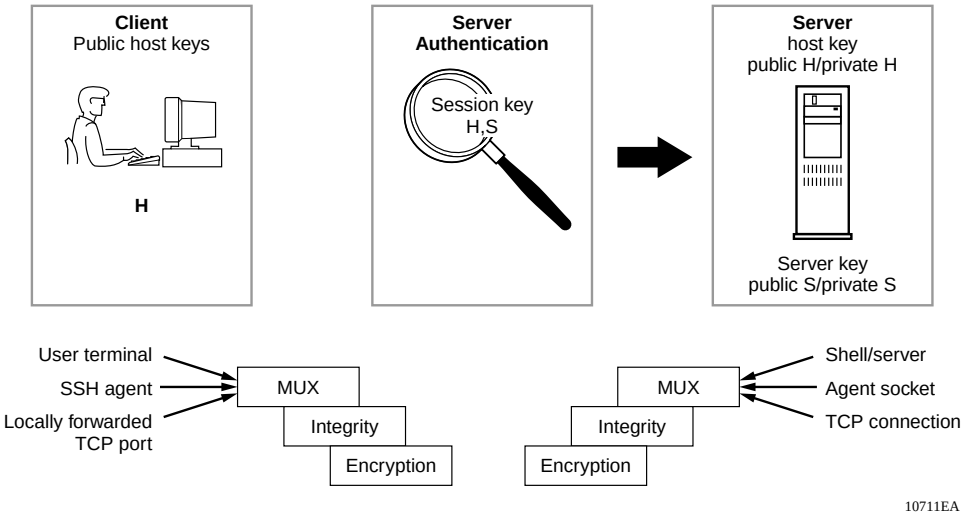
# Secure Shell (SSH)

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 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 8000 Series switch enables the SSH client to make a secure connection to a 8000 Series switch and will work with commercially available SSH clients. See Table 24 on page 84 for a list of supported clients.

**Note:** You must use the CLI to initially configure SSH. You can use Device Manager (DM) to change the SSH configuration parameters. However, Nortel Networks recommends using the 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)

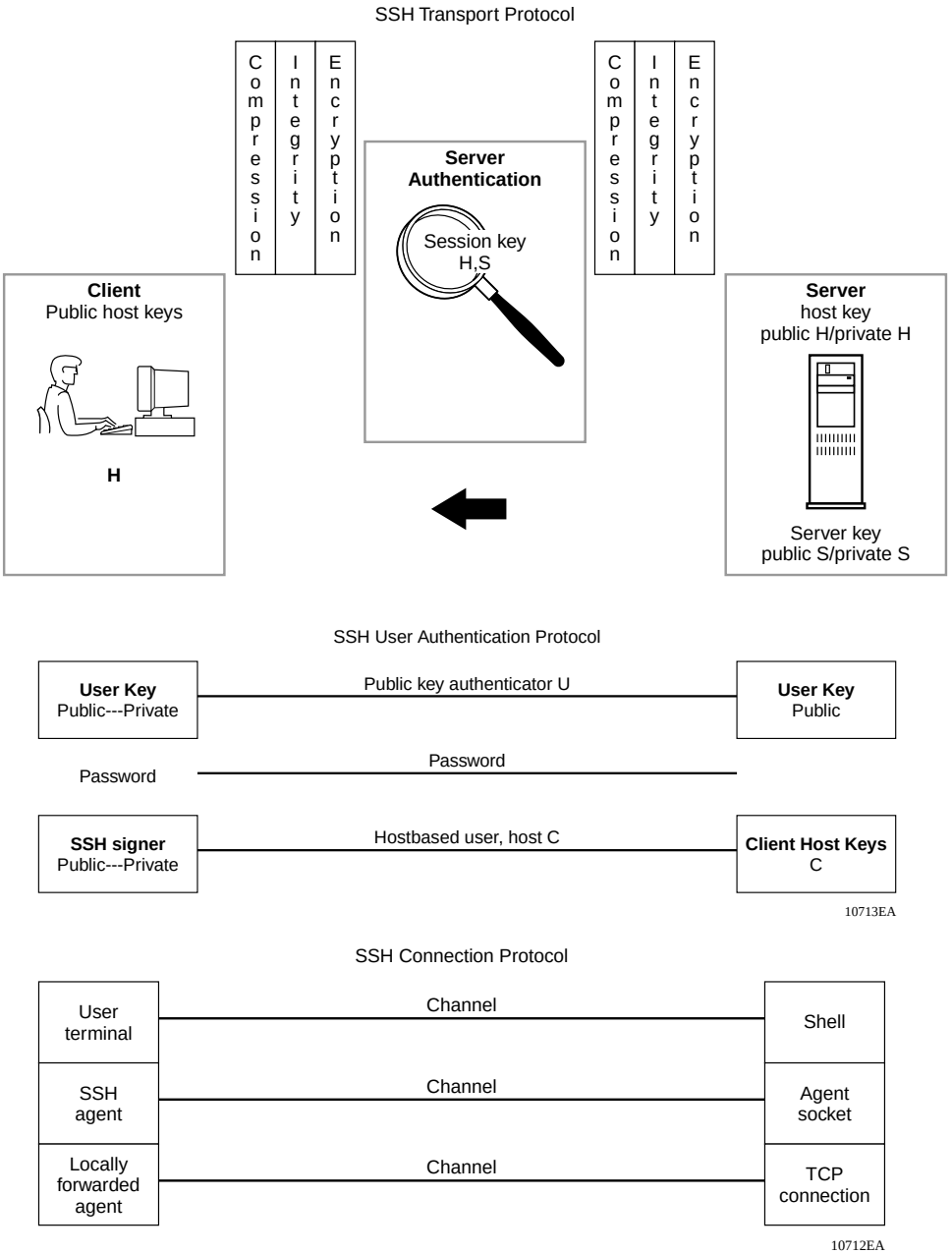
  The SSH authentication protocol runs on top of the SSH transport layer and authenticates the client-side user to the server. SSH-AUTH defines three authentication methods; public key, host-based, and password. SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- 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 the three layers of the SSH-2 protocol.

**Figure 3** Separate SSH version 2 protocols



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 8000 Series switch supports both versions of SSH, Nortel Networks recommends use of the more secure version, the SSH-2 protocol.

# RADIUS

RADIUS (Remote Access Dial-In User Services) 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 8000 Series switch, you use RADIUS authentication and accounting to:

to secure access to the switch (console/Telnet/SSH), and RADIUS accounting to track the management sessions (CLI only).

## 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 and client

For complete information about configuring a RADIUS server, refer to the documentation that came with the server software. For information about setting up the RADIUS server for use with an 8000 Series switch, see “Security Concepts” on page 21.

**Note:** The 8000 Series software supports BaySecure Access Control (BSAC*) and the Merit Network servers. To use these servers, you must first obtain the software for the server you will use. Also, 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 server, see “Configuring a BSAC RADIUS server” on page 50. For detailed information about the changes that must be made for the Merit Network server, see “Configuring a Merit Network server” on page 52.

For information about configuring the RADIUS client, see:

- “Setting security features using Device Manager” on page 55
- “Setting security features using the CLI” on page 99

## 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.<br>**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).<br>— A secret key for each server to authenticate the RADIUS client<br>— The server's UDP port<br>— Maximum retries allowed<br>— 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 Address Server (NAS)<br>• IP address. |
| Accounting is turned off at router | • Accounting off request: NAS IP address. |
| User logs in | • Accounting start request: NAS IP address<br>• Session Id<br>• User Name |
| More than 40 CLI commands are executed | • Accounting Interim request: NAS IP address<br>• Session Id<br>• CLI commands<br>• User Name. |
| User logs off | • Accounting Stop request: NAS IP Address<br>• Session Id<br>• Session duration<br>• User Name<br>• number of input octets for session<br>• number of octets output for session<br>• number of packets input for session<br>• number of packets output for session<br>• 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 timeout 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.

# Using High-Secure mode to prevent denial of service (DOS) attacks

To protect the Passport 8600 against IP packets with an illegal source address of 255.255.255.255 from being routed (per RFC 1812 Section 4.2.2.11 and RFC 971Section 3.2), the Passport 8600 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. Please see Table 2 for the mapping between OctaPIDs and ports.

**Table 2** Available module types and OctaPID ID assignments

| Module type | Port type | OctaPID ID assignment |
|---|---|---|
| 8608GBE and 8608GBM Modules | 1000BASE-SX (GBIC) | Table 3 next |
| | 1000BASE-LX (GBIC) | |
| | 1000BASE-ZX (GBIC) | |
| | 1000BASE-XD (GBIC) | |
| | 1000BASE-TX (GBIC) | |
| 8608GTE and 8608GTM Modules | 1000BASE-T | Table 3 next |
| 8608SXE Module | 1000BASE-SX | Table 3 next |
| 8616SXE Module | 1000BASE-SX | Table 4 on page 43 |
| 8624FXE Module | 100BASE-FX | Table 5 on page 44 |
| 8632TXE and 8632TXM Modules | 10BASE-T/100BASE-TX | Table 6 on page 44 |
| | 1000BASE-SX (GBIC) | |
| | 1000BASE-LX (GBIC) | |
| | 1000BASE-ZX (GBIC) | |
| | 1000BASE-XD (GBIC) | |
| | 1000BASE- TX (GBIC) | |
| 8648TXE and 8648TXM Modules | 10/100 Mb/s | Table 7 on page 45 |
| 8672ATME and 8672ATMM Modules | OC-3c MDA | Table 8 on page 45 |
| | OC-12c MDA | |

**Table 2** Available module types and OctaPID ID assignments (continued)

| Module type | Port type | OctaPID ID assignment |
|---|---|---|
| | DS3 | |
| 8681XLR Module | 10GBASE-LR | Table 9 on page 46 |
| 8681XLW Module | 10GBASE-LW | Table 10 on page 46 |
| 8683POSM Module | OC-3c MDA | Table 11 on page 47 |
| | OC-12c MDA | |

Table 3 describes the OctaPID ID and port assignments for the 8608GBE, Passport 8608GBM, 8608GTE, 8608GTM, and 8608SXE modules.

**Table 3** 8608GBE, 8608GBM, 8608GTE, 8608GTM, and 8608SXE module OctaPID - Port assignments

| 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 4 describes the OctaPID ID and port assignments for the 8616SXE module.

**Table 4** 8616SXE module OctaPID - Port assignments

| 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 |

**Table 4** 8616SXE module OctaPID - Port assignments (continued)

| OctaPID ID assignment | Port assignment |
|---|---|
| OctaPID ID: 6 | Ports 13 and 14 |
| OctaPID ID: 7 | Ports 15 and 16 |

Table 5 describes the OctaPID ID and port assignments for the 8624FXE module.

**Table 5** 8624FXE module OctaPID - Port assignments

| 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 6 describes the OctaPID ID and port assignments for the 8632TXE and 8632TXM module.

**Table 6** 8632TXE and 8632TZM modules OctaPID - Port assignments

| 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 7 describes the OctaPID ID and port assignments for the 8648TXE and 8648TXM module.

**Table 7** 8648TXE and 8648TXM module OctaPID - Port assignments

| 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 through 40 |
| OctaPID ID: 7 | Port 41 through 48 |

Table 8 describes the OctaPID ID and port assignments for the 8672ATME and 8672ATMM module.

**Table 8** 8672ATME and 8672ATMM module OctaPID - Port assignments

| OctaPID ID assignment | Port assignment |
|---|---|
| OctaPID ID: 0 | • Ports 1 through 4 (with OC-3c MDA)<br>• Port 1 (with OC-12c MDA)<br>• Ports 1 through 2 (with DS-3 MDA) |
| OctaPID ID: 1 | • Ports 5 through 8 (with OC-3c MDA)<br>• Port 5 (with OC-12c MDA)<br>• Ports 5 through 6 (with DS-3 MDA) |
| OctaPID ID: 2 | Not used |

Table 9 describes the OctaPID ID and port assignments for the 8681XLR module.

**Table 9** 8681XLR module OctaPID - Port assignments

| 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 10 describes the OctaPID ID and port assignments for the 8681XLW module.

**Table 10** 8681XLW module OctaPID - Port assignments

| 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 11 describes the 8683 POSM module OctaPID ID and port assignments.

**Table 11** 8683POSM module OctaPID - Port assignments

| OctaPID ID assignment | Port assignment |
|---|---|
| OctaPID ID: 0 | • Ports 1 and 2 (with OC-3c MDA)<br>• Port 1 (with OC-12c MDA) |
| OctaPID ID: 1 | • Ports 3 and 4 (with OC-3c MDA)<br>• Port 3 (with OC-12c MDA) |
| OctaPID ID: 2 | • Ports 5 and 6 (with OC-3c MDA)<br>• Port 5 (with OC-12c MDA) |

# Chapter 2
# Configuration Considerations and Guidelines

## Setting up RADIUS servers

Before you can enable RADIUS accounting on the switch, you must create at least one RADIUS server.

