

Part No. 317346-C
June 2005

4655 Great America Parkway
Santa Clara, CA 95054

Configuring and Managing Security using Device Manager

Ethernet Routing Switch 8300
Software Release 2.2



NORTEL

Copyright © Nortel Networks Limited 2005. All rights reserved.

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, Passport, and BayStack are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Aegis is a trademark of Meetinghouse Data Communications, Inc.

LINUX is a trademark of Linus Torvalds.

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

Red Hat is a trademark of Red Hat, Inc.

UNIX is a trademark of UNIX System Laboratories, Inc.

Zone Labs is a trademark of Zone Labs, Inc.

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 foregoing 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

Preface	13
Before you begin	13
Text conventions	14
Hard-copy technical manuals	16
How to get help	17
Chapter 1: Overview of security features	19
CLI passwords	20
Port lock feature	20
Access policies for services	20
SNMP version 3 (SNMPv3)	21
SNMP engine	22
snmpEngineID	22
Dispatcher	22
Message processing	23
Security	23
Access control	24
View-based Access Control (VACM)	25
Secure Shell and Secure Copy	26
SSH version 2 (SSH v2)	28
SSH guidelines	30
Key generation and removal	30
Block SNMP	31
SCP command	31
RADIUS	31
How RADIUS works	32
Configuring the RADIUS server	32
Configuring the RADIUS client	33
RADIUS authentication	34

RADIUS accounting	34
EAPoL	36
EAPoL terminology	36
Standard 802.1x configuration (single supplicant per port)	37
EAPoL static-based security mode	41
Non-standard 802.1x guest VLAN	43
Guest VLAN	43
Guest VLAN security mode	45
Configuration guidelines for setting up a guest VLAN	47
Enabling multiple EAPoL sessions per port	48
Basic EAPoL multihost-based security	49
Enhanced EAPoL multihost-based security	51
EAPoL dynamic VLAN assignment	56
RADIUS MAC centralization	57
Working with RADIUS	60
RADIUS configuration prerequisites for EAPoL	61
RADIUS accounting for EAPoL	62
Configuring the Ethernet Routing Switch 8300 for EAP and RADIUS	64
System requirements	66
TACACS+	66
TACACS+ architecture	67
TACACS+ authentication	68
TACACS+ authorization	69
TACACS+ access levels	69
Chapter 2: Setting passwords, locking ports, and viewing SNMP errors.	71
Controlling access to the CLI	71
Locking a port	75
Viewing SNMP errors	76
Chapter 3: Configuring access policies	79
Creating a new access policy	79
Enabling access policy for rlogin or rsh access	82
Chapter 4: Configuring SNMPv3	85
Loading the encryption module	85

Logging on using SNMPv3	87
Creating a user security model	89
Creating a user security model	90
Creating membership for a group	93
Creating access for a group	94
Assigning MIB view access for an object	97
Creating a community	99
Chapter 5: Configuring SSH	101
Changing Secure Shell configuration parameters	101
Supported SSH and SCP clients	104
Using DSA authentication	105
Using RSA authentication	106
Chapter 6: Setting up RADIUS servers	109
Updating files for the BSAC RADIUS server	110
Updating the dictionary file for a Merit Network server	112
Updating files for the freeRadius server	113
Using a third-party RADIUS server	115
Enabling EAP authentication	116
Chapter 7: Configuring RADIUS authentication and accounting	119
Enabling RADIUS authentication	119
Enabling RADIUS accounting	122
Adding a RADIUS server	122
Showing RADIUS server authentication statistics	125
Showing RADIUS server accounting statistics	126
Modifying a RADIUS configuration	127
Deleting a RADIUS configuration	128
Chapter 8: Configuring EAPoL	129
Configuration prerequisites	130
Configuring EAPoL globally	130
Configuring EAPoL on a port	132
Configuring general authenticator port settings	132
Configuring non-EAPoL clients on a port	136

Configuring non-EAPoL MAC addresses on a port	137
Viewing the status of non-EAPoL clients that use RADIUS	139
Configuring EAPoL multihosts on a port	141
Enabling or disabling multiple clients on switch ports	142
Displaying multiple clients statistics	143
Displaying multiple clients session information	145
Enabling or disabling Guest VLANs on a port	147
Changing the authentication status of a port	148
Graphing EAPoL statistics	149
Graphing EAPoL Authenticator statistics	149
Graphing EAPoL diagnostic statistics	151
Graphing EAPoL session statistics	154
Chapter 9: Configuring TACACS+	157
Configuration prerequisites	157
Configuring TACACS+ globally	157
Adding a TACACS+ server	158
Modifying a TACACS+ configuration	160
Deleting a TACACS+ configuration	161
Index	163

Figures

Figure 1	USM association with VACM	25
Figure 2	Overview of the SSH protocol	26
Figure 3	SSH v2 protocols	29
Figure 4	SSH user authentication protocol	29
Figure 5	SSH connection protocol	30
Figure 6	EAPoL standard 802.1x packet path example	38
Figure 7	Standard 802.1x state machine example	40
Figure 8	EAPoL static-based security example	42
Figure 9	Accessing the guest VLAN	44
Figure 10	EAPoL Guest VLAN security example	46
Figure 11	Basic EAPoL multihost-based security example	50
Figure 12	Multiple EAPoL client example	52
Figure 13	Enhanced EAPoL multihost-based security example	54
Figure 14	Connecting the TACACS+ server through a local interface	68
Figure 15	Connecting the TACACS+ server through the management interface	68
Figure 16	Security dialog box—EAPoL tab	72
Figure 17	Security dialog box—CLI tab top part	73
Figure 18	Security dialog box—Port Lock tab	75
Figure 19	Security dialog box—SNMP tab	76
Figure 20	AccessPolicy dialog box — Access Policies tab	80
Figure 21	AccessPolicy, Insert Access Policies dialog box	80
Figure 22	Chassis dialog box—System tab	82
Figure 23	FTP sample output from DOS window	86
Figure 24	Device Manager window	87
Figure 25	Open Device dialog box	88
Figure 26	USM dialog box	90
Figure 27	USM, Insert USM Table dialog box	91
Figure 28	VACM dialog box	93
Figure 29	VACM, Insert Group Membership dialog box	94

Figure 30	VACM dialog box — Group Access Right tab	95
Figure 31	VACM, Insert Group Access Right dialog box	95
Figure 32	VACM dialog box—MIB View tab	97
Figure 33	VACM—Insert MIB View dialog box	98
Figure 34	Community Table dialog box	99
Figure 35	Community Table, Insert Community Table dialog box	99
Figure 36	Ssh dialog box — SSH tab	102
Figure 37	Radius dialog box — RADIUS Global tab	120
Figure 38	Radius dialog box — RADIUS Servers tab	123
Figure 39	Radius, Insert RADIUS Servers dialog box	123
Figure 40	Radius dialog box — RADIUS Server Auth Stats tab	125
Figure 41	Radius dialog box — RADIUS Server Accounting Stats tab	126
Figure 42	Security dialog box — EAPOL tab	131
Figure 43	Port dialog box — Interface tab	133
Figure 44	Port dialog box — EAPOL tab	134
Figure 45	Non EAPOL MAC dialog box — Non-EAP Config tab	137
Figure 46	Non EAPOL MAC dialog box — Allowed Non-EAP MAC tab	138
Figure 47	Insert Allowed Non-EAP MAC dialog box	138
Figure 48	Non EAPOL MAC dialog box — Non-EAP Using Radius tab	140
Figure 49	EAPOL MultiHosts dialog box — Multi Hosts tab	142
Figure 50	EAPOL MultiHosts dialog box — Multi Hosts Status tab	144
Figure 51	EAPOL MultiHosts dialog box — Multi Hosts Session tab	146
Figure 52	EAPOL Guest VLAN dialog box — Guest VLAN tab	147
Figure 53	Graph Port dialog box — Interface tab	150
Figure 54	Graph Port dialog box — EAPOL Stats tab	150
Figure 55	Graph Port dialog box — EAPOL Diag tab	152
Figure 56	Graph Port dialog box — EAPOL Session tab	155
Figure 57	Tacacs dialog box — TACACS+ Globals tab	158
Figure 58	Tacacs dialog box — TACACS+ Servers tab	158
Figure 59	Tacacs, Insert TACACS+ Servers dialog box	159

Tables

Table 1	Accounting events and logged information	35
Table 2	Summary of accounting events and information logged.	63
Table 3	802.1x session termination mapping	64
Table 4	Ethernet Routing Switch 8300 access levels	69
Table 5	CLI tab fields	74
Table 6	Port Lock tab fields	75
Table 7	SNMP tab fields	77
Table 8	AccessPolicy and Insert Access Policies fields	81
Table 9	Open Device box fields	89
Table 10	USM dialog box fields	90
Table 11	USM—Insert USM Table dialog box fields	92
Table 12	VACM dialog box tab fields	93
Table 13	VACM dialog box—Insert Group Membership tab fields	94
Table 14	VACM dialog box—Insert Group Access Right tab fields	96
Table 15	VACM dialog box—MIB View tab fields	98
Table 16	Community Table, Insert Community Table dialog box fields	100
Table 17	Ssh dialog box — SSH tab fields	102
Table 18	Third party SSH and SCP client software	104
Table 19	DSA authentication access level and filename	105
Table 20	RSA authentication access level and file name	106
Table 21	RADIUS dialog box — RADIUS Global tab fields	120
Table 22	RADIUS Servers tab and Insert RADIUS Servers dialog box fields	124
Table 23	Radius dialog box — RADIUS Server Auth Stats tab fields	125
Table 24	Radius dialog box — RADIUS Server Accounting Stats tab fields	127
Table 25	Port dialog box — EAPOL tab fields	135
Table 26	Non EAPOL MAC dialog box — Non-EAP using Radius tab fields	140
Table 27	Port dialog box — Multi Hosts tab fields	143
Table 28	Port dialog box — Multi Host Status tab fields	144
Table 29	Port dialog box—Multi Host Session tab fields	146

12 Tables

Table 30	Graph Port dialog box — EAPOL Stats tab fields	151
Table 31	Graph Port dialog box — EAPOL Diag tab fields	153
Table 32	Graph Port dialog box—EAPOL Session tab fields	155
Table 33	TACACS+ Servers tab and Insert TACACS+ Servers dialog box fields .	159

Preface

The Nortel* Ethernet Routing Switch 8300 is a flexible and multifunctional Layer 2/Layer 3 switch that supports diverse network architectures and protocols. The Ethernet Routing Switch 8300 provides security and control features such as Extensible Authentication Protocol over LAN (EAPoL), Simple Network Management Protocol, Version 3 (SNMP3), and Secure Shell (SSH). The Ethernet Routing Switch 8300 provides quality of service (QoS) for a high number of attached devices and supports future network requirements for QoS for critical applications, such as Voice over IP (VoIP).

This guide describes the security features available for the Ethernet Routing Switch 8300 Software Release 2.2. The guide provides instructions for starting and customizing these features using the Java Device Manager (Device Manager).

Device Manager is a graphical user interface (GUI) used to configure and manage 8300 Series switches. You install it on a management station in the network. For instructions on installing and starting Device Manager on a Windows*, UNIX*, or Linux* platform, refer to *Installing and Using Device Manager* (316808-C). The manual also describes some common startup problems and how to troubleshoot them.

Before you begin

This guide is intended for network administrators who have the following background:

- basic knowledge of networks, Ethernet bridging, and IP routing
- familiarity with networking concepts and terminology
- experience with windowing systems or GUIs
- basic knowledge of network topologies

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

1 Install the switch.

For installation instructions, see *Installing and Maintaining the Ethernet Routing Switch 8306 and 8310 Chassis* (316795-C) and *Installing Ethernet Routing Switch 8300 Series Modules* (316796-C).

2 Connect the switch to the network.

For more information, see *Getting Started* (316799-C).

Ensure that you are running the latest version of Nortel Ethernet Routing Switch 8300 software. For information about upgrading the Ethernet Routing Switch 8300, see *Upgrading to Ethernet Routing Switch 8300 Software Release 2.2* (318769-C).

Text conventions

This guide uses the following text conventions:

- | | |
|--------------------------|---|
| angle brackets (<>) | Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.
Example: If the command syntax is <code>ping <ip_address></code> , you enter ping 192.32.10.12 |
| bold body text | Indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, tabs, and menu items. |
| bold Courier text | Indicates command names, options, and text that you must enter.
Example: Use the dinfo command.
Example: Enter show ip {alerts routes} . |

braces ({})	<p>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.</p> <p>Example: If the command syntax is <code>show ip {alerts routes}</code>, you must enter either show ip alerts or show ip routes, but not both.</p>
brackets ([])	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is <code>show ip interfaces [-alerts]</code>, you can enter either show ip interfaces or show ip interfaces -alerts.</p>
ellipsis points (...)	<p>Indicate that you repeat the last element of the command as needed.</p> <p>Example: If the command syntax is <code>ethernet/2/1 [<parameter> <value>]...</code>, you enter ethernet/2/1 and as many parameter-value pairs as needed.</p>
<i>italic text</i>	<p>Indicates variables in command syntax descriptions. Also indicates new terms and book titles. Where a variable is two or more words, the words are connected by an underscore.</p> <p>Example: If the command syntax is <code>show at <valid_route></code>, <i>valid_route</i> is one variable and you substitute one value for it.</p>
plain Courier text	<p>Indicates command syntax and system output, for example, prompts and system messages.</p> <p>Example: Set Trap Monitor Filters</p>

separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP command on the Protocols menu.
vertical line ()	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is <code>show ip {alerts routes}</code> , you enter either show ip alerts or show ip routes , but not both.

Hard-copy technical manuals

You can download current versions of technical documentation for your Ethernet Routing Switch 8300 from the Nortel customer support web site at www.nortel.com/support.

If, for any reason, you cannot find a specific document, use the **Search** function:

- 1 Click **Search** at the top right-hand side of the web page.
The **Search** page opens.
- 2 Ensure the **Support** tab is selected.
- 3 Enter the title or part number of the document in the **Search** field.
- 4 Click **Search**.

You can print the technical manuals and release notes free, directly from the Internet. 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.

How to get help

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

If you purchased a Nortel service program, contact Nortel Technical Support. To obtain contact information online, go to the www.nortel.com/contactus web page and click Technical Support.

Information about the Nortel Technical Solutions Centers is available from the www.nortel.com/callus web page.

An Express Routing Code (ERC) is available for many Nortel 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 the ERC for your product or service, go to the www.nortel.com/erc web page.

Chapter 1

Overview of security features

This section describes the security features that allow you to restrict access to the Ethernet Routing Switch 8300.

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, SNMPv3)

You protect the data path using:

- Layer 2 MAC address filtering
- Layer 3 filtering (for example, IP, UDP/TCP filtering)
- Mechanisms to prevent DOS (Denial of Service) attacks

You can use the supported command line interfaces (NNCLI or the Ethernet Routing Switch 8300 CLI) to set up passwords and community strings for access to all the management functions of the switch.

This chapter provides overview information for the following topics:

Topic	Page
CLI passwords	20
Port lock feature	20
Access policies for services	20
SNMP version 3 (SNMPv3)	21
RADIUS	31
EAPoL	36

CLI passwords

The Ethernet Routing Switch 8300 is shipped with default passwords set for access to the CLI through a console or telnet session. Community strings are stored in encrypted format and are not stored in the configuration file. If the switch is booted for the first time, the password is set to default values and a log is generated that indicates any changes. If you are 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 strongly recommends that you change the default passwords/community strings immediately after the first login.



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

Port lock feature

The Port Lock feature allows you to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. Locked ports cannot be modified in any way until the port is unlocked. For instructions on locking ports, see [Chapter 2, “Setting passwords, locking ports, and viewing SNMP errors,” on page 71](#).

Access policies for services

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

For information about enabling access services for a specific policy, see Chapter 3.

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

When you set up access policies, you can either:

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

SNMP version 3 (SNMPv3)

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

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

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

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

- Security for Messages
- Access Control

- Remote configuration of SNMP parameters
- New SNMP message format

SNMP engine

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

snmpEngineID

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

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

Dispatcher

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

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

Message processing

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

Security

Authentication

Authentication within the User-based Security Model (USM) allows the recipient of a message to verify the message sender and whether the message has been altered. If authentication is used, the integrity of the message is verified. Authentication uses a secret key to produce a *fingerprint* of the message. This fingerprint is included in the message. The receiving entity uses the same secret key to validate the fingerprint. The authentication protocols supported using USM are HMAC-MD5 and HMAC-SHA-96.

Privacy

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

Security

SNMPv3 security protects against the following:

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

SNMPv3 does not protect against:

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

Access control

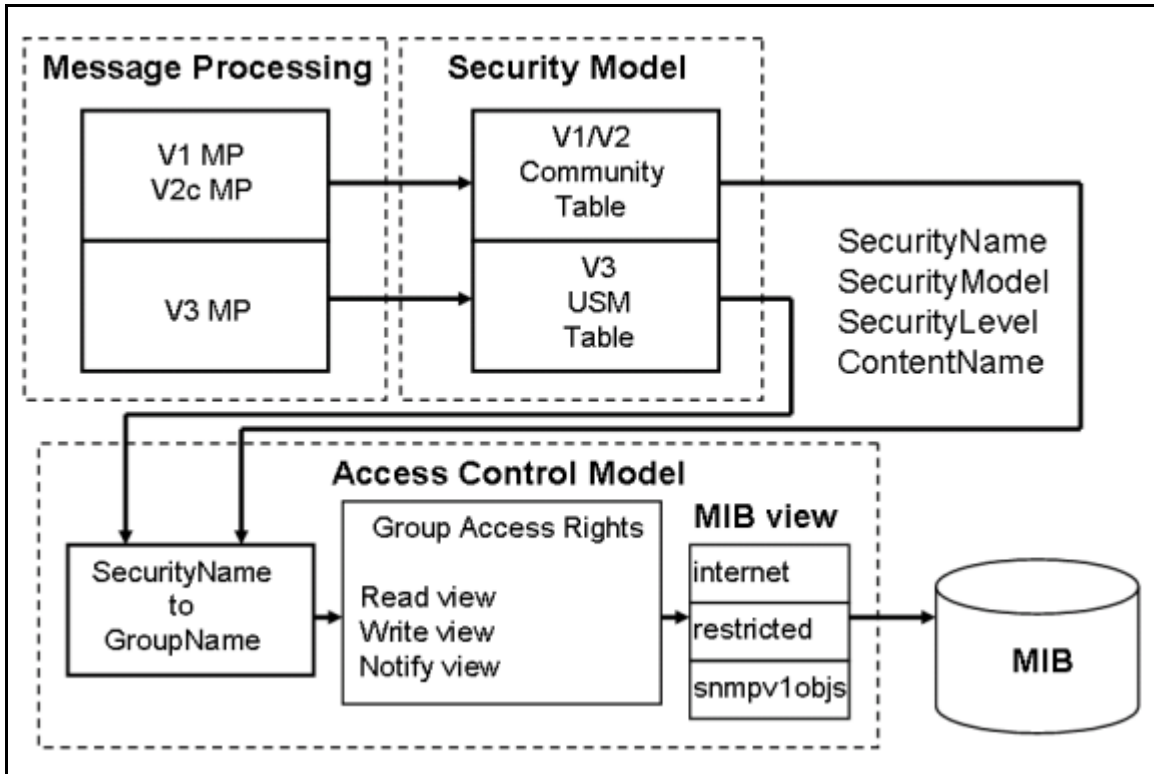
User-based Security Model (USM)

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

The USM security model provides the following levels of communication:

- NoAuthNoPriv
Communication without authentication and privacy
- AuthNoPriv
Communication with authentication and without privacy
- AuthPriv
Communication with authentication and privacy

[Figure 1 on page 25](#) shows the relationship between USM and View-based Access Control (VACM).

Figure 1 USM association with VACM

View-based Access Control (VACM)

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

VACM is the standard access control mechanism 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.

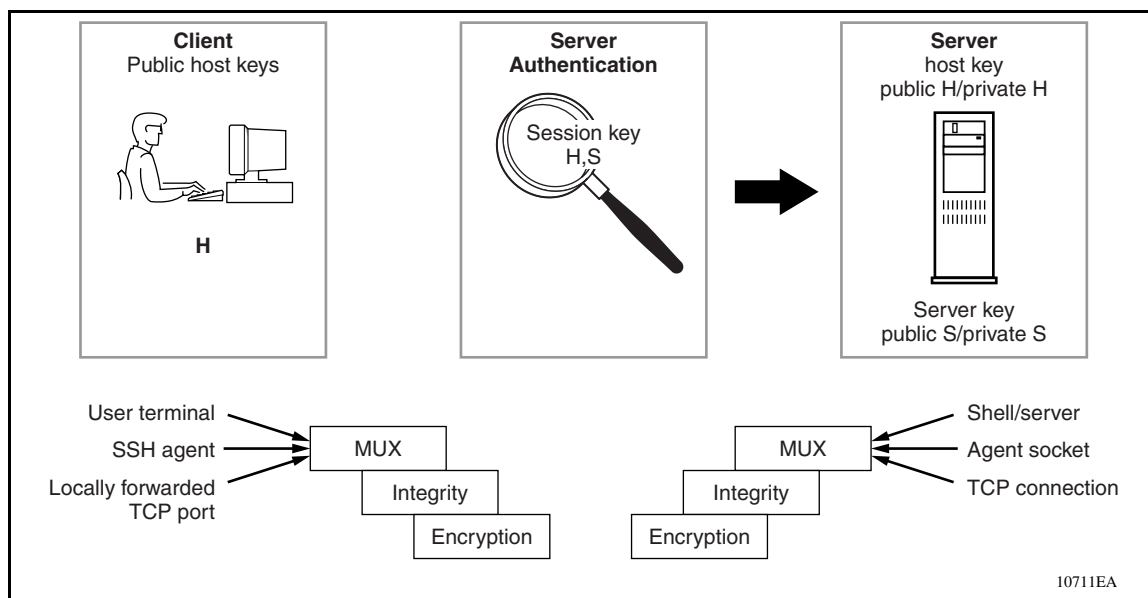
Secure Shell and Secure Copy

Secure Shell (SSH) is a client/server protocol that allows you to conduct secure communications over a network. SSH supports a variety of the 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.

Secure CoPy (SCP) is a secure file transfer protocol. SCP replaces remote access utilities such as FTP with an encrypted alternative.