The 8000 Series software supports BaySecure Access Control (BSAC*) and the Merit Network servers. To use these servers, you must first obtain the software for the server you will use. Also, 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 server, see "Configuring a BSAC RADIUS server" on page 50. For detailed information about the changes that must be made for the Merit Network server, see "Configuring a Merit Network server" on page 52.

This chapter includes the following topics:

## Single profile enhancement for BSAC RADIUS servers

Single Profile is a feature specific to BSAC RADIUS servers. In a BSAC RADIUS server, when you create a client profile, you can specify all the returnable attributes. When you use the same profile for different products (8000 Series and Baystack 450, for example) you specify all the returnable attributes in the single profile. The 8000 Series switch formerly rejected a user if there were non-8000 Series vendor-specific attributes in the server authentication response. This feature removes the limitation.

## Configuring a BSAC RADIUS server

You must make the following configuration changes for the BSAC server:

**1** Add the following lines in vendor.ini:

```
vendor-product = Nortel Passport 8000
dictionary = pprt8000
ignore-ports = no
port-number-usage = per-port-type
help-id = 0
```

**2** Add the following lines in files radius.dct and pprt8000.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]
```

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

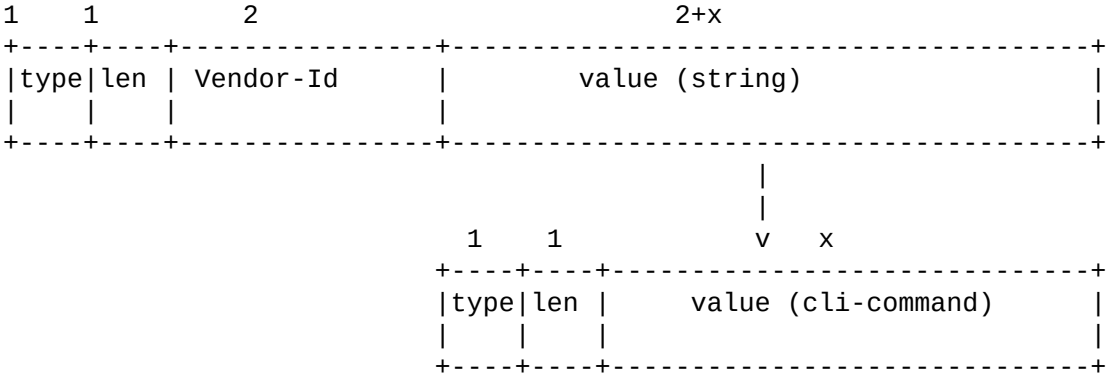
```
Cli-Command=
```

**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=
```

## 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:



## Configuring 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
```

## RADIUS on management ports

With software release 3.5, the management port supports RADIUS protocol. When RADIUS packets are sent out of the management port, the SRC-IP address is properly entered in the RADIUS header. Use the variable, `udpsrc-by-vip flag,` to hold and synchronize the status of the UDP SRC by virtual IP flag. For more information, see "RADIUS/SNMP header network address modifications" on page 150.

Refer to your RADIUS documentation for a list of supported RADIUS servers.

# SSH considerations

The following sections describe the operating limitations for SSH.

## 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`) 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.

## SSHv1 clients

If there are SSHv1 clients (both Unix and PC) connected to the switch and SSH is disabled, the following error messages displays before the logout message:

```
SwitchC:5# [09/24/02 13:41:16] ERROR Task=sshdSession Write
failed: S_iosLib_INVALID_FILE_DESCRIPTOR
```

## 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.

# SNMP cloned user considerations

If the user from which you are cloning has authentication, you can choose for the new user to either have the same authentication protocol as the user from which it was cloned, or no authentication. If you choose authentication for the new user, you must provide a password for that user. Please note that if you want a new user to have authentication, you must indicate that at the time you create it. You can assign a privacy protocol only to a user that has authentication.

If the user from which you are cloning does not have authentication, then the new user will not have authentication.

# Chapter 3
# Setting security features using Device Manager

This chapter includes the following topics that describe how to set up the security features.



## Controlling access to the CLI

### Changing passwords when upgrading to Passport 8000 3.3

In the Passport 8000 Series switch software release 3.5, community strings are stored (as passwords have been since release 3.2.1) in encrypted format and are no longer stored in the configuration file. If a configuration file saved prior to release 3.5 is loaded, any saved passwords from the configuration file are not recognized. If the switch is booted for the first time with the software release 3.5 image, the password is reset to default values and a log is generated indicating any changes.

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

For more information on SNMP community string encryption, see “Web server password and SNMP community string encryption” on page 30.

## Changing passwords

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 SNMPv3 only. If you do not have read/write/all privileges, the user name and password fields will be blank.

**Note:** You no longer have to reboot the switch for your telnet ID settings to take effect.

The CLI tab allows you to specify the number of allowed Telnet sessions and rlogin sessions. To prohibit Telnet or rlogin access to the switch, specify zero (0) as the number of allowed sessions.

To change passwords for access to the CLI:

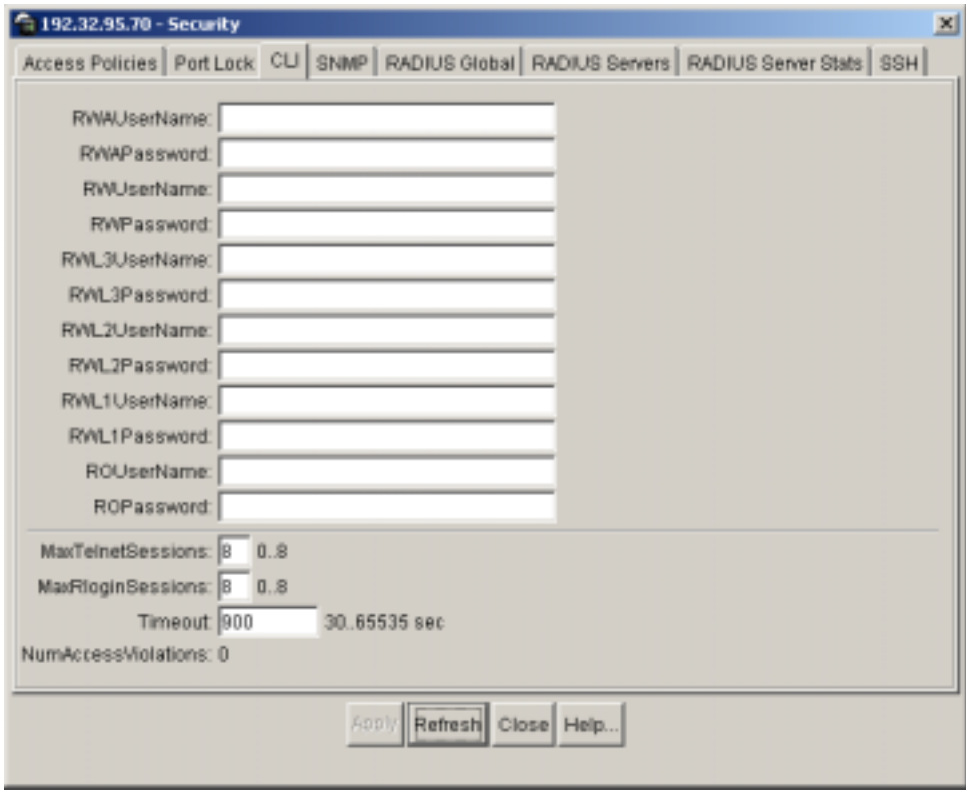
1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the Access Policies tab displayed.

2. Click the CLI tab.

   The CLI tab opens (Figure 4).

**Figure 4** Security dialog box—CLI tab




**Note:** When you access the switch with DM using the public,private community string, the fields in the Security dialog box appear blank. To see what UserName is configured, you must log onto the switch using the secret,secret community string.

Table 12 describes the Security CLI tab fields.

**Table 12** 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. |

**Table 12** Security CLI tab fields (continued)

| Field | Description |
|---|---|
| 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 none to 8). |
| MaxRloginSessions | Indicates the maximum number of concurrent Rlogin sessions that are allowed (from none to 8). |
| Timeout | Indicates the number of seconds of inactivity for a Telnet or Rlogin session before automatic timeout 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 to the Access Policies tab.

2 Click the Port Lock tab.

The Port Lock tab opens (Figure 5).

**Figure 5** Security dialog box—Port Lock tab

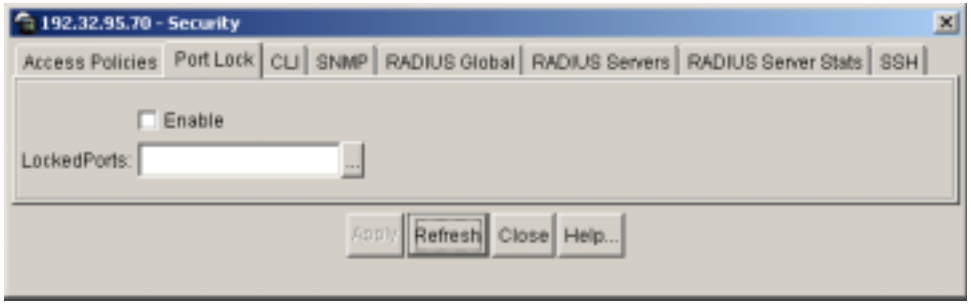



Table 13 describes the Security Port Lock tab fields.

**Table 13** 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. |

# Controlling access to a switch

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, rsh, and rlogin.

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.

To create a new access policy:

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

   The Security dialog box opens with the Access Policies tab active (Figure 6).

**Figure 6** Security dialog box—Access Policies tab


2. In the Security dialog box, click Insert.

   The Security, Insert Access Policies dialog box (Figure 7) opens. Refer to Table 14 for field descriptions. All fields are optional except ID.

3. Make sure PolicyEnable is checked.
4. Select the mode to allow or deny a service.
5. Select a service.
6. Set a precedence number for the service (lower numbers mean higher precedence).
7. Enter an IP address in the NetAddr field.
8. Enter the NetMask used for the NetAddr field.
9. Enter an IP address for the trusted host.
10. Enter a user name for the trusted host.

**11** Select AccessStrict, if desired.

**Note:** When you select this option, you specify that a user must have an access level identical to the one you selected in the dialog box to be able to use this service.

**12** Select the access level for the service.

**13** Click Insert.

**Figure 7** Security, Insert Access Policies dialog box

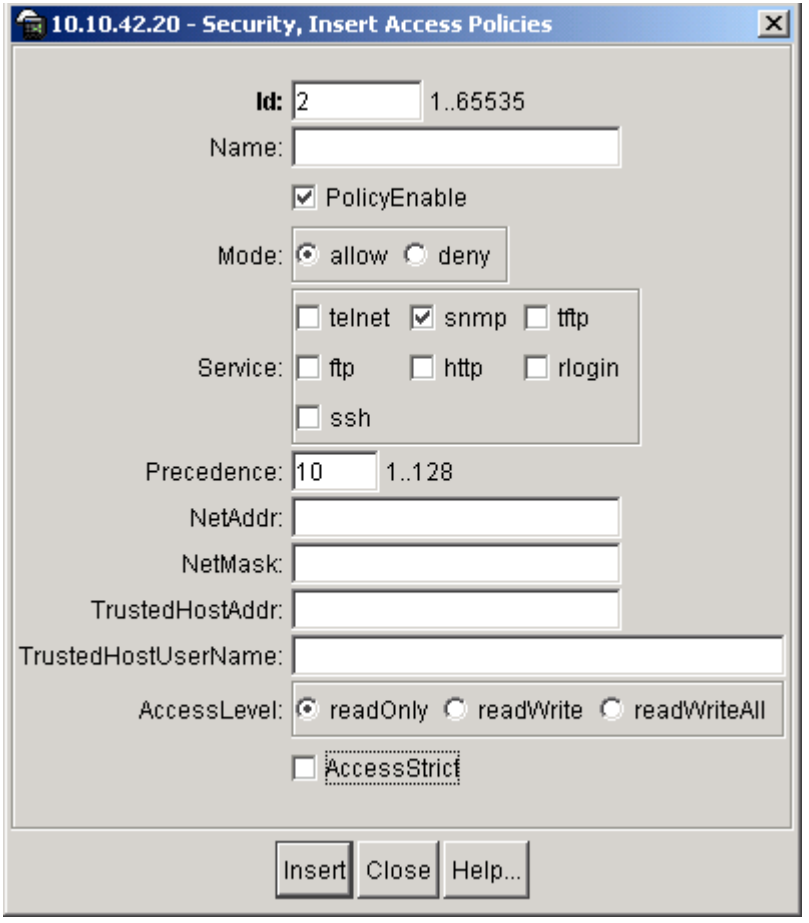



Table 14 describes the items on the Access Policies tab and the Security, Insert Access Policies fields.

**Table 14** 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.<br>**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).<br>**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). |
| Usage | Counts the number of times that an access service uses the access policy. This is a read-only field. |
| AccessStrict | If unchecked, a user must have an access level identical to the one you selected in the dialog box to be able to use this service.<br>If unchecked, a user with an access level of rw specified in the policy table for a policy id is allowed rw and rw access, and ro is denied access. |

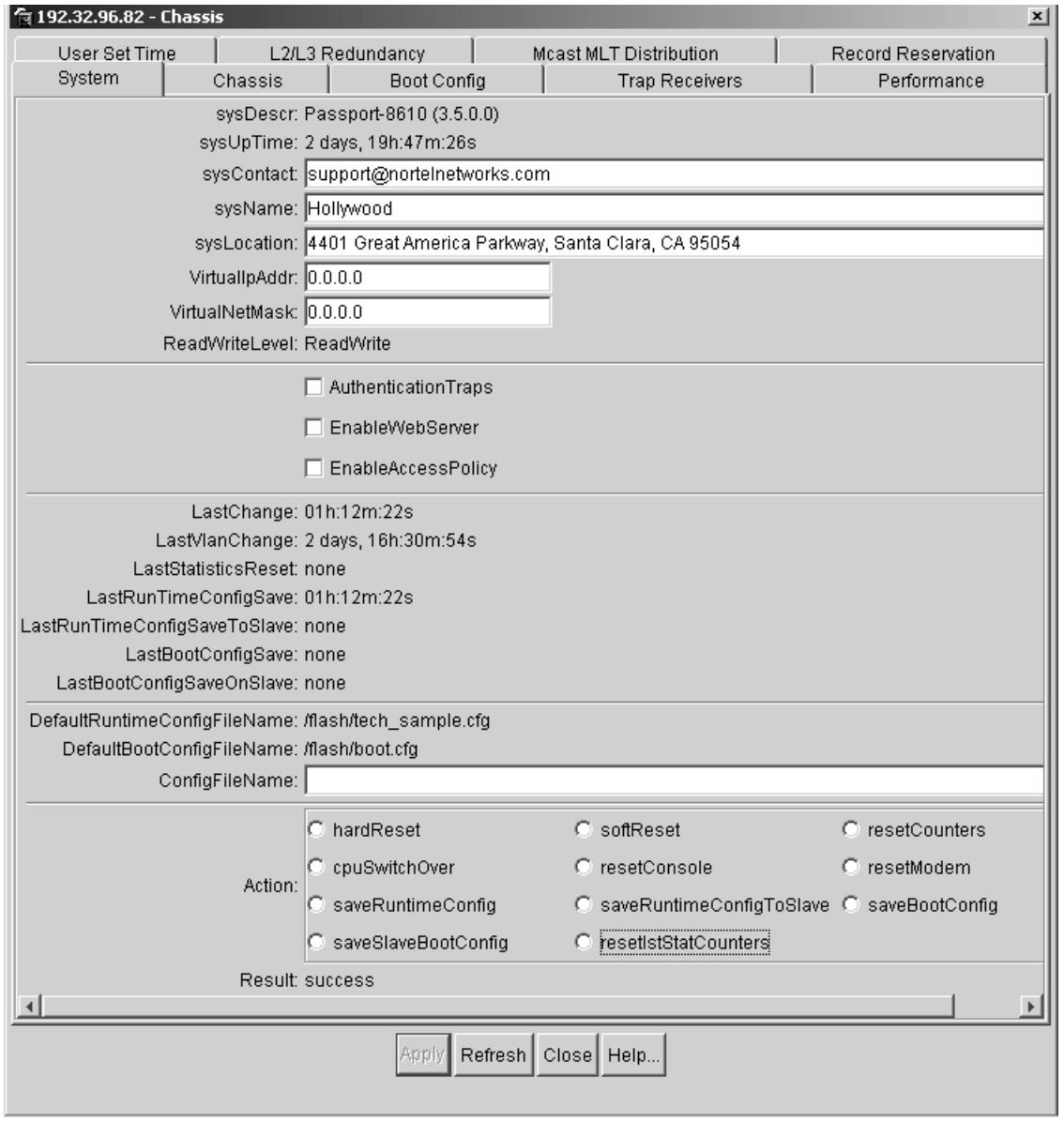
## Enabling rlogin or rsh access

To enable 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 8).

**Figure 8** Chassis dialog box—System tab




2 Check EnableAccessPolicy.

3 Click Apply.

4 Click Close.

# Configuring SNMPv3

This section describes how to use Device Manager to configure the following SNMPv3 options:



## Default login

When using Device Manager, there are default parameters in effect that you must use to initially log in when the SNMPv3 check box is enabled. For instructions on enabling the SNMPv3 check box, see *Configuring Network Management and Diagnostics*. These default parameters are also listed in the USM Table.

- V3 enable checkbox is selected
- Login name: initialmd5
- Authentication Protocol: MD5
- Authentication password: initial
- Privacy Protocol: None
- Privacy Password: None

**Note:** To log on using SNMPv3, you must configure SNMPv3. See "Creating a user security model" on page 67.

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.

The following sections describe how to set up your SNMP configuration:



## Loading the encryption module

Before you access the switch using SNMPv3 with DES encryption, you must load the encryption module, p80c3300.des, which allows you to use the Privacy protocol.

1. Open a browser and enter the following URL:

   `www.nortelnetworks.com/support/downloads`

2. Log in and search for the following:

   Passport 8000 Routing Switch

3. Double-click on the Passport 3des hyper link.
4. Answer the questions on the questionnaire.

   A download dialog box appears.

5. Enter a file location in which to copy the p80c3300.des encryption module.
6. Click OK.
7. 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.

## Logging on using SNMPv3

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

## Creating a user security model

**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 9).

**Figure 9** USM dialog box


Table 15 describes the USM tab fields.

**Table 15** USM dialog box fields

| Field | Description |
|---|---|
| EngineID | Indicates the SNMP engine's administratively-unique Identifier |
| Name | Indicates 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. |

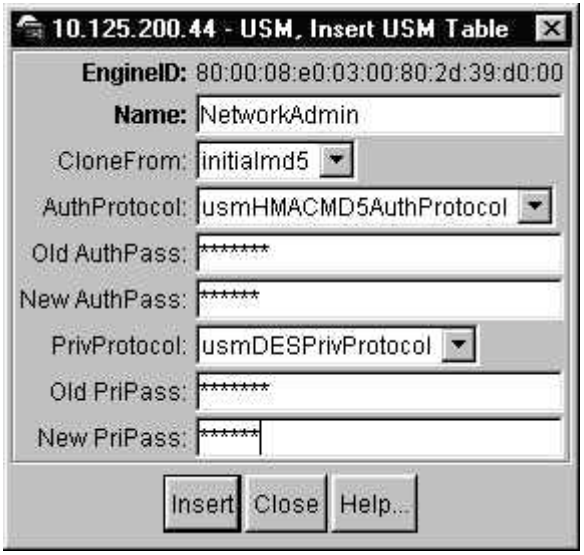
**Table 15** USM dialog box fields (continued)

| Field | Description |
|---|---|
| AuthProtocol | Identifies the Authentication protocol used |
| PrivProtocol | Identifies the privacy protocol used |

**2** Click Insert.

The USM, Insert USM Table dialog box opens (Figure 10).

**Figure 10** USM, Insert USM Table dialog box




**3** Enter a name.

**4** In the CloneFrom field, select a security name from which the new entry copies authentication data and private data.

**5** Select an authentication protocol.

**6** Enter the old authentication password.

**7** Enter a new authentication password for this user model

**8** Select a privacy protocol.

**9** Enter the old privacy password.

**10** Enter a new a privacy password for this user model

**11** 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 16 describes the USM, Insert USM Table dialog box fields.

**Table 16** USM, Insert USM Table dialog box fields

| Field | Description |
|---|---|
| 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. |
| CloneFrom | Specifies the security name from which the new entry must copy privacy and authentication parameters. The range is 1 to 32 characters. |
| AuthProtocol (Optional) | Assigns an authentication protocol (or no authentication) from a pulldown menu. If you select this, you must enter and old AuthPass and a new AuthPass. |
| Old AuthPass | Specifies the current authentication password |
| New AuthPass | Specifies the name of the new authentication password |
| PrivProtocol (Optional) | Assigns a privacy protocol (or no privacy) from a pulldown menu. If you select this, you must enter and old PrivPass and a new PrivPass. |
| Old PriPass | Specifies the current privacy password |
| New PriPass | Specifies the name of the new 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 with the Group Membership tab options visible opens (Figure 11).

**Figure 11** VACM dialog box

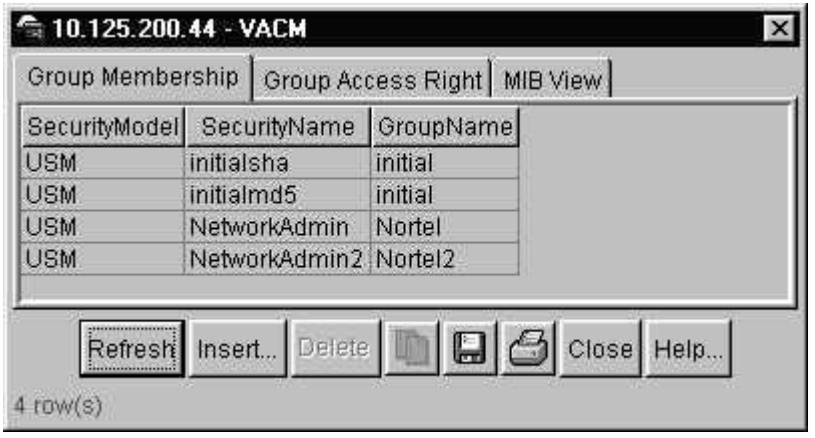



Table 17 describes the VACM tab fields.

**Table 17** 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 12).

**Figure 12** VACM, Insert Group Membership dialog box


3 Select a SecurityModel.

4 Enter a SecurityName.

5 Enter a GroupName.

6 Click Insert.

The VACM dialog opens. The new group membership is shown in the list.

Table 18 describes the Insert Group Membership tab fields.

**Table 18** VACM dialog box—Insert Group Membership tab fields

| Field | Description |
|---|---|
| SecurityModel | The authentication checking to communicate to the switch. |
| 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:

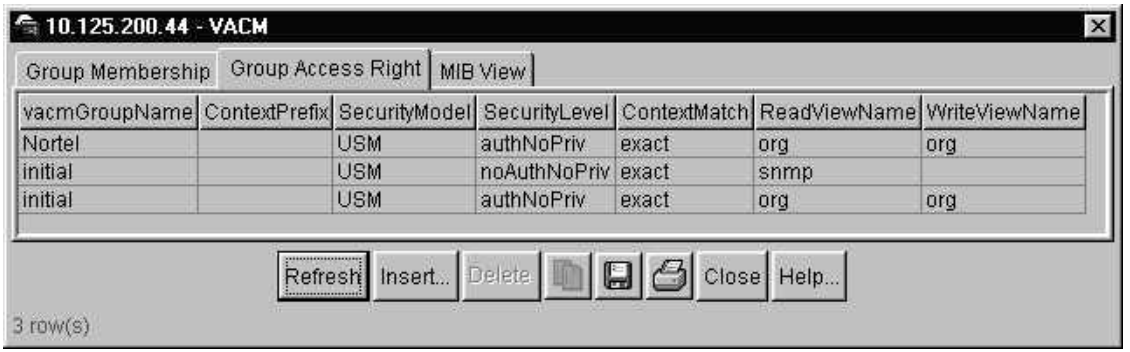
1 From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

The VACM dialog box opens (Figure 11).

2 Click the Group Access Right tab.

The Group Access Right tab displays (Figure 13).

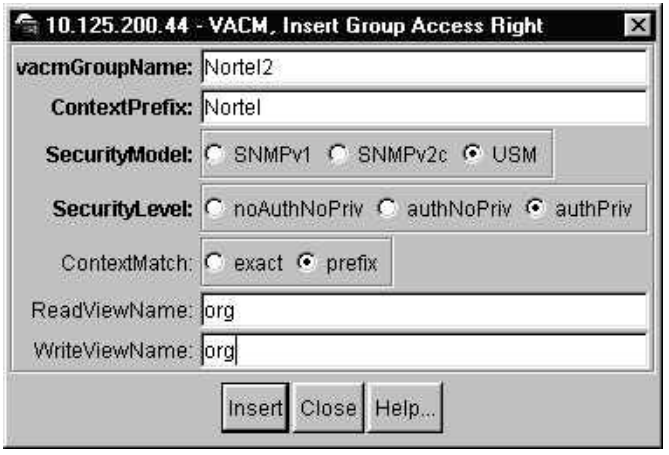
**Figure 13** Group Access tab




**3** Click Insert.

The VACM, Insert Group Access Right dialog box opens (Figure 14).

**Figure 14** VACM, Insert Group Access Right dialog box




**4** Enter a vacmGroupName.

**5** Enter a ContextPrefix.

**6** Select a SecurtyModel.

**7** Select a SecurityLevel.

**8** If desired, select a ContextMatch.

**9** In the ReadViewName field, enter the number of object instances authorized for the group when reading objects.

**10** In the WriteViewName field, enter the number of object instances authorized for the group when writing objects.

**11** Click Insert.

The VACM dialog opens. The new group access is shown in the list.

Table 19 describes the Group Access tab fields.

**Table 19** VACM dialog box—Group Access Right tab fields

| Field | Description |
|---|---|
| vacmGroupName | 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 contextName must match exactly or partially the value of the instance of this object. The range is an SnmpAdminString, 1 to 32 characters. |
| SecurityModel | The authentication checking to communicate to the switch. |
| SecurityLevel | The minimum level of security required to gain the access rights allowed. The security levels are:<br>• noAuthNoPriv<br>• authNoPriv<br>• authpriv |
| ContextMatch<br>(Optional) | There are two types of match:<br>• Exact –Specifies that all rows where the context Name exactly matches the context prefix are selected.<br>• Prefix – Specifies that all rows where the contextName whose starting octets exactly match the context prefix are selected. |
| ReadViewName | The number of object instances authorized for the group when reading objects. |
| WriteViewName | The number of object instances authorized for the group when writing objects. |

## Assigning MIB view access for an object

To assign MIB view access for an object:

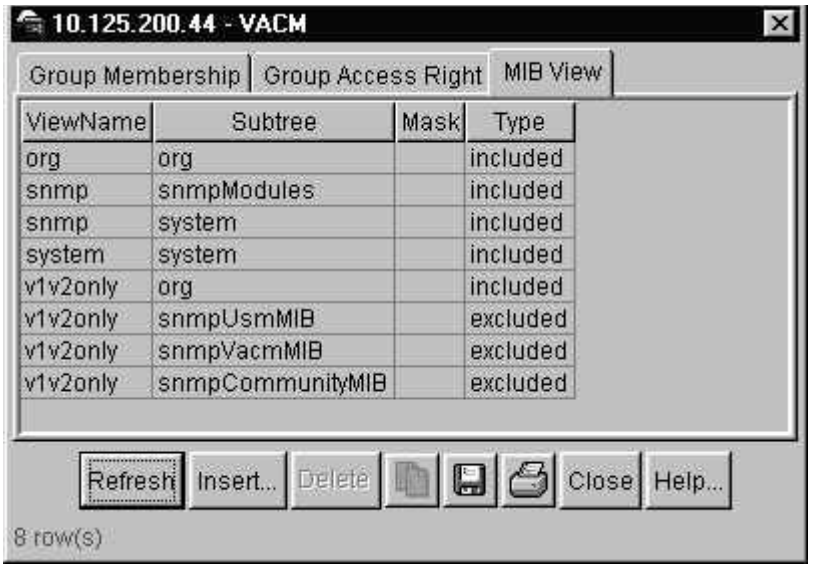
1. From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

   The VACM dialog box opens (Figure 11).

2. Select the MIB View tab.

   The MIB View tab opens (Figure 15).

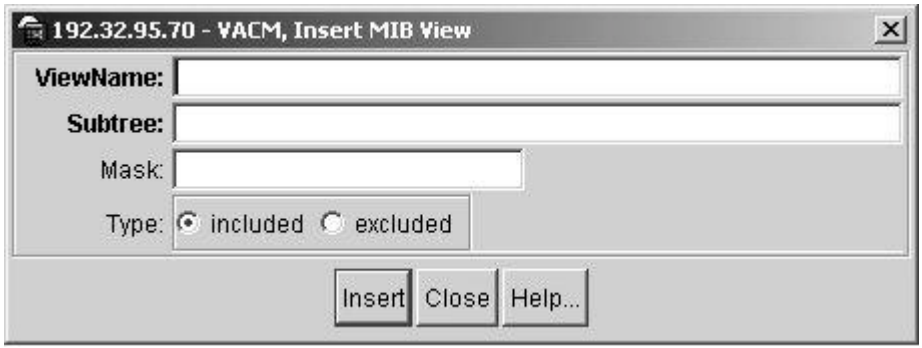
**Figure 15** MIB View tab




3. Click Insert.

   The VACM, Insert MIB View dialog box opens (Figure 16).

**Figure 16** VACM, Insert MIB View dialog box




4 Enter a ViewName.

5 Enter a Subtree.

6 Enter a Mask.

7 Select a Type.

8 Click Insert.

The VACM dialog opens. The assigned MIB view appears in the list.

Table 20 describes the MIB View tab fields.

**Table 20** VACM dialog box—MIB View tab fields

| Field | Description |
|---|---|
| ViewName | Creates a new entry with this group 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<br>(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 17).

**Figure 17** Community Table dialog box


2 Click Insert.

The Community Table, Insert Community Table dialog box opens (Figure 18).

**Figure 18** Community Table, Insert Community Table dialog box


3 Enter an Index.

4 Enter name that is a community string.

5 Enter a SecurityName.

6 Click Insert.

The Community Table dialog opens. The new community is shown in the list.

Table 21 describes the Community Table dialog box fields.

**Table 21** 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. |

# Modifying the SNMP community strings

If you have read/write/all access authority, you can modify the SNMP community strings for access to the device through Device Manager.

To change SNMP community strings:

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

The Security dialog box opens with the Access Policies tab displayed.

2 Click the SNMP tab.

The SNMP tab opens (Figure 19).

**Figure 19** Security dialog box—SNMP tab

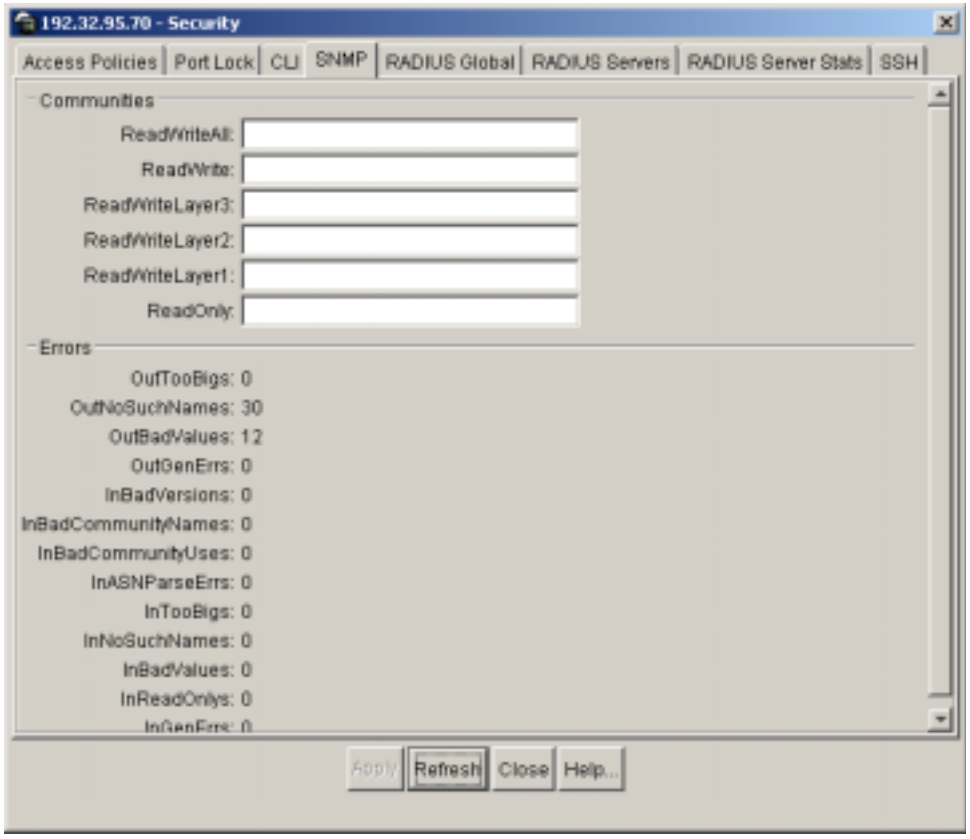



Table 22 describes the SNMP tab fields.

**Table 22** SNMP tab fields

| Field | Description |
|---|---|
| ReadWriteAll | When an SNMP message is received, the community string in the message is compared with this string first. If it matches, read/write access is granted to all items in the MIB. If it does not match, the read/write string is compared next. |
| ReadWrite<br>ReadWriteLayer3<br>ReadWriteLayer2<br>ReadWriteLayer1 | When an SNMP message is received, the community string in the message is compared with these strings second, third, and fourth, respectively. If it matches, read/write access is granted to the appropriate items in the MIB except community strings. (Community strings appear empty when read and return a noSuchName error when an attempt is made to write them.) If it does not match, the ReadOnly string is compared next. |
| ReadOnly | When an SNMP message is received by this entity, the community string in the message is compared with this string fifth. If it matches, read-only access is granted to all items in the MIB except community strings. (Community strings appear empty when read.) If it does not match, no access is granted, no response is sent back to the SNMP requester, and SNMP traps are sent to the SNMP trap receivers if configured. |
| 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.” |
| OutGenErrors | 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. |
| InBadCommunity Names | The total number of SNMP messages delivered to the SNMP protocol entity that used an SNMP community name not known to said entity. |
| InBadCommunity Users | 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. |

**Table 22** SNMP tab fields (continued)

| Field | Description |
|---|---|
| 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.” |
| 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. |
| InGenErrors | 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.” |

# Changing Secure Shell (SSH) configuration parameters

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

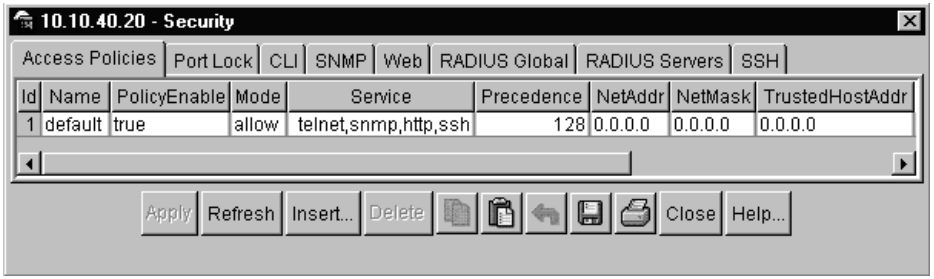
— The user Access Level is set to read/write/all community strings.
— The SNMP protocol is enabled.

To change SSH parameters:

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

The Security dialog box opens with the Access Policies tab displayed (Figure 20).

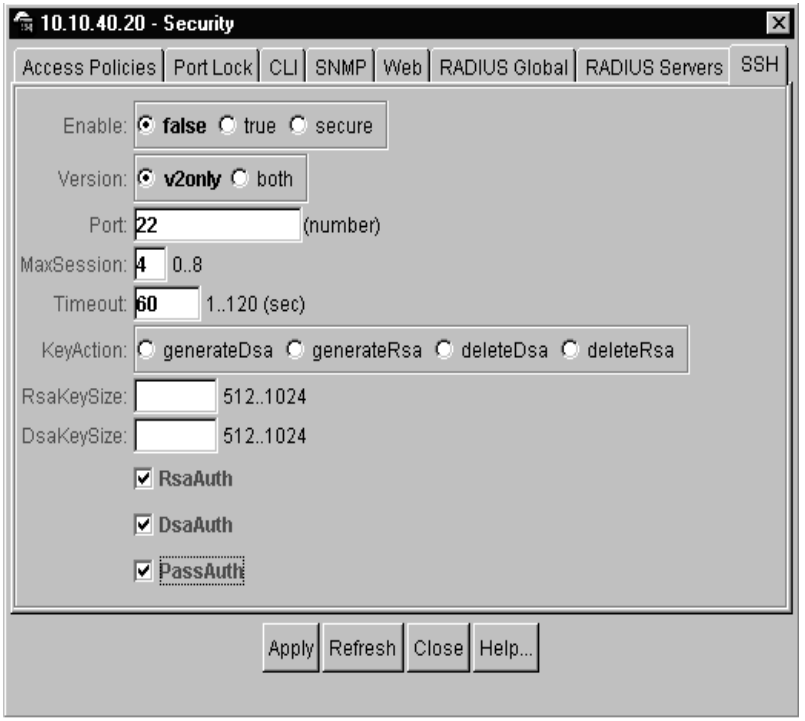
**Figure 20** Security dialog box—Access Policies tab




2 Click SSH.

The SSH tab is displayed (Figure 21).

**Figure 21** 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.<br>The value can be from 0 to 8. Default is 4. |

**Table 23** Security dialog box—SSH tab fields (continued)

| Field | Description |
|---|---|
| Connect 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<br>Windows 2000 | • Supports SSH-1 client only.<br>• Authentication:<br>- RSA<br>- Password<br>• Does not include a keygen tool.<br>• A separate key generation tool such as PuTTYgen must be used to generate an RSA key in SSHv1 format.<br>• **Note:** The 8600 does not generate a log message when a RSA key is manually generated. | • Client distribution does not include SCP client.<br>• Tested on the 8600 with the following applications:<br>- Pageant (authentication agent holding private keys in memory)<br>- PSCP (secure copy client) |
| Secure Shell Client<br>Window 2000 | • Supports SSH-2 client.<br>• Authentication:<br>- DSA<br>- Password<br>• Provides a keygen tool.<br>• It creates a DSA key in SSHv2 format.<br>• **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<br>Unix Solaris 2.5 / 2.6 | • Supports SSH-1 and SSH-2 clients.<br>• Authentication:<br>- RSA<br>- DSA<br>- Password<br>• Provides a keygen tool.<br>• 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 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 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 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* |

**Table 25** DSA authentication access level and file name (continued)

| Client key format or WSM | Access Level | File name |
|---|---|---|
| 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 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 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 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* |

# Configuring RADIUS authentication and accounting

## Overview

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 client information, user information, password, 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 8000 series switch, you use RADIUS authentication to secure access to the switch (console/Telnet/SSH), and RADIUS accounting to track the management sessions (CLI only).

RADIUS authentication allows the remote server to authenticate logins. RADIUS accounting logs all of the activity of each remote user in a session on the centralized RADIUS accounting server.

For more information on RADIUS authentication or RADIUS accounting in your network, see Chapter 1.

This section discusses the following topics:

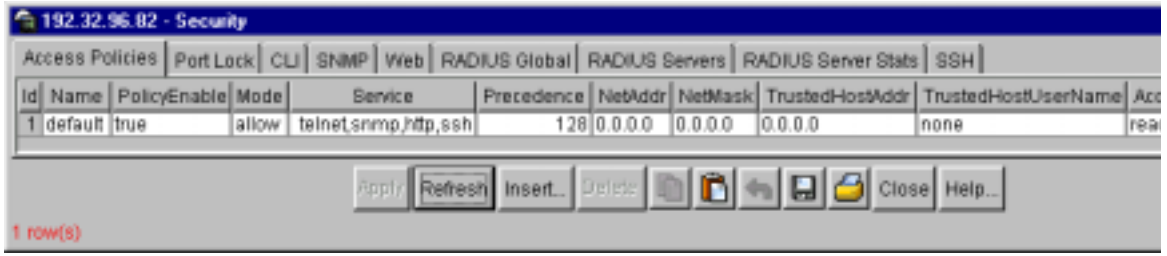
## Enabling RADIUS authentication

To enable RADIUS authentication globally:

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

The Security dialog box opens with the Access Policies tab displayed (Figure 22).

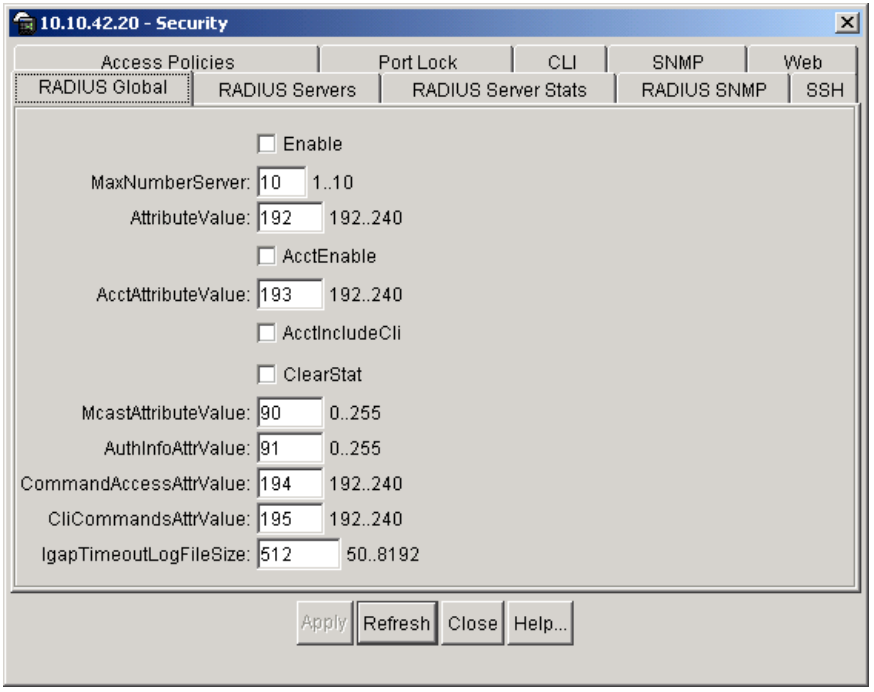
**Figure 22** Security dialog box—Access Policies tab




2 Click the RADIUS Global tab.

The RADIUS Global tab opens (Figure 23).

**Figure 23** 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 AttributeValue field (by default, this value is 192).

6 Click Apply.

Table 27 describes the RADIUS Global tab fields.

**Table 27** 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. |

**Table 27** Security dialog box—RADIUS Global tab fields (continued)

| Fields | Description |
|---|---|
| AttributeValue | 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 8000 Series switches. |
| AcctEnable | Enables RADIUS accounting. |
| AcctAttributeValue | 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. |
| McastAttribute Value | Specifies the value of the Mcast attribute. The valid values are 0 through 255. The default value is 90. |
| AuthInfoAttrValue | Specifies the value of the authentication information attribute. The valid values are 0 through 255. The default value is 91. |
| CommandAccessAttrValue | Specifies the value of the command access attribute. The valid values are 192 through 240. The default value is 194. |
| CliCommandAttrValue | Specifies the value of the CLI command attribute. The valid values are 192 through 240. The default value is 195. |
| IgapTimeoutLogFileSize | Specifies the size of the IGAP timeout log file. The valid values are 50 through 8192. The default value is 512. |

## 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 Access Policies tab displayed (Figure 22).

2 Click the RADIUS Global tab (Table 27).

The RADIUS Global tab opens (Figure 23).

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:

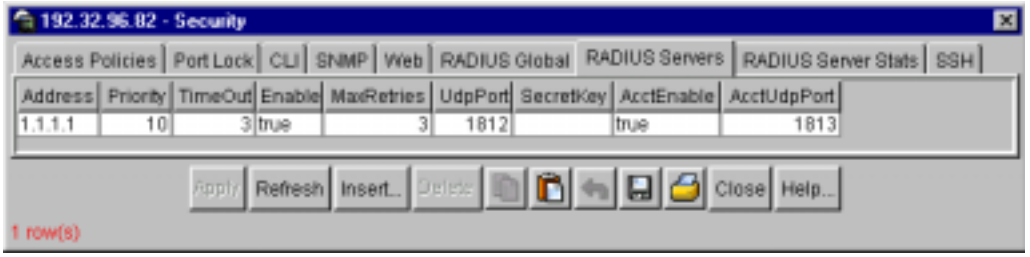
1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the Access Policies tab displayed (Figure 22).

2. Click the RADIUS Servers tab.

   The RADIUS Servers tab opens (Figure 24).

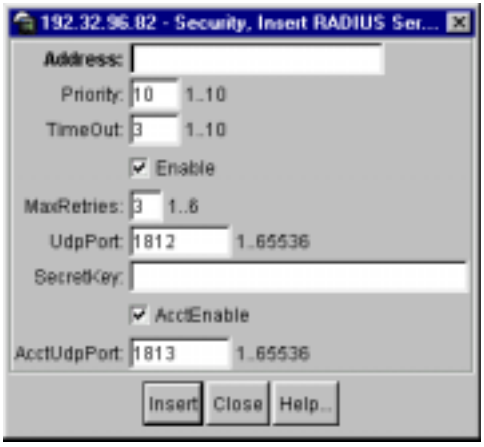
**Figure 24** Security dialog box—RADIUS Servers tab




3. Click Insert.

   The Security, Insert RADIUS Servers dialog box opens (Figure 25).

**Figure 25** RADIUS Servers tab—Insert RADIUS Servers dialog box




4 Enter the IP address of the RADIUS server that you want to add in the Address field.

5 Enter a secret key.

6 Click Insert.

The information for the configured RADIUS server appears in the RADIUS Servers tab of the Security dialog box (Figure 24).

Table 28 describes the Security, Insert RADIUS Servers tab fields.

**Table 28** Security dialog box—RADIUS Servers tab fields

| Fields | Description |
|---|---|
| Address | The IP address of the RADIUS server. |
| 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. |

**Table 28** Security dialog box—RADIUS Servers tab fields (continued)

| Fields | Description |
|---|---|
| UdpPort | Specifies the UDP port that the client uses to send requests to the server (1 to 65536). The default value is 1812.<br>**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.<br>**Note:** The UDP port value set for the client must match the UDP value set for the RADIUS server. |

## Reauthenticating the RADIUS SNMP server session

To reautheticate the RADIUS SNMP server session:

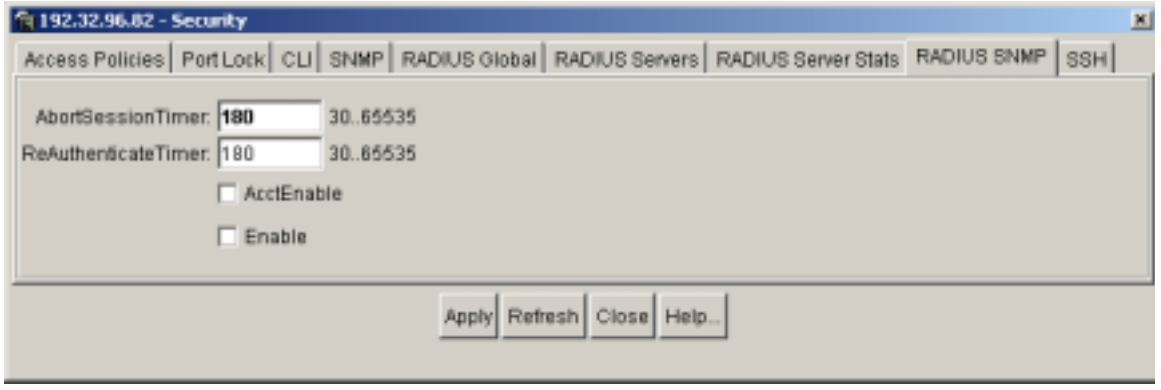
1 From the Device Manager menu bar, choose Edit > Security.

The Security dialog box opens with the Access Policies tab displayed.

2 Click the RADIUS SNMP tab.

The RADIUS SNMP tab opens (Figure 26).

**Figure 26** 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 sAbortSessionTimer, and then click Enable.

5 To enable accounting and record the number of packets/octets received during the SNMP session, click AcctEnable.

Table 29 describes the Security, RADIUS SNMP tab fields.

**Table 29** 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 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.

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 Access Policies tab displayed (Figure 22).

2 Click the RADIUS Servers Stats tab.

The RADIUS Servers Stats tab opens (Figure 27).

**Figure 27** Security dialog box—RADIUS Servers Stats tab

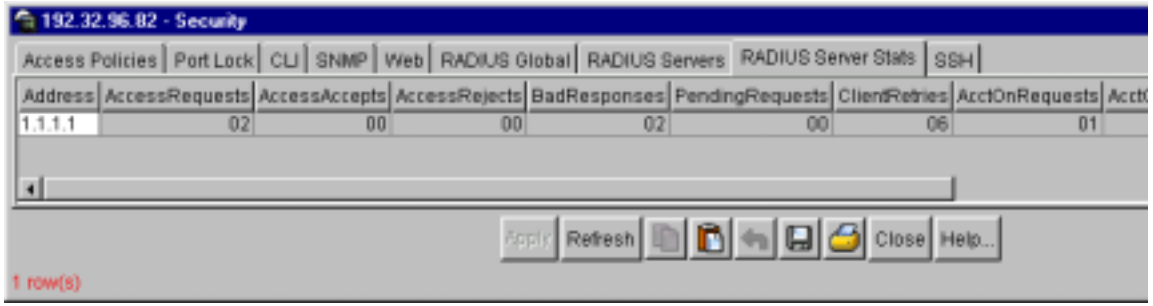



Table 30 describes the RADIUS Servers Stats tab fields.

**Table 30** Security dialog box—RADIUS Server Stats tab fields

| Item | Description |
|---|---|
| Address | The IP address of the RADIUS server. |
| AccessRequests | Number of access-response packets sent to the server; does not include retransmissions. |
| AccessAccepts | Number of access-accept packets, valid or invalid, received from the server. |
| AccessRejects | Number of access-reject packets, valid or invalid, received from the server. |
| BadResponses | Number of invalid access-response packets received from the server. |
| PendingRequests | Access-request packets sent to the server that have not yet received a response, or have timed out. |
| ClientRetries | Number of authentication retransmissions to the server. |
| AcctOnRequests | Number of accounting On requests sent to the server. |
| AcctOffRequests | Number of accounting Off requests sent to the server. |

**Table 30** Security dialog box—RADIUS Server Stats tab fields (continued)

| Item | Description |
|---|---|
| AcctStartRequests | Number of accounting Start requests sent to the server. |
| AcctStopRequests | Number of accounting Stop requests sent to the server. |
| AcctInterimRequests | Number of Accounting Interim requests sent to the server.<br>**Note:** The AcctInterimRequests counter will increment only if you select AcctIncludeCli from the RADIUS Global tab (Figure 23 on page 89). |
| AcctBadResponses | Number of Invalid Responses from the server that are discarded. |
| AcctPendingRequests | Number of requests waiting to be sent to the server. |
| AcctClientRetries | Number of retries made to this server. |

**Note:** To clear server statistics, select ClearStat from the RADIUS Global tab (Figure 23 on page 89) 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 (Figure 22).
2. Click the RADIUS Servers tab.

   The RADIUS Servers tab opens (Figure 24).
3. In the row to modify, type 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 (Figure 22).

2. Click the RADIUS Servers tab.

   The RADIUS Servers tab opens (Figure 24).

3. Identify the configuration to delete by clicking anywhere in the row.
4. Click Delete.
5. Click Apply.

# Chapter 4
# Setting security features using the CLI

This chapter includes the following topics that describe how to set up the security features:



**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

## Roadmap of Security commands

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

| Command | Parameter |
|---|---|
| config cli password | ro <username> [<password>] |
| | l2 <username> [<password>] |
| | l3 <username> [<password>] |
| | rw <username> [<password>] |
| | rwa <username> [<password>] |
| config cli password info | |
| config sys access-policy enable <true\|false> | |
| config sys access-policy policy <pid> | info |
| | accesslevel <level> |
| | create |
| | delete |
| | disable |
| | enable |
| | host <ipaddr> |
| | mode <allow\|deny> |
| | 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> |
| | ssh <enable\|disable> |

| Command | Parameter |
|---|---|
| | telnet <enable\|disable> |
| | tftp <enable\|disable> |
| config sys set snmp community <ro\|rw\|l2\|l3\|rwa> <commstr> | |
| config snmp-v3 usm create <User Name> [<auth protocol>] [auth <value>] [priv <value>] | user name |
| | auth protocol |
| | auth |
| | priv |
| config snmp-v3 group-member create <user name> <model> [<group name>] | user name |
| | Security model <usm\|snmpv1\|snmpv2c> |
| | group name |
| config snmp-v3 group-access create <group name> <prefix> <model> <level> [match <value>] | group name |
| | prefix |
| | model <usm \| snmpv1 \| snmpv2c> |
| | level |
| | match <exact\|prefix> |
| config snmp-v3 mib-view create <View Name> <subtree oid> [mask <value>] [type <value>] | View Name |
| | subtree |
| | mask |
| | type <include\|exclude> |
| config snmp-v3 community create <Comm Idx> <name> <security> | Comm Idx |
| | name |
| | securityname |

| Command | Parameter |
|---|---|
| show config module sys | |
| config sys set ssh | info |
| | action |
| | dsa-auth <true\|false> |
| | enable <true\|false\|secure> |
| | max-sessions <integer> |
| | pass-auth <true\|false> |
| | port <integer> |
| | rsa-auth <true\|false> |
| | timeout <integer> |
| | version <both\|v2only> |
| show sys ssh | global |
| | session |
| config radius | info |
| | acct-attribute-value <value> |
| | acct-enable <true\|false> |
| | attribute-value <value> |
| | clear-stat |
| | acct-include-cli-commands <true\|false> |
| | enable <true\|false> |
| | maxserver <value> |
| config radius server | info |
| | create <ipaddr> |
| | secret <value>—the secret key of the authentication client.delete <ipaddr> |
| | usedby <value>—specifies CLI, or IGAP, or SNMP. |
| | delete <ipaddr> |

| Command | Parameter |
| --- | --- |
| | set <ipaddr> |
| | [usedby <value>] [port <value>] [priority <value>] [retry <value>] [timeout <value>] [enable <value>] [acct-port <value>] [acct-enable <true\|false>] |
| show radius server config | |
| show radius server stat | |

# Controlling access to the CLI

## Changing passwords when upgrading to PP8000 3.3

In the Passport 8000 Series switch software release 3.5, community strings are stored (as passwords have been since release 3.2.1) in encrypted format and are no longer stored in the configuration file. If a configuration file saved prior to release 3.5 is loaded, any saved passwords from the configuration file will not be recognized. If the switch is booted for the first time with the software release 3.5 image, the password is reset to default values and a log is generated indicating any changes.

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

To change the passwords, see the following section, Changing passwords.

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