Figure 2 shows 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 provides strong authentication and secure communication over a non-secure network. The SSH protocol offers protection from the following security risks:

- IP spoofing
- IP source routing

- DNS spoofing
- man-in-the-middle/TCP hijacking attacks (interception of cleartext passwords and other data by intermediate hosts, or manipulation of data by people in control of intermediate hosts)
- 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 — identifies the SSH client. During the login process the SSH client is queried for a digital proof of identity.
Supported authentications are RSA (SSH v1), DSA (SSH v2), and passwords (both SSH v1 and SSH v2).
- Encryption — The SSH server uses encryption algorithms to scramble data and render 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 the alteration.



Note: Currently, 3DES is the only encryption algorithm supported for the 8000 series Ethernet Routing 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 does not function properly without the use of this image.

The implementation of the SSH server in the 8000 series Ethernet Routing Switch enables the SSH client to make a secure connection to an 8000 series Ethernet Routing Switch, and will work with commercially available SSH clients.



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

SSH version 2 (SSH v2)

SSH protocol, version 2 (SSH v2) is a complete rewrite of the SSH v1 protocol. SSH v1 contains multiple functions in a single protocol. SSH v2 divides the functions 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, 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 on page 29](#) shows SSH v2 protocols. [Figure 4 on page 29](#) shows SSH user authentication protocol. [Figure 5 on page 30](#) shows SSH connection protocol.

Figure 3 SSH v2 protocols

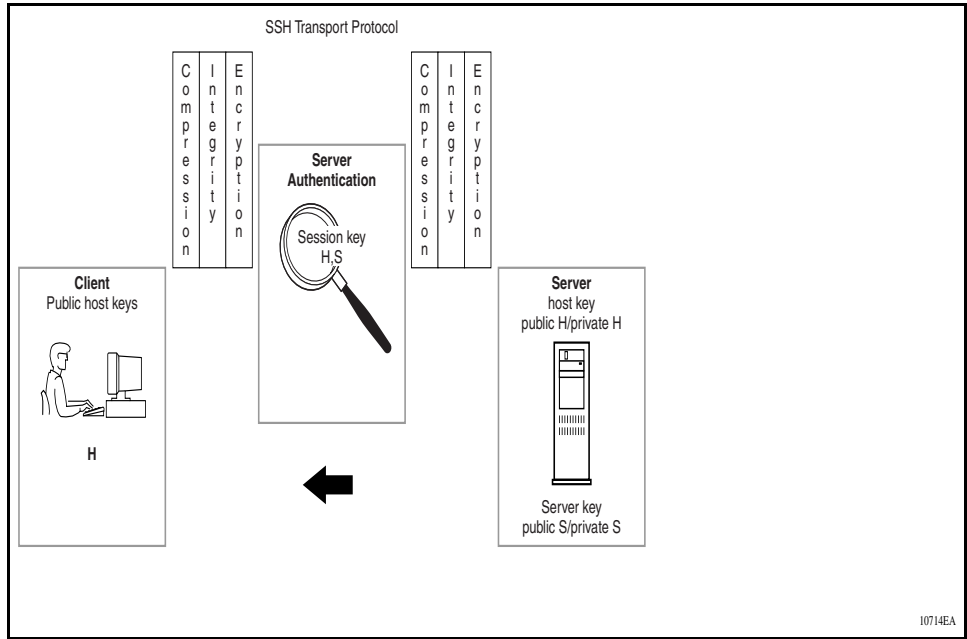


Figure 4 SSH user authentication protocol

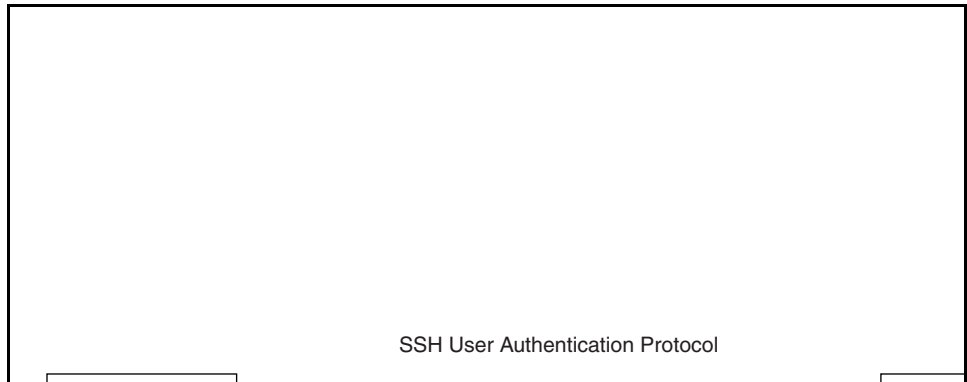
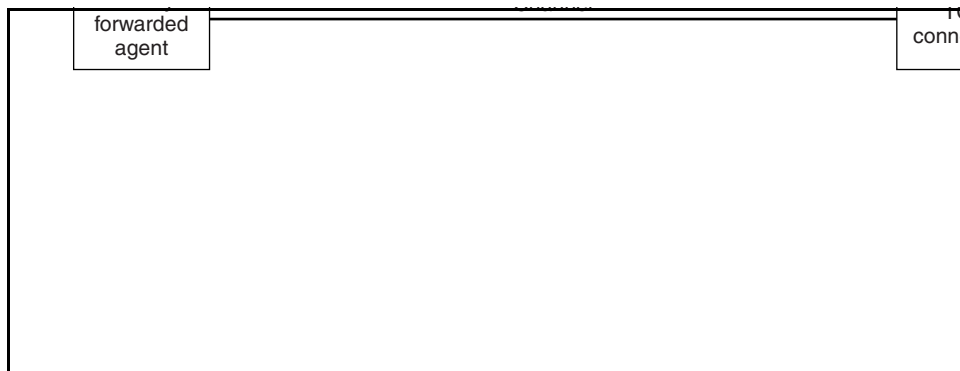


Figure 5 SSH connection protocol

The modular approach of SSH v2 offers improvements to the security, performance, and portability of the SSH v1 protocol.



Note: The SSH v1 and SSH v2 protocols are not compatible. While the SSH implementation in the 8000 series Ethernet Routing Switch supports both versions of SSH, Nortel recommends use of the SSH v2 protocol because it is more secure than SSH v1.

SSH guidelines

The following section provide guidelines for implementing SSH:

- [“Key generation and removal](#)
- [“Block SNMP” on page 31](#)
- [“SCP command” on page 31](#)

Key generation and removal

Generating keys requires that you have free space on the flash. A typical configuration requires less than 2 KBytes 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. If you receive the error message, you must delete unused files and re-generate the key.

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

Block SNMP

The boot flag setting for `block-snmp` (`config bootconfig flags block-snmp <true/false>`) and the runtime config `SSH secure` (`config sys set ssh enable <true/false/secure>`) each modify the `block-snmp` boot flag. If you enable `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`, first disable `SSH secure` mode.

SCP command

Nortel recommends that you use short filenames with the `SCP` command. The entire `SCP` command, including all options, usernames, and filenames should never exceed 80 characters.

RADIUS

Remote Access Dial-In User Services (RADIUS) is a distributed client/server system that assists in securing networks against unauthorized access, allowing a number of communication servers and clients to authenticate users' identities 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 [RFC 2865] and accounting [RFC 2866]). The Ethernet Routing Switch 8300 uses RADIUS authentication and accounting to:

- secure access to the switch using Telnet, rlogin, or the console port
- track the management sessions (CLI only)

This section includes the following topics:

- [“How RADIUS works,”](#) next
- [“Configuring the RADIUS server”](#) on page 32
- [“Configuring the RADIUS client”](#) on page 33
- [“RADIUS authentication”](#) on page 34

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
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 RADIUS process includes:

- RADIUS authentication, which allows you to identify remote users before you give them access to a central network site.
- RADIUS accounting, which enables data collection on the server during a remote user's dial-in session with the client.

Configuring the RADIUS server

The Ethernet Routing Switch 8300 software supports BaySecure Access Control (BSAC* — now known as the Steel-Belted Radius server (SBR)), Merit Network, and freeRadius servers. For instructions on installing the BSAC, Merit Network, or freeRadius server software on the server that you use, see the installation manual that came with your software. After the software is installed, you must make changes to one or more configuration files for these servers. For detailed information about the changes that must be made for the BSAC, Merit Network, or freeRadius server, see [Chapter 6, “Setting up RADIUS servers,” on page 109](#).

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

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

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

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

Configuring the RADIUS client

You use the Ethernet Routing Switch 8300 CLI, the NNCLI, or Device Manager to configure the RADIUS client so that it can contact its RADIUS server. To configure the client, you must:

- Enable RADIUS.
- Configure the IP address of the RADIUS server to be used.
- Configure the shared secret. This secret must match the one defined in the RADIUS server.
- Configure the access priority attribute value. This value must match the type value set in the dictionary file on the RADIUS server. The default value (192) is the recommended value.
- Configure the order or priority in which the RADIUS server is used (if you have more than one RADIUS server in the network).

- Set the UDP port that will be used by the client and the server during the authentication process. The UDP port between the client and the server must have the same value. For example, if the server is configured with UDP 1812, then the client must use the same UDP port value.

RADIUS authentication

RADIUS authentication allows a remote server to authenticate users attempting to log in. 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.

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 four characters in the string form a random number in hexadecimal format. The last eight characters in the string indicate, in hexadecimal format, the number of user sessions started since reboot.

The Network Access Server (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	<ul style="list-style-type: none"> • <i>Accounting on</i> request: Network Access Server (NAS) • IP address.
Accounting is turned off at router	<ul style="list-style-type: none"> • <i>Accounting off</i> request: NAS IP address.
User logs in	<ul style="list-style-type: none"> • <i>Accounting start</i> request: NAS IP address • Session Id • Username
More than 40 CLI commands are executed	<ul style="list-style-type: none"> • <i>Accounting Interim</i> request: NAS IP address • Session Id • CLI commands • Username
User logs off	<ul style="list-style-type: none"> • <i>Accounting Stop</i> request: NAS IP Address • Session Id • Session duration • Username • number of octets input for session • number of octets output for session • number of packets input for session • number of packets output for session • CLI commands

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

- If the server sends an invalid response, the response is silently discarded and no attempt is made to resend the request.
- 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 ten RADIUS servers for redundancy.

EAPoL

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access control protocol. This protocol is part of the IEEE 802.1x standard, which defines port-based network access control. EAPoL provides security by preventing users from accessing network resources before they have been authenticated. Without authentication, any user can access a network to assume a valid identity and access confidential material, or launch Denial of Service (DOS) attacks.

EAPoL allows you to set up network access control on internal LANs and to exchange authentication information between any end station or server connected to the Ethernet Routing Switch 8300 and an authentication server (such as a RADIUS server). This security feature extends the benefits of remote authentication to internal LAN clients. For example, if a new client PC fails the authentication process, EAPoL prevents it from accessing the network.

This section includes the following topics:

- [“EAPoL terminology,”](#) next
- [“Standard 802.1x configuration \(single supplicant per port\)”](#) on page 37
- [“EAPoL static-based security mode”](#) on page 41
- [“Non-standard 802.1x guest VLAN”](#) on page 43
- [“Enabling multiple EAPoL sessions per port”](#) on page 48
- [“EAPoL dynamic VLAN assignment”](#) on page 56
- [“Working with RADIUS”](#) on page 60
- [“RADIUS configuration prerequisites for EAPoL”](#) on page 61
- [“System requirements”](#) on page 66

EAPoL terminology

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

- Supplicant, which is a device, such as a PC, that applies for access to the network.
- Authenticator, which is software on the Ethernet Routing Switch 8300 that authorizes or rejects a supplicant attached to the other end of a LAN segment.