```
prompt:

reset-passwd
```

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

## Changing passwords

The switch is shipped with default passwords set for access to the CLI. When using SNMPv3, you can change passwords that are in encrypted format. 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: | |
|---|---|
| ro <*username*> [<*password*>] | Changes the read-only login and/or password.<br>*username* is the login name.<br>*password* is the password associated with the login name. |
| l2 <*username*> [<*password*>] | Changes the layer 2 read/write login and/or password.<br>*username* is the login name.<br>*password* is the password associated with the login name. |
| l3 <*username*> [<*password*>] | Changes the layer 3 read/write login and/or password (applies only to the Passport 8600 switch).<br>*username* is the login name.<br>*password* is the password associated with the login name. |
| rw <*username*> [<*password*>] | Changes the read/write login and/or password.<br>*username* is the login name.<br>*password* is the password associated with the login name. |

| **config cli password** followed by: | |
|---|---|
| `rwa <username> [<password>]` | Changes the read/write/all login and/or password.<br>*username* is the login name.<br>*password* is the password associated with the login name. |
| `slboper <username>` | Sets the server load balancing (SLB) Operator login to connect to the Web Switch Module (WSM).[1] |
| `l4oper <username>` | Sets the Layer 4 Operator login to connect to the WSM.[1] |
| `oper <username>` | Sets the Operator login to connect to the WSM.[1] |
| `slbadmin <username>` | Sets the SLB Administrator login to connect to the WSM.[1] |
| `l4admin <username>` | Sets the Layer 4 Administrator login to connect to the WSM.[1] |
| `ssladmin <username>` | Sets the ssladmin login to connect to and configure the SAM (ssl acceleration module). |

1 For more information about the WSM, refer to *Installing the Web Switching Module for the 8000 series switch*.

**Caution:** The ssladmin users are granted a broad range of rights that incorporate the 8600 read/write access. Users with ssladmin access can also add, delete, or modify all 8600 configurations and the WSM software image and configuration. For more information, see *Configuring the SSL acceleration module*.

To verify the current CLI password settings, use the following command:

```
config cli password info
```

### *Configuration example: passwords*

This configuration example uses the command described in this section to check the current CLI password settings. After setting the password or passwords, use the **`info`** command to show a summary of the results.

```
8610:5# config cli password ro test 12345

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

Password changed successfully
8610:5# config cli password
8610:5/config/cli/password# info

Sub-Context:
Current Context:

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

        l4admin   l4admin
        slbadmin  slbadmin
        oper      oper
        l4oper    l4oper
        slboper   slboper
        ssladmin ssladmin

8610:5/config/cli/password#
```

### Synchronizing the master and slave CPU passwords

To synchronize the master and slave CPU passwords, perform the following steps:

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

1. Change the password on the master CPU.
2. Save the password by executing the following CLI command: **`save config`**
3. Execute the following CLI command: **`save config file config.cfg standby`**
4. Go to the slave CPU and change the password by executing the following CLI command: **`config cli password rwa <username> [<password>]`**

**Note:** This does not apply to HA CPU mode, in which case the passwords are automatically synchronized on the master and slave CPUs.

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

## Controlling access to the switch

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, and rlogin.

**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 with the Management Software*.

**Note:** You no longer have to reboot the switch for your telnet ID settings to take effect.

For information about enabling access services for a specific policy using the CLI, see "Enabling an access service" on page 115.

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.

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 section discusses the following topics:

## 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 an 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` | |
| `accesslevel <level>` | Allows you to specify the level of access if the policy is to allow access.<br>• *`level`* is the access level (ro, rw, or rwa) or equivalent community string designation (read-only, read/write, or read/write/all). |
| `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. |
| `enable` | Enables the access policy on the switch |
| `host <ipaddr>` | For rlogin access, specifies the trusted host address. |

| **config sys access-policy policy <*pid*>** followed by: | |
|---|---|
| mode <allow\|deny> | 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.<br>• *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*

This configuration example uses the commands described in this section to configure access policies. After configuring the parameters, use the **info** command to show a summary of the results.

```
8610:5# config sys access-policy policy 2345
8610:5/config/sys/access-policy/policy/2345# info

Sub-Context: service
Current Context:

                    create : not created
                    delete : N/A

8610:5/config/sys/access-policy/policy/2345# create
8610:5/config/sys/access-policy/policy/2345# info

Sub-Context: service
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 : readWrite

8610:5/config/sys/access-policy/policy/2345# network 12.12.12.12/
255.255.255.255
8610:5/config/sys/access-policy/policy/2345# username test
8610:5/config/sys/access-policy/policy/2345# host 5.5.5.5
8610:5/config/sys/access-policy/policy/2345# name testpolicy
8610:5/config/sys/access-policy/policy/2345# precedence 100
8610:5/config/sys/access-policy/policy/2345# host 6.6.6.6
8610:5/config/sys/access-policy/policy/2345# info

Sub-Context: service
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 : readWrite

8610:5/config/sys/access-policy/policy/2345#
```

## 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.

## 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 8600, 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 and you must change them here.

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 pprtl2l2.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 and you must change them here.

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 Passport8600 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 the status (disable or enable) of each service (e.g., ftp, http, rlogin). |
| `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. |
| `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*

This configuration example uses the commands described in this section to enable or disable a service. After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5# config sys access-policy policy 1234
8610:5/config/sys/access-policy/policy/1234# service?

Sub-Context:
Current Context:

    ftp <enable|disable>
    http <enable|disable>
    info
    rlogin <enable|disable>
    snmp <enable|disable>
    ssh <enable|disable>
    telnet <enable|disable>
    tftp <enable|disable>

8610:5/config/sys/access-policy/policy/1234# service ftp enable
8610:5/config/sys/access-policy/policy/1234# service snmp enable
8610:5/config/sys/access-policy/policy/1234# service telnet
enable
8610:5/config/sys/access-policy/policy/1234# service
8610:5/config/sys/access-policy/policy/1234/service# info

Sub-Context:
Current Context:

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

Passport-8610:5/config/sys/access-policy/policy/1234/service#
```

## 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 a 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.

# Configuring SNMPv3

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.

The following sections describe how to set up your SNMP configuration:



## Loading the encryption module

Before you access the switch using SNMPv3 with DES encryption, you must load the encryption module, p80c3300.des, which allows you to use the Privacy protocol.

1. Open a browser and enter the following URL:

   `www.nortelnetworks.com/support/downloads`

2. Log in and search for the following:

   Passport 8000 Routing Switch

3. Double-click on the Passport 3des hyper link.

4. Answer the questions on the questionnaire.

   A download dialog box appears.

5. Enter a file location in which to copy the p80c3300.des encryption module.

6 Click OK.

7 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.

## Creating a new user in the USM table

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

```
config snmp-v3 usm create <User Name> [<auth protocol>]
[auth <value>] [priv <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` | Specifies an authentication password. If no value is entered, the entry has no authentication capability. The range is 1 to 32 characters. |
| `priv` | Assigns a privacy password. If no value is entered, the entry has no privacy capability. The range is 1 to 32 characters.<br>**Note:** You must set authentication before you can set the privacy option. |

*Configuration example: USM*

This configuration example uses the above commands to create a new user in the USM table and display configuration information on the user.

```
8610:5# config snmp-v3 usm create fleming
8610:5# config snmp-v3 usm info

Engine ID = 80:00:08:E0:03:00:01:81:2C:90:00

=============================================================
                      USM Configuration
=============================================================
User Name                       Protocol
-------------------------------------------------------------
fleming                         NO AUTH,  NO  PRIVACY
initialmd5                      HMAC_MD5, DES PRIVACY
initialsha                      HMAC_SHA, DES PRIVACY

8610:5#
```

### 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` | Deletes a user for the v3 VACM table |
| `auth` | Change the authentication password |
| `priv` | Change privacy password |

## Configuring SNMPv3

Perform these SNMPv3 configuration steps from CLI.

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

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

**2** Create a group and assign that to the user.

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

**3** Assign an access level to the newly created group.