- Authentication Server, which is a RADIUS server that provides authorization services to the authenticator.
- Port Access Entity (PAE), which is software that controls each port on the switch. The PAE, which resides on the Ethernet Routing Switch 8300, supports the authenticator and supplicant functionalities.
- Controlled port, which is any port on the switch with EAPoL enabled.

Standard 802.1x configuration (single supplicant per port)

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

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

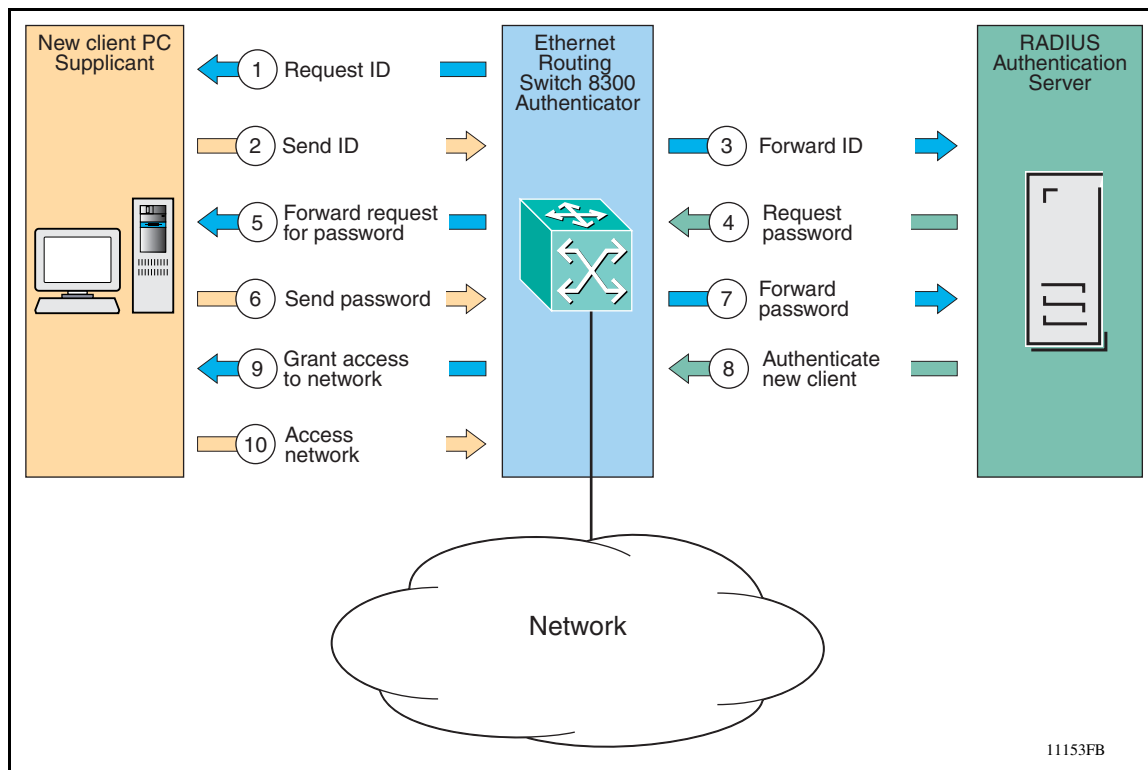
The Ethernet Routing Switch 8300 transmits and receives EAPoL frames, regardless of whether the port is authorized or unauthorized. Non-EAPoL frames are transmitted according to the rules below:

- If authentication succeeds, the controlled port's operational state is set to Forwarding. This means that all the incoming and outgoing traffic is allowed through the port.
- If authentication fails, the controlled port forwards traffic according to how you configure the port's traffic control. The traffic control command can have one of the following two values:
 - Incoming and Outgoing—All non-EAPoL frames received on the controlled port are discarded, and the controlled port's state is set to Blocking.
 - Incoming—All non-EAPoL frames received on the port are discarded, but transmit frames are forwarded through the port.

Configuration example

Figure 6 illustrates an EAPoL standard packet path between a supplicant, the authenticator (Ethernet Routing Switch 8300), and the RADIUS server

Figure 6 EAPoL standard 802.1x packet path example



In the above example, the Ethernet Routing Switch 8300 uses the following steps to authenticate a new client:

- 1** The Ethernet Routing Switch 8300 detects a new connection on one of its EAPoL-enabled ports and requests a user ID from the new client PC.
- 2** The new client sends its user ID to the switch.
- 3** The switch uses RADIUS to forward the user ID to the RADIUS server.
- 4** The RADIUS server responds with a request for the user's password.
- 5** The switch forwards the RADIUS server's request to the new client.

- 6 The new client sends an encrypted password to the switch, within the EAPoL packet.
- 7 The switch forwards the EAPoL packet to the RADIUS server.
- 8 The RADIUS server authenticates the password.
- 9 The switch grants the new client access to the network.
- 10 The new client accesses the network.



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

To operate your Ethernet Routing Switch 8300 in the standard legacy 802.1x security mode, prepare the switch as follows:

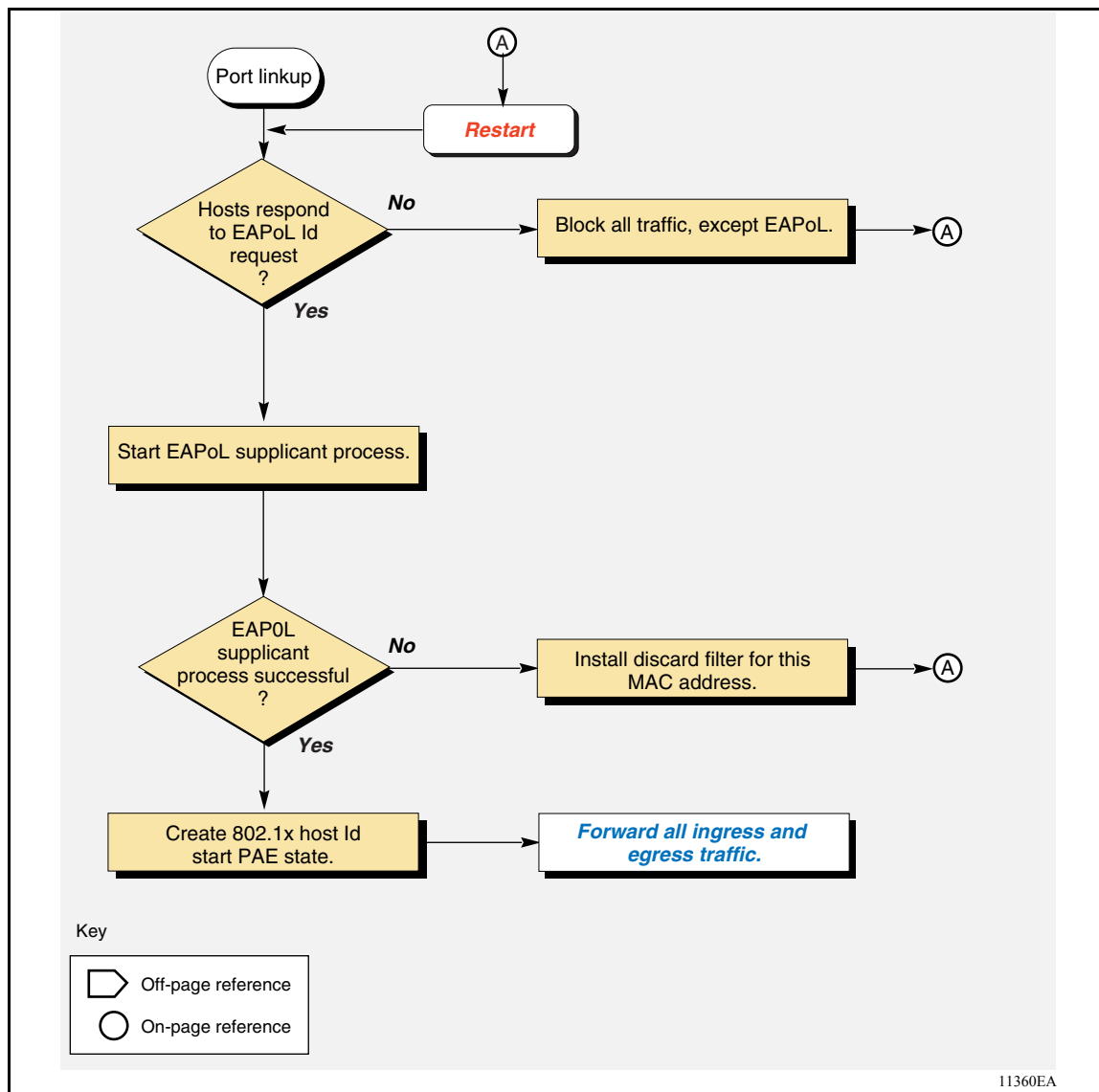
- 1 Globally enable EAPoL on your switch.
- 2 Configure a RADIUS server to include existing user accounts, and set the EAPoL configurations with **usedby** set for each account.
- 3 Set the EAPoL port properties to **Admin-state Auto**.



Note: You cannot enable Guest VLAN or multi-host support while in the standard legacy 802.1x security mode.

[Figure 7 on page 40](#) shows how the Ethernet Routing Switch 8300 responds to a port request when in this operational mode.

Figure 7 Standard 802.1x state machine example



EAPoL static-based security mode

This section describes the configuration prerequisites for operating your Ethernet Routing Switch 8300 in the EAPoL static-based security mode.

When you operate the Ethernet Routing Switch 8300 switch in the EAPoL static-based security mode, the switch allows you to statically add up to eight hosts to the port MAC address table, while maintaining EAPoL security safeguards.

When in this mode, the non-eap-mac feature allows you to override the PAE-state machine.



Note: The EAPoL static-based security mode allows all configured hosts to have complete access to the same broadcast/unicast data on the port.

Port behavior using this type of operational mode resembles that of a shared media concept, where you can insert a hub between the switch port and the hosts. In this mode, you can configure up to eight non-eap-mac hosts. Once enabled, MAC addresses of only eight hosts are learned or allowed. If the Ethernet Routing Switch 8300 senses more than eight hosts, the discard record is set for the new host.

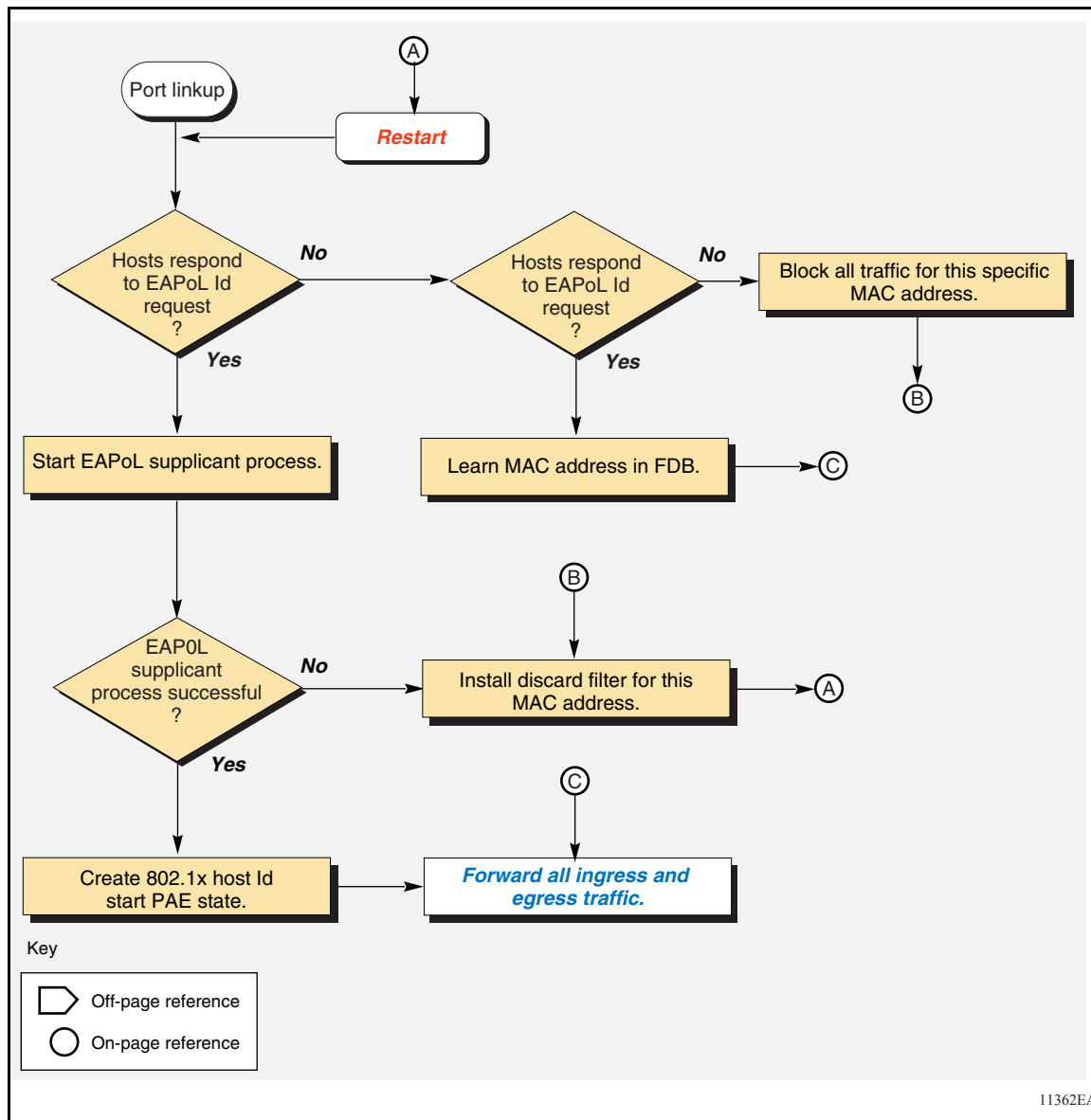
To operate your Ethernet Routing Switch 8300 in the EAPoL static-based security mode, prepare the switch as follows:

- 1 Globally enable EAPoL on your switch.
- 2 Configure a RADIUS server to include existing user accounts, and set the EAPoL configurations with **usedby** set for each account.
- 3 Set the EAPoL port properties to **Admin-state Auto**.
- 4 Disable non-eap-mac and add each MAC address in the format of `XX:XX:XX:XX:XX:XX`.
- 5 Enable non-eap-mac.

The switch is now ready to accept frames from only the specified MACs.

Figure 8 shows how the Ethernet Routing Switch 8300 responds to a port request when in this operational mode.

Figure 8 EAPoL static-based security example



Non-standard 802.1x guest VLAN

This section describes how the Ethernet Routing Switch 8300 allows you to setup a guest VLAN for users connected on EAPoL-enabled ports.

This section includes the following topics:

- [“Guest VLAN,: next](#)
- [“Guest VLAN security mode” on page 45](#)
- [“Configuration guidelines for setting up a guest VLAN” on page 47](#)

Guest VLAN

You can configure the switch to allow users connected on EAPoL-enabled ports to a guest network (with restricted-access until the port is authenticated).

This feature allows network access to users via the *guest* VLAN. A typical application for this scenario is for network partners, who are not currently registered, but can use the guest VLAN to register.

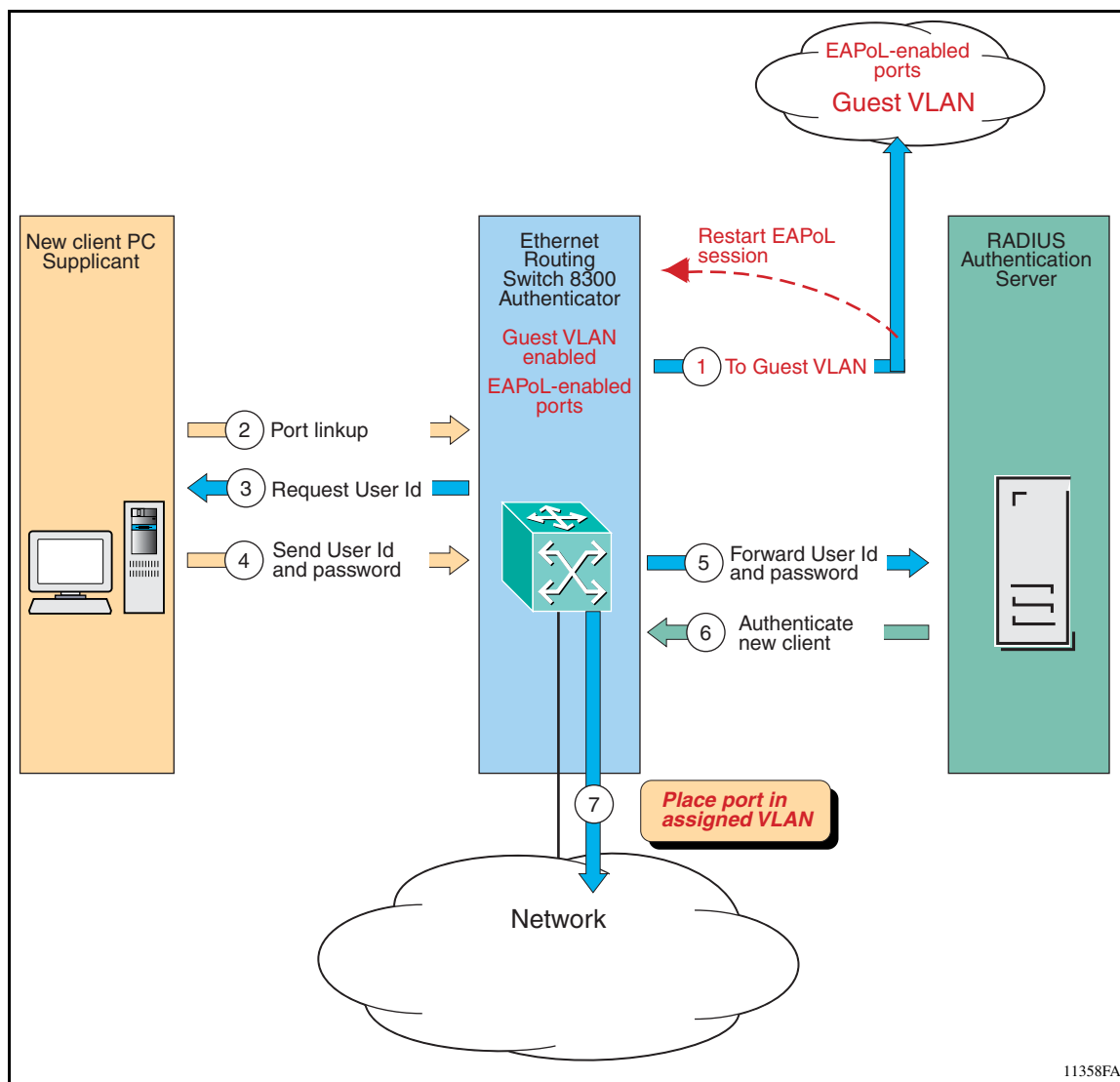


Note: In the following scenario, there is only one user, or one personal computer (PC). The guest VLAN applies to IP telephones and PCs that do not have EAPoL stacks to get to the guest VLAN. If any device, which has been provided guest access, is authenticated, the port moves to the assigned VLAN.

Your Ethernet Routing Switch 8300 uses the following steps to enable the guest VLAN (refer to [Figure 9 on page 44](#)):

- 1 If Guest VLAN is enabled, the Ethernet Routing Switch 8300 moves EAPoL-enabled ports to the guest VLAN (Item 1 in [Figure 9 on page 44](#)).
- 2 When the Ethernet Routing Switch 8300 detects a new connection on one of its EAPoL-enabled ports, the switch requests a user Id from the new client (Item 2 and 3 in [Figure 9 on page 44](#)).

- When the new client replies with a user Id and password, the authenticator sends the information to the RADIUS server for authentication (Item 4 and 5 in Figure 9).
- If the RADIUS server authenticates the new client, the port is placed in the assigned VLAN; otherwise, it remains in the guest VLAN (Item 6 and 7 in Figure 9).

Figure 9 Accessing the guest VLAN

11358FA

Guest VLAN security mode

This section describes the configuration prerequisites for operating the Ethernet Routing Switch 8300 in the EAPoL Guest VLAN security mode. In this mode, only a single untrusted host is supported on EAPoL-enabled ports.

For this operating mode, although the host is untrusted, the Ethernet Routing Switch 8300 allows the host access to the network, as follows:

- 1 If the host responds to an EAPoL Identity Request, the host is treated similar to an 802.1x supplicant and enters the EAP authentication phase.
- 2 If EAPoL authentication is successful, the host is moved to the assigned VLAN.
- 3 If EAPoL authentication fails, or if there is no response to the EAPoL Identity Request, the port is moved to the Guest VLAN.

To operate your Ethernet Routing Switch 8300 in the EAPoL Guest VLAN security mode, prepare the switch as follows:

- 1 Globally enable EAPoL on your switch.
- 2 Set the EAPoL port properties to Admin-state Auto.
- 3 Globally configure Guest VLAN ID on your switch.
- 4 Enable Guest VLAN support on the switch ports.