```
config snmp-v3 group-access create newgroup pref usm
authPriv
```

**4** Assign a mib view to the group.

```
config snmp-v3 group-access view newgroup pre usm
authPriv read newmibview write newmibview
```

**5** Create a MIB view.

```
config>v3>mib-view > create newmibview subtree 1.3
```

**6** Load a p80c3300.des encryption module by entering the following command:

```
Passport-8610:5/config# load-module DES /flash/
p80c3500b040.des
```

**7** Open the Device Manager in snmpv1/v2 and do the following:

**a** Go to edit > VACM table >group Access right tab

**b** Delete newgroup

**c** Click Insert button and enter the following information in the window:

VacmGroupName: newgroup

ContextPrefix:

Security model: USM

SecurityLevel: authpriv

ContextMatch: exact

ReadViewName: newmibview

WriteViewName: newmibview

StorageType: nonvolatile

The new user can now log in.

**8** In the Device Manager, click Open.

The Open Device dialog box appears.

**Figure 28** Open Device dialog box


**9** Enter the device IP address in the Device Name field.

**10** Select v3 Enabled.

**11** Enter a user name in the User Name field.

**12** Select MD5 in the Authentication Protocol field.

**13** Enter the Authentication password.

**14** Select DES in the Privacy Protocol field.

**15** Enter the Privacy password.

**16** Click Open.

The Device opens.

A description of the Open Device dialog box fields is shown in Table 31.

**Table 31** Open Device dialog box fields

| Field | Description |
|---|---|
| User Name | Indicates the name of the user in usmUser |
| Authentication Protocol | Identifies the Authentication protocol used |
| Authentication Password | Creates 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 | Creates 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 new user group member

To create a new group member on the 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. |
| `Security model <usm\|snmpv1\|snmpv2c>` | Specifies the message processing model to use when generating an SNMP message. |
| `group name` | Assigns the user to the group for data access. The range is 1 to 32 characters. |

### *Configuration example: SNMPv3 group*

This configuration example uses the above commands to create a new user for a group and then display the access levels for each member of a group.

```
8610:5# config snmp-v3 group-member info

=================================================================
             VACM Group Membership Configuration
=================================================================
Sec Model        User Name                  Group Name
-----------------------------------------------------------------
usm              initialmd5                 initial
usm              initialsha                 initial


8610:5# config snmp-v3 group-member create john usm group 2
8610:5# config snmp-v3 group-member create nick snmpv2c group 2
8610:5# config snmp-v3 group-member info
=================================================================
             VACM Group Membership Configuration
=================================================================
Sec Model  User Name      Group Name
-----------------------------------------------------------------
usm        john              group
nmpv2c     nick              group
usm        initialmd5        initial
usm        initialsha        initial
8610:5# config snmp-v3 group-member delete nick usm
8610:5# config snmp-v3 group-member info
=================================================================
             VACM Group Membership Configuration
=================================================================
Sec Model  User Name      Group Name
-----------------------------------------------------------------
usm        john              group
usm        initialmd5        initial
usm        initialsha        initial

8610:5#
```

### 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 | Deletes a user group for the v3 VACM table |
| name | Change group name for the v3 VACM table |

## Creating v3 group access

To create new access for a group in the view-based access control model (VACM) table on the 8000 series switch, use the following command:

```
config snmp-v3 group-access create <group name> <prefix>
<model> <level> [match <value>]
```

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. |
| model <*usm* \| *snmpv1* \| *snmpv2c*> | Assigns the authentication checking to communicate to the switch. |
| level | Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. |
| match <*exact*\|*prefix*> (Optional) | • Exact –Specifies that all rows where the context Name exactly matches the context prefix are selected.<br>• Prefix – Specifies that all rows where the contextName whose starting octets exactly match the context prefix are selected. |

### *Configuration example: SNMPv3 group access*

This configuration example uses the above commands to create new access for two groups in the view-based access control model (VACM) table, delete one of the groups, display the group access information, view read write information, and redisplay the access configuration data.

```
8610:5# config snmp-v3 group-access create secondary team usm noAuthNoPriv match exact
8610:5# config snmp-v3 group-access create tertiary control usm noAuthNoPriv match exact
8610:5# config snmp-v3 group-access info


================================================================================
                            VACM Group Access Configuration
================================================================================
Group      Prefix     Model   Level             Match      ReadV      WriteV
--------------------------------------------------------------------------------
secondary  team       usm      noAuthNoPriv      exact
tertiary   control    usm      noAuthNoPriv      exact
initial               usm      noAuthNoPriv      exact      snmp
initial               usm      authNoPriv        exact      org            org

config snmp-v3 group-access delete 1 2 usm noAuthNoPriv
config snmp-v3 config snmp-v3 group-access view 3 4 usm noAuthNoPriv read 3 write 3
8610:5# config snmp-v3 group-access info

================================================================================
                          VACM Group Access Configuration
================================================================================
Group      Prefix Model   Level        Match ReadV      WriteV
--------------------------------------------------------------------------------
tertiary       control  usm       noAuthNoPriv       exact  tertiary        tertiary
initial                 usm       noAuthNoPriv       exact snmp
initial                 usm       authNoPriv       exact  org              org
```

## 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 |
| `delete` | Removes group access for the v3 VACM table |

| **config snmp-v3 group-access**<br>followed by: | |
|---|---|
| `match` *exact\|prefix>* | Change group access context match for the v3 VACM table<br>• Exact –Specifies that all rows where the context Name exactly matches the context prefix are selected.<br>• Prefix – Specifies that all rows where the contextName whose starting octets exactly match the context prefix are selected. |
| `view` | Change group access view name match for the v3 VACM table |

## Creating a new entry for the MIB in the View table

To create a new entry for the MIB View table on the 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**<br>followed by: | |
|---|---|
| `View Name` | Creates a new entry with this group name. The range is 1 to 32 characters. |
| `subtree` | The prefix that defines the set of MIB objects accessible by this SNMP entity. The range is 1 to 32 characters. |
| `mask`<br>(Optional) | Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree. |
| `type <`*include\|exclude*`>`<br>(Optional) | Determines whether access to a mib object is granted or denied. |

### *Configuration example: MIB view*

This configuration example uses the above commands to create a MIB view, change the MIB view mask and type, and display configuration information on the MIB view.

```
8610:5# config snmp-v3 mib-view create dev 1.3.8.7.1.4 mask wless
type include
8610:5# config snmp-v3 mib-view info

================================================================
                            MIB View
================================================================
View Name           Subtree              Mask      Type
----------------------------------------------------------------
dev                 1.3.8.7.1.4           wless     include
org                 1.3                             include
snmp                1.3.6.1.6.3                     include
snmp                1.3.6.1.2.1.1                   include
system              1.3.6.1.2.1.1                   include
v1v2only            1.3                             include
v1v2only            1.3.6.1.6.3.15                  exclude
v1v2only            1.3.6.1.6.3.16                  exclude
v1v2only            1.3.6.1.6.3.18                  exclude

8610:5# config snmp-v3 mib-view mask dev 1.3.8.7.1.4 wire
8610:5# config snmp-v3 mib-view info

================================================================
                            MIB View
================================================================
View Name           Subtree              Mask       Type
----------------------------------------------------------------
dev                 1.3.8.7.1.4 7        wire       include
org                 1.3                             include
snmp                1.3.6.1.6.3                     include
snmp                1.3.6.1.2.1.1                   include
system              1.3.6.1.2.1.1                   include
v1v2only            1.3                             include
v1v2only            1.3.6.1.6.3.15                  exclude
v1v2only            1.3.6.1.6.3.16                  exclude
v1v2only            1.3.6.1.6.3.18                  exclude

8610:5# config snmp-v3 mib-view type dev1.3.8.7.1.47exclude
8610:5# config snmp-v3 mib-view info
```

```
=================================================================
                            MIB View
=================================================================
View Name           Subtree              Mask       Type
-----------------------------------------------------------------
dev                 1.3.8.7.1.4 7          wire         exclude
org                 1.3                                include
snmp                1.3.6.1.6.3                        include
snmp                1.3.6.1.2.1.1                      include
system              1.3.6.1.2.1.1                      include
v1v2only            1.3                                include
v1v2only            1.3.6.1.6.3.15                     exclude
v1v2only            1.3.6.1.6.3.16                     exclude
v1v2only            1.3.6.1.6.3.18                     exclude

8610:5#
```

### 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` | Deletes an entry an entry for the mib-view table |
| `mask` | Changes the view mask for an entry in the mib-view table |
| `type` | Changes the type for an entry in the mib-view table |

## Creating a community

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

```
config snmp-v3 community create <Comm Idx> <name> <security>
```

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 |
| `securityname` | Maps community string to the security name in the VACM Group Member Table. |

### *Configuration example: community*

This configuration example uses the above commands to create a new community, change the community name and security name, and display configuration information on the community.

```
8610:5# config snmp-v3 community create third public v1v2only
8610:5# config snmp-v3 community info

INDEX           NAME            SECURITYNAME
first           public          v1v2only
second          private         v1v2only
third           public          v1v2only

8610:5# config snmp-v3 community name third private
8610:5#
8610:5# config snmp-v3 community info

INDEX           NAME            SECURITYNAME
first           public          v1v2only
second          private         v1v2only
third           private         v1v2only
8610:5# config snmp-v3 community security third v1v3only
8610:5# config snmp-v3 community info
INDEX           NAME            SECURITYNAME
first           public          v1v2only
second          private         v1v2only
third           private         v1v3only
8610:5#
```

### Other community commands

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

| **`config snmp-v3 community`** followed by: | |
|---|---|
| `info` | Displays the current level parameter settings and next level directories |
| `delete` | Deletes an entry for community table |
| `name` | Changes the name for an entry in community table |
| `security` | Changes the security name for an entry in community table |

## Displaying SNMP system information

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

```
show config module sys
```

### *Configuration example: show SNMP system information*

This configuration example uses the **`show config module sys`** command to display SNMP system information.

```
8610:5# show config module sys
Preparing to Display Configuration...
#
# THU MAR 07 16:20:17 2002 UTC
# box type             : 8010
# software version     : REL3.3.0.0_B062
# monitor version      : 3.3.0.0/063
#
#
# Asic Info :
# SlotNum|Name  |CardType|MdaType |Parts Description
#
# Slot  1   8624FX 20310118 00000000   IO: PLRO= 3 OP=2 TMUX=2 RARU=2 CPLD=4
# Slot  2     --   00000001 00000000
# Slot  3  8672ATM 20550108 20540204  205d1202  OP=2 TMUX=2 RARU=2 CPLD=4
# Slot  4     --   00000001 00000000
# Slot  5   8690SF 200e0100 00000000  CPU: CPLD=15 OP=2 TMUX=2 SWIP=2 FAD=1 CF=11
# Slot  6     --   00000001 00000000
# Slot  7     --   00000001 00000000
# Slot  8     --   00000001 00000000
# Slot  9     --   00000001 00000000
# Slot 10     --   00000001 00000000
config
#
# SYSTEM CONFIGURATION
#
sys set snmp trap-recv 192.32.229.101 v1 public

sys set snmp trap-recv 192.32.229.129 v1 public

sys set snmp trap-recv 192.168.1.100 v1 public

#
# LINK-FLAP-DETECT CONFIGURATION
#
# ACCESS-POLICY CONFIGURATION
#
sys access-policy policy 1 service ssh enable
#
# SNMP V3 GROUP MEMBERSHIP CONFIGURATION
#
v3 group-member create 3 usm snmpv2c
```