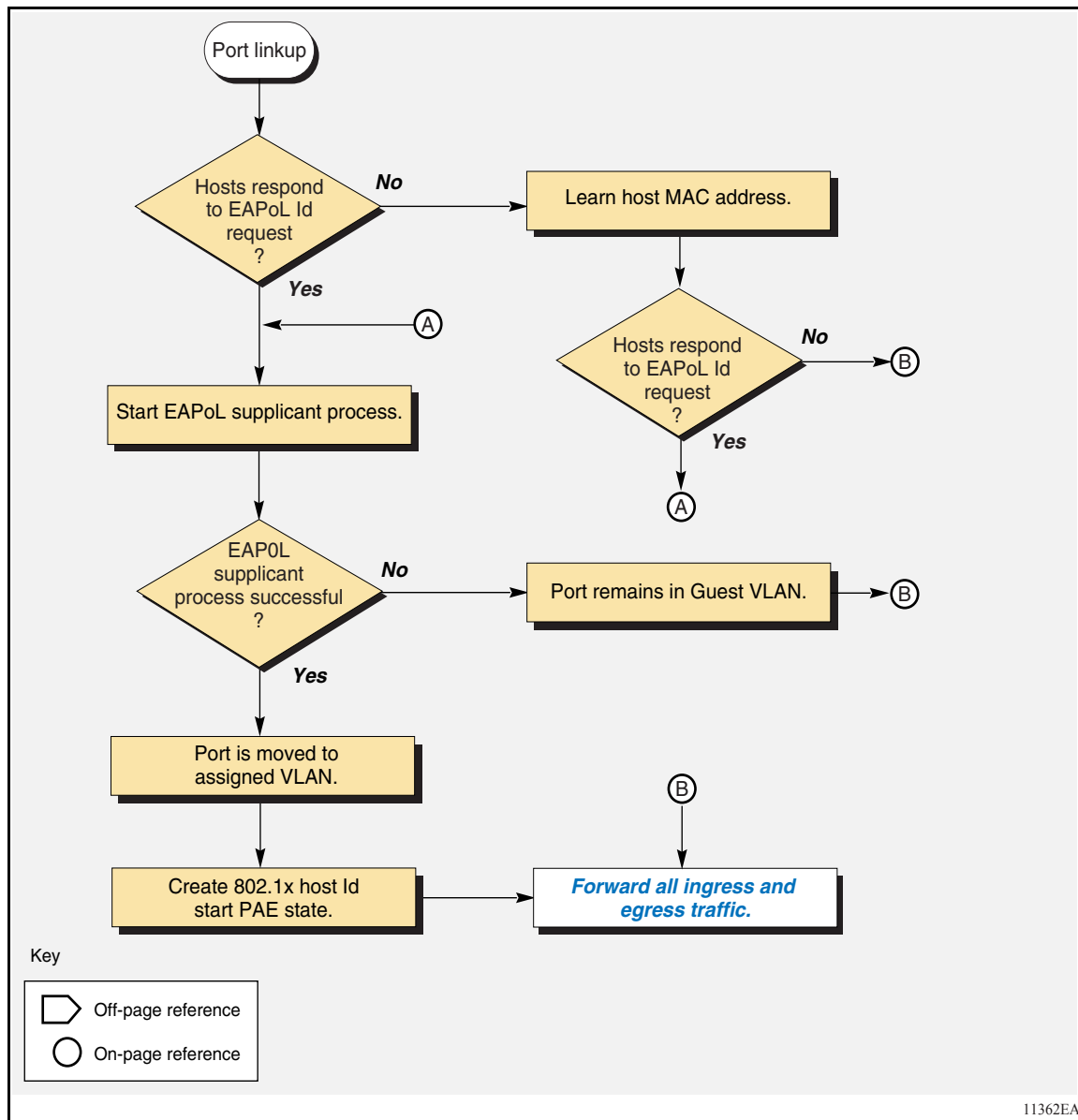
Note: You cannot use Guest VLANs with multihost set to enabled.



Note: The Guest VLAN feature only allows one MAC address to be learned. If a second MAC address is learned, a discard filter is installed for any additional MAC addresses learned by the switch.

Figure 10 shows how the Ethernet Routing Switch 8300 responds to a port request when in this operational mode.

Figure 10 EAPoL Guest VLAN security example



Configuration guidelines for setting up a guest VLAN

- You must configure a global default guest VLAN (refer to [“Configuring a guest VLAN:” on page 48](#)).
- Guest VLAN Support is a per-port option
You can enable Guest VLANs with a valid Guest VLAN Id, per port. If the *local* Guest VLAN Id is not valid, you can still enable Guest VLAN features, as long as the configured *global* Guest VLAN Id is valid.
- The Guest VLAN must be a port-based VLAN.
- The Guest VLAN configuration settings are saved across resets.
- If the port authorization fails, the port is placed back into the Guest VLAN, and an authentication failure error log message is displayed.
- This feature affects ports in the EAP-Auto administrative state. It does not affect ports with force-authorized or force-unauthorized administrative state.
- When the port is EAPoL-enabled:
 - If Guest VLAN is enabled, the port is placed in the Guest VLAN (for example, the port PVID = Guest VLAN Id).
 - If Guest VLAN is not enabled, the port only services EAPoL packets until it is Authenticated. Although the port may be preconfigured with an association with a specific VLAN, only EAPoL packets are processed until Authentication is complete and successful.
 - You cannot modify the Guest VLAN Id on an EAPoL-enabled port with Guest VLAN set to enabled.
- When the port is EAPoL-disabled, the port is placed back into the preconfigured VLAN.
- EAP Authentication:
 - Upon successful Authentication, the port is placed in a preconfigured VLAN or a RADIUS-assigned VLAN.
 - Upon Authentication Failure, if Guest VLAN is enabled, the port will be placed in a Guest VLAN. If Guest VLAN is not enabled, the port only services EAPoL packets.
- Explicit Log Off by the supplicant:
 - If Guest VLAN is enabled, the port is placed in the Guest VLAN (for example, the port PVID = Guest VLAN Id).
 - If Guest VLAN is not enabled, the port only services EAPoL packets.

- ReAuthentication can be enabled for the authMAC address.
If ReAuthentication fails, the port is placed back into the Guest VLAN.

Configuring a guest VLAN:

You can configure guest VLAN using the CLI, NNCLI, and Device Manager.

- To configure a guest VLAN using Device Manager, refer to [Chapter 8, “Configuring EAPoL,”](#) on page 129.
- To configure a guest VLAN using the NNCLI and the CLI, see *Configuring and Managing Security using the NNCLI and CLI* (part number 316804-C).

Enabling multiple EAPoL sessions per port

The multiple EAPoL feature allows for two modes of operation:

- [“Basic EAPoL multihost-based security,”](#) next

When in this operational mode, the Ethernet Routing Switch 8300 supports up to eight EAPoL supplicants on a single switch port. If more than eight EAPoL supplicant are sensed by the Ethernet Routing Switch 8300, the port is shut down and a console message and trap is sent to Device Manager.

- [“Enhanced EAPoL multihost-based security”](#) on page 51

When in this operational mode, the Ethernet Routing Switch 8300 supports up to eight authenticated 802.1x EAPoL supplicants and, in addition, up to eight non-EAPoL MAC-based hosts can be supported on a single switch port.

Basic EAPoL multihost-based security

This section describes the configuration prerequisites for operating the Ethernet Routing Switch 8300 in the Basic EAPoL multihost-based security mode.

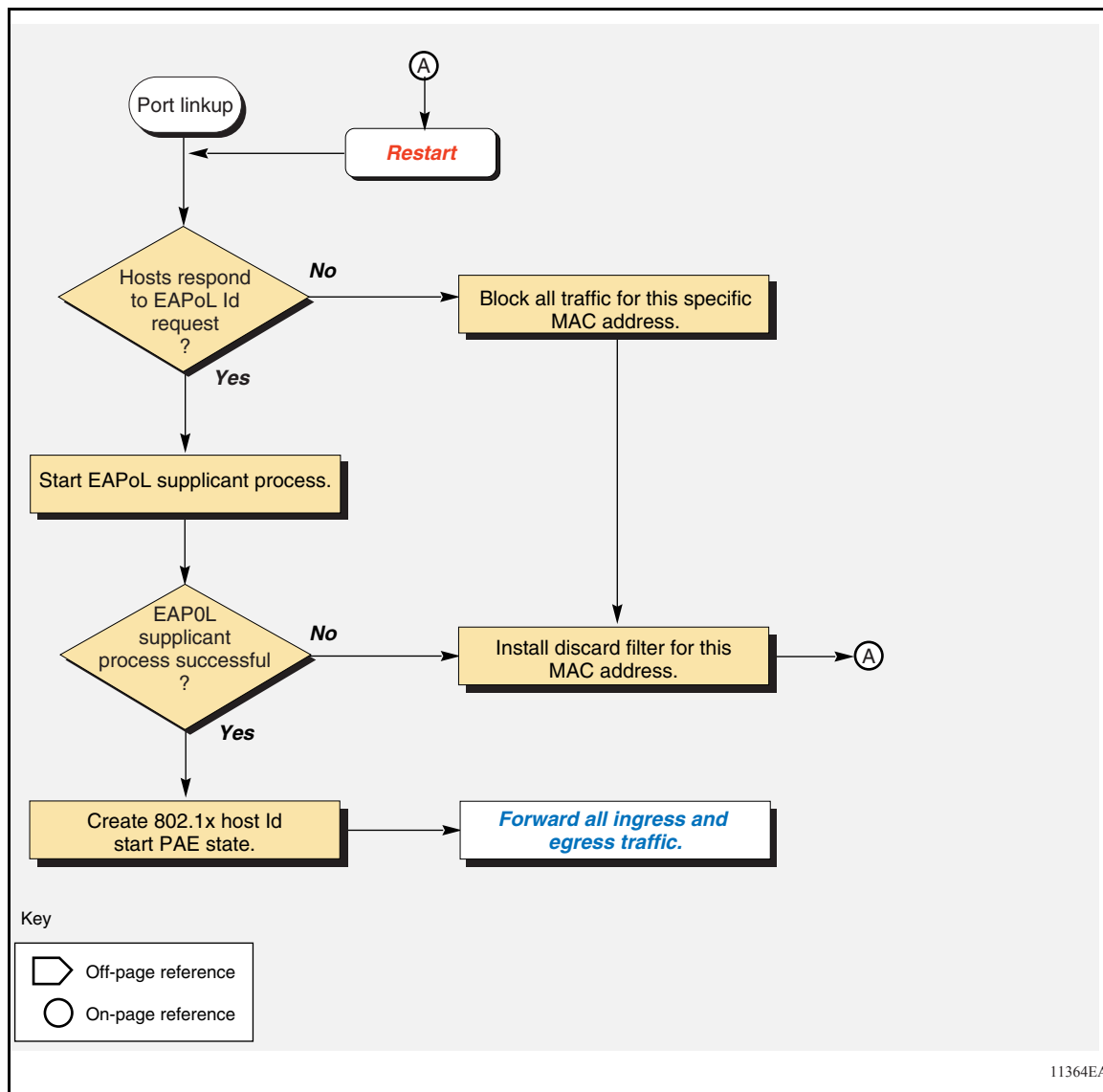
When you operate the Ethernet Routing Switch 8300 in the Basic EAPoL multihost-based security mode, your switch supports up to eight EAPoL supplicants on a single switch port. If the Ethernet Routing Switch 8300 senses more than eight EAPoL supplicants on the port, the port is blocked, a warning message is displayed on the console, and a trap is sent to the Device Manager application.

To operate your Ethernet Routing Switch 8300 in the Basic EAPoL multihost-based security mode, prepare the switch as follows:

- 1 Globally enable EAPoL on your switch.
- 2 Configure a RADIUS server to include existing user accounts, and set the EAPoL configurations with “usedby,” set for each account.
- 3 Set the EAPoL port properties to Admin-state Auto.
- 4 Set the multi-host parameter to enable, and set the max-allowed-hosts value to the desired number of hosts.

[Figure 11 on page 50](#) shows how the Ethernet Routing Switch 8300 responds to a port request when in this operational mode.