```
#
# SNMP V3 GROUP ACCESS CONFIGURATION
#
v3 group-access create 3 "4" usm noAuthNoPriv match exact
v3 group-access view 3 "4" usm noAuthNoPriv read "3" write "3"
#
# SNMP V3 MIB VIEW CONFIGURATION
#
v3 mib-view create 2 5 mask 7SLF1007X6″pÙd type exclude
#
# SNMP V3 COMMUNITY TABLE CONFIGURATION
#
v3 community create third private v1v3only
#
# SSH CONFIGURATION
#
back
8610:5#
```

**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.

## Setting the SNMP community strings

SNMP community strings are required for access to the switch using Device Manager or other SNMP-based management software.

To set SNMP community strings, use the following command:

`config sys set snmp community <ro|rw|l2|l3|rwa> <`*`commstr`*`>`

where:
`ro|rw|l2|l3|rwa` is the choice of community**.** `ro` is read-only, `rw` is read/write, `l2` is layer 2 read/write, `l3` is layer 3 (and layer 2) read/write, and `rwa` is read/write/all.
*`commstr`* is the input community string up to 1024 characters.

# Configuring SSH

This section describes how to implement SSH in your network, and discusses the following topics:



## 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.

For the latest information on how to download the 3DES encryption image, refer to the release notes accompanying your software release.

## 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 true`**

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: | |
|---|---|
| `block-snmp <true\|false>` | Block or unblock the SNMP protocol.<br>• `<true\|false>` Set to true to block SNMP. Set to false to unblock SNMP. |
| `sshd <true\|false>` | Enable or disable the SSH services on the switch.<br>• *`<true\|false>`* Set to true to enable the SSH services. Set to false to disable the SSH services. |

## Setting SSH configuration parameters

To set SSH configuration parameters on an 8000 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>]` | Set the SSH key action.<br>• `<action choice>` choose one of the following actions:<br>- rsa-keygen<br>- rsa-keydel<br>- dsa-keygen<br>- dsa-keydel<br>• `[<integer>]` the SSH host key size. Can be a value from 512 to 1024. Default is 1024. |
| `dsa-auth <true\|false>` | Enable or disable the DSA authentication.<br>• <true\|false> true enables the authentication and false disables the authentication. Default is true. |
| `enable <true\|false\|secure>` | Enable, or disable, the SSH daemon.<br>• `<true\|false\|secure>`<br>- true, enable SSH<br>- false, disable SSH<br>- secure, enables SSH and disables insecure services (SNMP, tftp, and Telnet). These insecure services will be disabled after reboot. Default is false. |
| `max-sessions <integer>` | The maximum number of SSH sessions allowed.<br>• <integer> a value from 0 to 8. Default is 4. |
| `pass-auth <true\|false>` | Enable or disable password authentication.<br>• `<true\|false>` set to true to enable authentication and false to disable authentication. Default is true. |
| `port <integer>` | Sets the SSH connection port.<br>• `<integer>` port number. Default is 22. |
| `rsa-auth <true\|false>` | Enable or disable RSA authentication.<br>• `<true\|false>` set to true to enable authentication and false to disable authentication. Default is true. |

| **config sys set ssh**<br>followed by: | |
|---|---|
| `timeout <integer>` | The SSH connection authentication timeout in seconds.<br>• `<integer>` number of seconds. Default is 60 seconds. |
| `version <both\|v2only>` | Set the SSH version.<br>• `<both\|v2only>` both\|v2only. Default is v2only.<br>**Note:** Nortel Networks recommends setting the version to v2only. |

## *Configuration example: SSH*

This configuration example uses the previous commands and shows a summary of the results using the **`info`** command.

```
Passport-8606:6# config sys set ssh action rsa-keygen 1024
Passport-8606:6# config sys set ssh action dsa-keygen 1024
Passport-8606:6# config sys set ssh dsa-auth true
Passport-8606:6# config sys set ssh max-sessions 4
Passport-8606:6# config sys set ssh pass-auth true
Passport-8606:6# config sys set ssh port 22
Passport-8606:6# config sys set ssh rsa-auth true
Passport-8606:6# config sys set ssh timeout 60
Passport-8606:6# config sys set ssh version v2only
Passport-8606:6# config sys set ssh enable true
Passport-8606:6# config sys set ssh info

Total Active Sessions  : 0
        version            : v2only
        port               : 22
        max-sessions       : 4
        timeout            : 60
        action rsa-keygen  : rsa-keysize 1024
        action dsa-keygen  : dsa-keysize 1024
        rsa-auth           : true
        dsa-auth           : true
        pass-auth          : true
        enable             : true

Passport-8606:6#
```

## Verifying and displaying SSH configuration information

To verify that SSH services are enabled on the 8000 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 29 shows examples of **`show sys ssh global`** and **`session`** commands output.

**Figure 29** show sys ssh global and session commands output

```
8610:5# show sys ssh global

Total Active Sessions  : 1
        version            : v2only
        port               : 22
        max-sessions       : 4
        timeout            : 60
        action rsa-keygen  : rsa-keysize 1024
        action dsa-keygen  : dsa-keysize 1024
        rsa-auth           : true
        dsa-auth           : true
        pass-auth          : true
        enable             : true

8603:3ssh# show sys ssh session

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

# Configuring RADIUS authentication and accounting

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 client information, user information, password, 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 8000 series switch, you use RADIUS authentication to secure access to the switch (console/Telnet/SSH), and RADIUS accounting to track the management sessions (CLI only).

RADIUS authentication allows the remote server to authenticate logins. RADIUS accounting logs all of the activity of each remote user in a session on the centralized RADIUS accounting server.

For more information on RADIUS authentication or RADIUS accounting in your network, see Chapter 1.

This section discusses the following topics:



## Configuring RADIUS

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

```
config radius
```

This command includes the following parameters:

| **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.<br>*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. |
| `attribute-value <value>` | 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. Nortel Networks recommends the default setting of 192 for Passport 8000 Series switches.<br>*value* is between 192 and 240 |
| `clear-stat` | Clears RADIUS statistics from the server. |
| `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. |
| `enable <true\|false>` | Enables (true) or disables (false) the RADIUS authentication feature. |
| `maxserver <value>` | Specific to RADIUS authentication. Sets the maximum number of servers allowed for the switch.<br>*value* is between 1 and 10 |

## 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.

## Modifying user access to RADIUS CLI commands

This functionality provides Network Administrator the ability to override the access to CLI commands given to the user as per the access level for Passport 8600, This is done by configuring the Radius Server for user authentication (See Section 1.2.3 below). This capability is absent in the current Passport 8600 implementation. Network administrator has to give access based on the already existing six access levels in Passport 8600. Now with this feature network administrator can allow/disallow a user of certain CLI commands in addition to what the user can execute based on the access level.

## 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 attribute-value <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*

This configuration example uses the commands described in this section to enable RADIUS accounting and authentication on the switch. After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5# config radius
8610:5/config/radius# acct-enable true
8610:5/config/radius# enable true
8610:5/config/radius# info

Sub-Context: server
Current Context:

             acct-attribute-value : 193
                      acct-enable : true
        acct-include-cli-commands : false
                  attribute-value : 192
                           enable : true
                        maxserver : 10

8610:5/config/radius#
```

## Showing RADIUS information

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

```
config radius info
```

or

```
show radius info
```

Figure 30 shows sample command output for the `config radius info` command. The output for the `show radius info` command is the same as that for `config radius info`.

**Figure 30** config radius info sample output

```
8610:5# config radius info

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

             acct-attribute-value : 193
                      acct-enable : true
        acct-include-cli-commands : false
                attribute-value : 192
                         enable : false
                      maxserver : 10
8610:5# config radius clearstat
```

## Adding a RADIUS server

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

### *Configuration example: Adding a RADIUS server*

This configuration example uses the commands described in this section to add a RADIUS server. After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5/config/radius# config radius server
8610:5/config/radius/server# create 12.12.12.12 secret 9
8610:5/config/radius/server# info

Sub-Context:
Current Context:

                     create :

Name              Secret              Port    Prio  Retry Timeout
Enabled Acct-port Acct-enabled
10.10.10.10      6                1812    10    3     3      true
1813    true
12.12.12.12      9                1812    10    3     3      true
1813    true

                     delete : N/A
                        set : N/A

8610:5/config/radius/server#
```

## Showing RADIUS server configurations

To display current RADIUS server configurations, use the following command:

```
show radius server config
```

Figure 31 shows sample output for this command.

**Figure 31** show radius server config sample command output

```
8010# show radius server config

Sub-Context:
Current Context:

                      create :

Name          Secret   Port  Prio  Retry Timeout Enabled Acct-port Acct-enabled
10.10.50.19 test3   1812 10    6    3      true   1813     true

                      delete : N/A
                         set : N/A

8010#
```

## Showing RADIUS server statistics

**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.

To display statistics for the current RADIUS servers, use the following command:

```
show radius server stat
```

Figure 32 shows sample output for this command.

**Figure 32** show radius server stat command output

```
8010# show radius server stat

           Radius Server : 172.16.200.19
----------------------------------------
         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

8010#
```

Table 32 describes the fields for this command.

**Table 32** show radius server stat command fields

| Item | Description |
|---|---|
| RADIUS Server | The IP address of the RADIUS server. |
| AccessRequests | Number of access-response packets sent to the server; does not include retransmissions. |
| AccessAccepts | Number of access-accept packets, valid or invalid, received from the server. |
| AccessRejects | Number of access-reject packets, valid or invalid, received from the server. |
| BadResponses | Number of invalid access-response packets received from the server. |
| PendingRequests | Access-request packets sent to the server that have not yet received a response, or have timed out. |
| ClientRetries | Number of authentication retransmissions to the server. |
| AcctOnRequests | Number of accounting On requests sent to the server. |
| AcctOffRequests | Number of accounting Off requests sent to the server. |

**Table 32** show radius server stat command fields (continued)

| Item | Description |
|---|---|
| AcctStartRequests | Number of accounting Start requests sent to the server. |
| AcctStopRequests | Number of accounting Stop requests sent to the server. |
| AcctInterimRequests | Number of accounting Interim Requests sent to the server.<br>**Note:** The AcctInterimRequests counter will increment only if the parameter acct-include-cli-commands is set to true. |
| AcctBadResponses | Number of Invalid Responses from the server that are discarded. |
| AcctPendingRequests | Number of requests waiting to be sent to the server. |
| AcctClientRetries | Number of retries made to this server. |

**Note:** To clear server statistics, use the **`config radius clear-stat`** command.

## RADIUS/SNMP header network address modifications

In the 3.5 release, 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 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.

## Configuring RADIUS Accounting for SNMP

You can authenticate the users logging into the Passport 8600 switches through SNMP. The authentication request is forwarded to 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 BSAC 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 8600, 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 free RADIUS server

To configure a free RADIUS 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 8600, 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 8600 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 8600 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*

This configuration example uses the commands described in this section to add a RADIUS server. After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5/config/radius# config radius server
8610:5/config/radius/server# create 12.12.12.12 secret 9 useby snmp
8610:5/config/radius/server/snmp#
```

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. |

# Configuring directed broadcast

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.

## Preventing certain types of DOS attacks

To protect the Passport 8600 against IP packets with illegal IP addresses such as loopback addresses or a Src IP address of all ones, or Class D or Class E addresses from being routed, the Passport 8600 now supports a configurable flag: `high-secure`, which is enabled using the CLI command:

```
config ethernet (slot/port) high-secure [true/false]
```

This command includes the following options:

| **config ethernet (slot/port) high-secure** followed by: | |
|---|---|
| `info` | Displays if high-secure is configured on that port. |
| Required parameters:<br>`[slot/port <value>]`<br>`high-secure <true/false>` | `high-secure <true/false>`— Enables the high Secure Feature which blocks packets with illegal IP address. |

This flag 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 (internally called *OctaPid*). See Table 2 for the mapping between OctaPids and ports.

### *Configuration example: Enable High-Secure mode*

This configuration example uses the **`config ethernet 4/1-4/2 high-secure true`** command to filter packets on ports 4/1-4/2 and the **`info`** command to show a summary of the results.

```
Passport8600-5:5# config ethernet 4/1-4/2 high-secure true
WARNING ! DHCP and BOOTP will be suppressed on these ports: - 4/1
Implement High Secure on all the other ports corresponding to MLT-ID :7
Implement High Secure on all the vlans to which these ports belong 4/1
WARNING ! DHCP and BOOTP will be suppressed on these ports: - 4/2
Implement High Secure on all the other ports corresponding to MLT-ID :25
Implement High Secure on all the vlans to which these ports belong 4/2
Passport8600-5:5#
Passport8600-5:5# config ethernet 4/1-4/2 info

Sub-Context: clear config dump monitor show test trace wsm
Current Context:
Port 4/1 :
                        lock : false
                        name :
              auto-negotiate : true
             enable-diffserv : false
             access-diffserv : false
                   qos-level : 0
          unknown-mac-discard : disable
                  high-secure : true
Port 4/2 :
                        lock : false
                        name :
              auto-negotiate : true
             enable-diffserv : false
             access-diffserv : false
                   qos-level : 0
          unknown-mac-discard : disable
                  high-secure : true
```

### *Configuration example: Disable High-Secure mode*

This configuration example uses the **`config ethernet 4/1 high-secure false`** command to disable high secure on port 4/1.

```
Passport8600-5:5# config ethernet 4/1 high-secure false
Implement High Secure on all the other ports corresponding to MLT-ID :25
Implement High Secure on all the vlans to which these ports belong 4/1
```

**Note:** The word **implement** in this reference means to **remove**.

# Index

## Numbers



## A



## B



## C



## D



## E



## I



## L



## M



## P

## R



## S



## T



## W