Figure 11 Basic EAPoL multihost-based security example



Enhanced EAPoL multihost-based security

You can configure your Ethernet Routing Switch 8300 to allow multiple EAPoL clients and non-EAPoL clients to be connected on the same EAPoL-enabled port. Each client has to be authenticated before it can access the network.

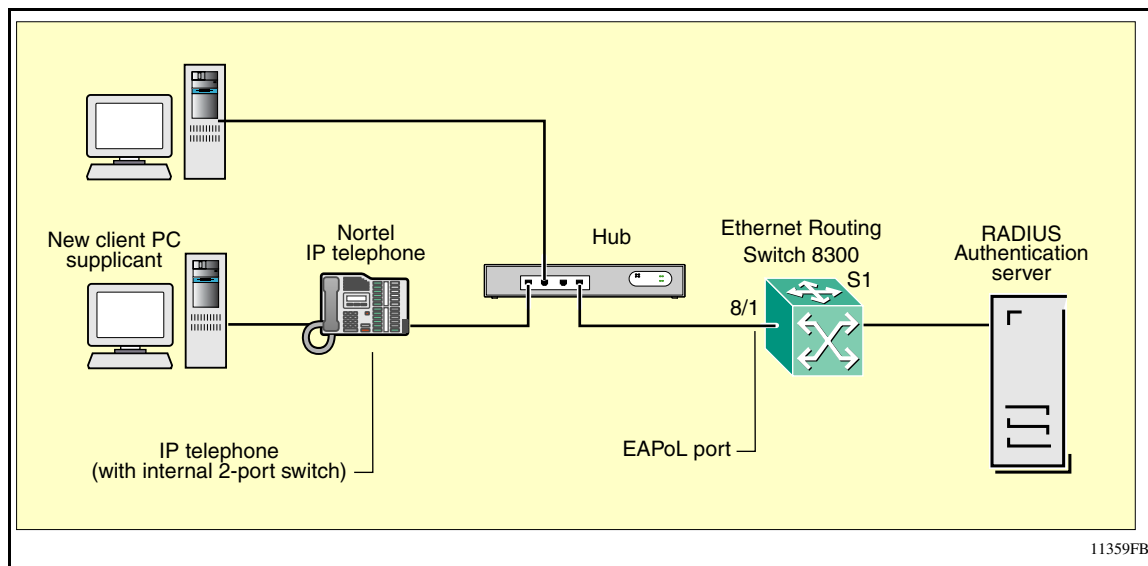
Traffic from unauthorized hosts is allowed on the controlled port as long as there is one authorized host on that port. To restrict network access for non-EAPoL clients, you add only the MAC addresses of trusted clients to the allowed MAC address list. Traffic from all other clients, whose MAC address is not present in the allowed MAC address list, is discarded.

This section includes the following topics:

- [“Multiple EAPoL client example,”](#) next
- [“Prerequisites for using the Enhanced multihost-based security mode”](#) on page 52
- [“Configuration guidelines for setting up multiple EAPoL sessions per port”](#) on page 55

Multiple EAPoL client example

A typical application for this feature is a 2-port switch included in an IP telephone, which provides connectivity for the IP phone and the connected station (refer to [Figure 12 on page 52](#)).

Figure 12 Multiple EAPoL client example

11359FB

Prerequisites for using the Enhanced multihost-based security mode

This section describes the configuration prerequisites for operating the Ethernet Routing Switch 8300 in the Enhanced EAPoL Multihost-based security mode.

When you operate the Ethernet Routing Switch 8300 in the EAPoL Multihost-based security (with EAPoL MAC-based security) mode, you can add up to eight authenticated 802.1x supplicants on a single switch port and, in addition to the eight authenticated 802.1x supplicants, you can add up to eight more non-EAPoL MAC-based hosts.

This port behavior is similar to the shared media concept, where you can connect a hub or an IP telephone to the switch port. This mode is designed with IP Telephone in mind, where you can have a non-EAPoL IP Telephone and a non-EAPoL supported host. If the IP Telephone does not support EAP authentication, you must enter the IP Telephone's MAC address in the "allow non-eap-mac" table. If the IP Telephone does support EAPoL, then the remaining eight non-EAPoL MAC-based hosts can be any host-type desired.

When in this mode, a new non-eap-mac feature allows you to override the PAE state machine.



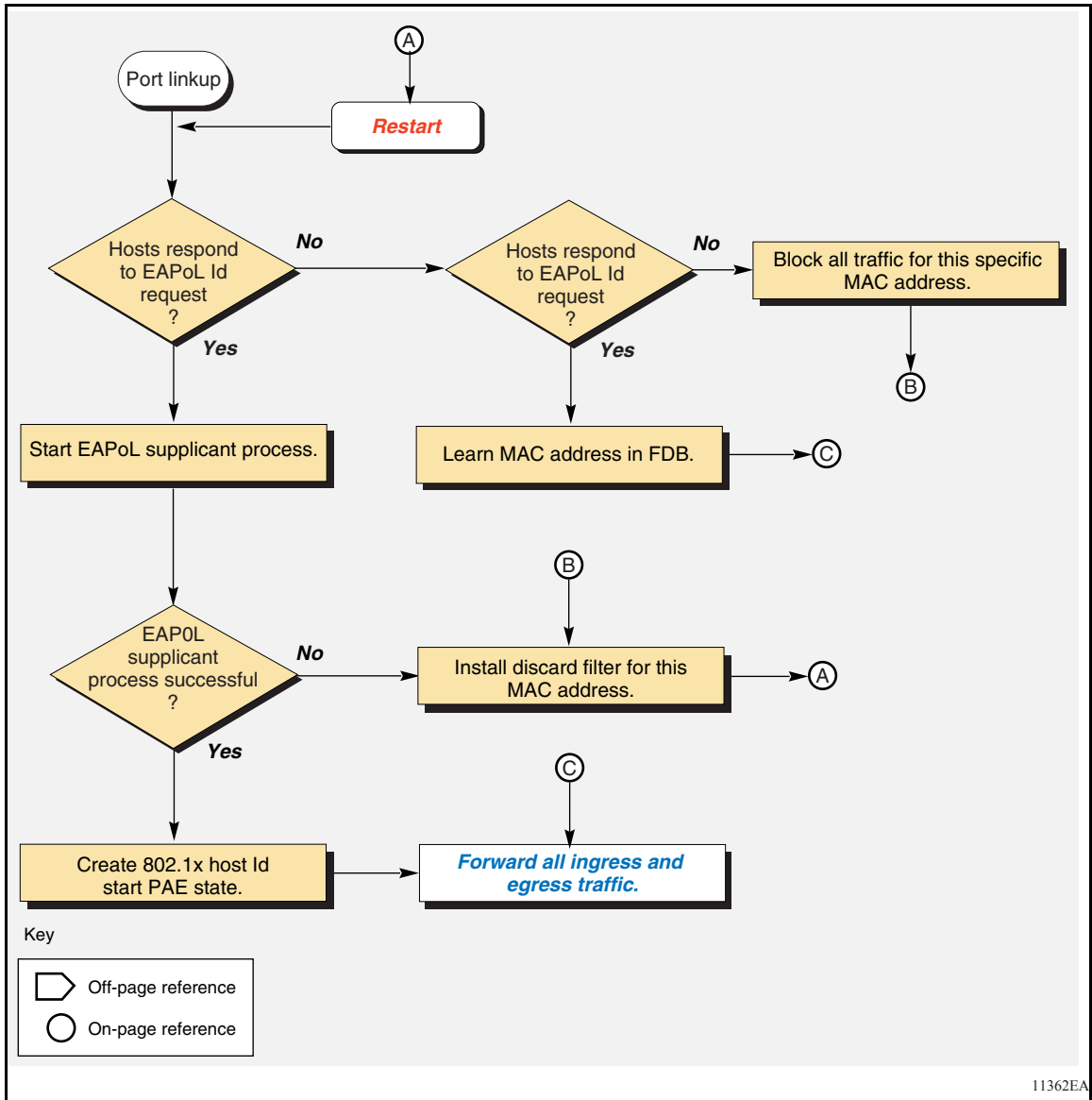
Note: This mode allows all configured hosts to have complete access to the same broadcast/unicast data on this port.

To operate the Ethernet Routing Switch 8300 in the EAPoL Multihost-based security (with EAPoL MAC-based security) mode, prepare the switch as follows:

- 1 Globally enable EAPoL on your switch.
- 2 Configure a RADIUS server to include existing user accounts, and set the EAPoL configurations with “usedby,” set for each account.
- 3 Set the EAPoL port properties to Admin-state Auto.
- 4 Set Multi-host to enable and define the maximum number of hosts desired for this port.
- 5 Disable allow-non-eap-mac and add up to eight non-eap-mac MAC addresses in the format of xx:xx:xx:xx:xx:xx.
- 6 Enable allow-non-eap-mac.

[Figure 13 on page 54](#) shows how the Ethernet Routing Switch 8300 responds to a port request when in this operational mode.

Figure 13 Enhanced EAPoL multihost-based security example



Configuration guidelines for setting up multiple EAPoL sessions per port

The following list provides configuration guidelines for setting up multiple EAPoL sessions per port:

When multiple hosts is enabled per port:

- Upon the first successful authentication:
 - Only EAPoL packets and data from the allowed MAC address is allowed on that port.
 - As subsequent authentications complete, those MAC addresses are allowed as well. Only a predefined maximum number of authenticated users (MAC addresses) are allowed on a port.
- If `allow-non-eap-clients` is disabled on the port, any traffic coming from non-EAPoL MAC addresses is discarded.
- If `allow-non-eap-clients` is enabled on the port, the MAC Address is checked against the list of allowed-MAC addresses in the non-eap-mac list. If the MAC Address is not in the list, the traffic to and from the MAC address is discarded.
- The default value for multiple authenticated host support, and non EAPoL clients is 1.
 - The maximum number of multiple authenticated clients that you can configure on a port is eight.
 - The maximum number of non-authenticated clients that you can configure on a port is eight.
- When the port is configured for multiple authentications, the control directions state machine is disabled.
- When the port is configured for multiple authentications, dynamic VLAN assignment from RADIUS is disabled.

When multiple hosts is disabled per port:

- All MAC addresses created by EAPoL with discard bits set are deleted.

When EAPoL is disabled on the port:

- All MAC addresses created by EAPoL with discard bits set are deleted.

Configuring multiple EAPoL sessions per port:

You can configure multiple EAPoL sessions per port using the NNCLI, CLI, and Device Manager.

- To configure multiple EAPoL sessions using Device Manager, refer to [Chapter 8, “Configuring EAPoL,” on page 129](#).
- To configure multiple EAPoL sessions using the NNCLI or CLI, see *Configuring and Managing Security using the NNCLI and CLI* (part number 316804-C).

EAPoL dynamic VLAN assignment

If EAPoL is enabled on a port, and then the port is authorized, the EAPoL feature dynamically changes the port’s VLAN configuration according to preconfigured values, and assigns a new VLAN. The new VLAN configuration values are applied according to previously stored parameters (based on the user_id) in the RADIUS server.

The following VLAN configuration values are affected:

- PVID
- Port priority

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

The following exceptions apply to dynamic VLAN assignments:

- Dynamic VLAN assignment is not supported in multihost mode.
- The dynamic VLAN configuration values assigned by EAPoL are **not** stored in the switch’s NVRAM.
- You can override the dynamic VLAN configuration values assigned by EAPoL; however, be aware that the values you configure are not stored in NVRAM.
- When EAPoL is enabled on a port, and you configure values other than VLAN configuration values, those values are applied and stored in NVRAM.

- You cannot enable EAPoL on tagged ports or MLT ports.
- You cannot change the VLAN/STG membership of EAPoL authorized ports.

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

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

RADIUS MAC centralization

This feature allows the centralization of MAC addresses for non-EAP clients (typically IP phones). An enable/disable flag is provided at the system level to globally enable/disable the RADIUS MAC centralization feature. Enabling RADIUS MAC centralization at port level takes effect only if the global flag is enabled.

Multiple clients can be connected to an EAP-enabled port (with multi-host feature enabled). Each of these clients must be authenticated to gain access to the network.

With `allow-non-eap-clients` enabled, traffic from the unauthorized host is allowed on the port. To restrict access to the non-EAP clients, the MAC address of that client must be added to the non-EAP MAC list. Traffic from clients that do not have a MAC address in the non-EAP MAC undergo RADIUS-based MAC authentication.



Note: To restrict access to the non-EAP clients, the MAC address (username) of the client that is to be allowed access to the network, and its corresponding password must be configured on the RADIUS server.

For a non-EAP client to be authenticated with RADIUS-based MAC authentication, an Access-Request packet is sent to the RADIUS server with the username and password attributes. The username is the MAC address of the non-EAP host. The password is a string composed of the following, and in this order:

- source-IP (configured using the `config radius server create <IP> secret <key> usedby eapol source-IP <IP>` command)
- MAC address of the non-EAP host
- slot number and port through which the non-EAP host is connected to the switch



Note: If the source IP is not configured, the IP address 0.0.0.0 is used in the password string (password string contains 000000000000 as the IP string).

The generated password is encrypted using MD5 hashing before sending the Access-Request packet to the radius server. If an entry is present for the non-EAP user, then the RADIUS server authenticates the user by sending an Access-Accept packet to the switch.

Traffic from a non-EAP client that does not have a MAC address present in the non-EAP MAC, and that cannot be authenticated by the RADIUS server, is discarded and a log message is generated.

The user can configure the number of non-EAP clients allowed for each port by configuring `max-non-eap-clients`. The `max-non-eap-clients` is the sum of the number of non-EAP clients statically configured in the allowed list and the number of non-EAP clients authenticated/rejected/pending by the RADIUS server.

The `config ethernet <slot/port> eapol non-eap-mac shut-down-on-intrusion enable/disable` CLI command allows the user to choose whether to shutdown the port when the `max-non-eap-clients` limit is reached, and the current number of EAP sessions has reached the maximum number of EAP sessions configured. By default, this option is disabled.

If the user opts for shutdown, when `non-eap-client [max + 1]` is attained, with the maximum number of EAP sessions already reached, the port is shut down by changing the port state from `auto` to `force-unauthorized`. Trap and log messages are also added. If the user opts not to allow shutdown, a discard record is added for the non-EAP client, and trap and log messages are sent.

When RADIUS MAC centralization is enabled, and the `allow-non-eap-mac` feature is enabled, the MAC address of a non-EAP client connecting to the switch is checked against the non-EAP MAC list. There are two possible outcomes:

- If the user's MAC address is found in the non-EAP MAC list, the user is allowed access to the network.
- If the user's Mac address is not in the non-EAP MAC list, an Access-Request packet is sent to the RADIUS server with the username and password attributes. A discard record is added for this MAC address until the RADIUS server authenticates it. The port is in a forwarding state. When a response is received from the RADIUS server, the discard record is either cleared or retained — depending on the result of the authentication.

Upon successful authentication, the user is allowed access to the network. The MAC address is learned on the port. The MAC priority, returned by the RADIUS server, is assigned as the QoS for the non-EAP MAC address.

Dynamic assignment of VLANs is not done for non-EAP clients.

If the RADIUS server cannot authenticate the user, the `src-discard/dst-discard` bits per MAC can be set to drop the intruder MAC. Traffic from non-EAP clients that do not have a MAC address assigned in the non-EAP MAC list, nor in the user configuration file of the RADIUS server, is discarded and a log message is generated.

To view the non-EAP clients and their state (authenticated/rejected/pending), use the `show port info eapol radius-non-eap-mac <slot/port>` command.

If `allow-non-eap-mac` is disabled on the EAP-enabled port, any traffic from non-eap MAC addressees is discarded using `src-discard/dst-discard` bits for the non-eap MAC.

The non-EAP host is re-authenticated every time the MAC address is learned. If the switch encounters the an identical MAC address from another port, the non-EAP host must be re-authenticated on the port on which it was originally authenticated.

When RADIUS MAC centralization is disabled, but the `allow-non-eap-mac` feature is enabled, the MAC address of a non-EAP client connecting to the switch is checked against the non-EAP MAC list. There are two possible outcomes in this case:

- If the user's MAC address is found in the non-EAP MAC list, the user is allowed access to the network.
- If the user's MAC address is not in the non-EAP MAC list, the `src-discard/dst-discard` bits per MAC can be set to drop the intruder MAC. Traffic from the non-EAP client whose MAC address is not present in the non-EAP MAC list is discarded.

Working with RADIUS

RADIUS (Remote Access Dial-In User Services) is a distributed client/server system that authenticates users identity through a central database. RADIUS is a fully open and standard protocol, defined by RFCs (Authentication: 2865, Accounting 2866).

In the Ethernet Routing Switch 8300, RADIUS performs the following functions:

- RADIUS authentication lets you identify remote users before you give them access to a central network site.

A RADIUS application has two components, the RADIUS server and the RADIUS client.

The RADIUS server is 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.



Note: Radius accounting is not supported for this release.

The RADIUS client can be a switch, router or a remote access server that is equipped with client software and 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. In the configuration described in this manual (see [Figure 6 on page 38](#)), the RADIUS client software resides on the Ethernet Routing Switch 8300.

RADIUS configuration prerequisites for EAPoL

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

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

Should be encoded by a string. For example, for VLAN 2, Tunnel-Private-Group-Id="2"; for VLAN 10, Tunnel-Private-Group-Id="10".
- Port priority (vendor-specific) attributes
 - Vendor Id: value 562, Nortel Vendor Id and value 1584, Bay Networks Vendor Id

- Attribute Number: value 1, Port Priority
- Attribute Value: value 0 (zero) to 7 (this value is used to indicate the port priority value assigned to the specified user)

RADIUS accounting for EAPoL

Ethernet Routing Switch 8300 supports accounting of EAPoL sessions using RADIUS accounting protocol. A user session is defined as the interval between the instance at which a user is successfully authenticated (port moves to authorized state) and the instance at which the port moves out of the authorized state.

[Table 2 on page 63](#) summarizes the accounting events and the information logged.

Table 2 Summary of accounting events and information logged.

Event	Radius Attributes	Description
User is authenticated by EAPoL and port enters authorized state	Acct-Status-Type	start
	Nas-IP-Address	IP address to represent Ethernet Routing Switch 8300
	Nas-Port	Port number on which the user is EAPoL authorized
	Acct-Session-Id	Unique string representing the session
	User-Name	EAPoL user name
User logs off and port enters un-authorized state	Acct-Status-Type	stop
	Nas-IP-Address	IP address to represent Ethernet Routing Switch 8300
	Nas-Port	Port number on which the user is EAPoL un-authorized
	Acct-Session-Id	Unique string representing the session
	User-Name	EAPoL user name
	Acct-Input-Octets	Number of octets input to the port during the session
	Acct-Output-Octets	Number of octets output to the port during the session
	Acct-Terminate-Cause	Reason for terminating user session. Please see Table 3 for the mapping of 802.1x session termination cause to RADIUS accounting attribute.
	Acct-Session-Time	Session interval

[Table 3 on page 64](#) describes the mapping of 802.1x session termination cause to RADIUS accounting attribute.

Table 3 802.1x session termination mapping

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

Configuring the Ethernet Routing Switch 8300 for EAP and RADIUS

The Ethernet Routing Switch 8300, through which UBP users connect, must be configured to communicate with the RADIUS server to exchange EAP authentication information, as well as user role information. You must specify the IP address of the RADIUS server, as well as the shared secret (a password that authenticates the device with the RADIUS server as an EAP access point). EAP must be enabled globally on each device, and EAP authentication settings must be set on each device port through which EAP/UBP users will connect.

Use the following procedure to set up the Ethernet Routing Switch 8300 for EAP and RADIUS:

- 1 Using the CLI, open a Telnet session.
- 2 Log in to the Ethernet Routing Switch 8300.

- 3** Enter the following command to create a RADIUS server to be used by EAPoL:

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

where:

- *IPaddr* is the IP address of your RADIUS server. This address tells the switch where to find the RADIUS server from which it will obtain EAP authentication and user role information.
 - *secretkey* is the shared secret for RADIUS authentication. The shared secret is held in common by the RADIUS server and all EAP-enabled devices in your network. It authenticates each device with the RADIUS server as an EAP access point. When you configure your RADIUS server, you must use the same shared secret value that you use here.
- 4** Enter the following commands to enable the switch to communicate through EAP, and to globally enable session management:

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



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

- 5** Enter the following commands to enable switch ports for EAP authentication:

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

- 6** Enter the following command to save your changes:

```
save
```

For more information about configuring RADIUS and EAP for the Ethernet Routing Switch 8300, see the appropriate chapters in this manual.

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

System requirements

The following are minimum system requirements for EAPoL:

- Ethernet Routing Switch 8300 running software release 2.1 and higher
- RADIUS server
 - Steel Belted RADIUS* (version 4.7 and 5.0)
 - Microsoft IAS (Windows 2000 SP4)
 - Zone Labs* (Identity Server 5.1)
 - Free RADIUS
- EAP clients (XP/Linux*)
 - Microsoft Windows 2000 SP4
 - Microsoft Windows XP SP2
 - Aegis* (version 2.2.1.27) available on Microsoft Windows 95 and beyond
 - Odyssey Client Manager (version 3.0.3.01194) available on Microsoft Windows 95 and beyond
 - Red Hat* 802.1x supplicant (version 9.0 with the appropriate package)

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

TACACS+

Ethernet Routing Switch 8300 supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a security application implemented as a client/server-based protocol that provides centralized validation of users attempting to gain access to a router or network access server.

TACACS+ differs from RADIUS in two important ways:

- TACACS+ is a TCP-based protocol

- TACACS+ uses full packet encryption, rather than just encrypting the password (RADIUS authentication request)



Note: TACACS+ encrypts the entire body of the packet, but uses a standard TACACS+ header.

TACACS+ provides management of users who access a device through any of the management channels: Telnet, rlogin, FTP, SSH v1, and SSH v2.

During the login process, TACACS+ client initiates TACACS+ authentication and authorization sessions with the server.



Note: Prompts for login and password occur prior to the authentication process. If both RADIUS and TACACS+ authentication are enabled, TACACS+ authentication always occurs before RADIUS authentication. If TACACS+ fails because there are no valid servers, then the username and password are used for RADIUS authentication. If RADIUS also fails, then the username and password are used for the local database. (That is, authentication is always attempted in the following order: TACACS+, RADIUS, the local database.)

If TACACS+ returns an access denied packet, then the user is offered a new authentication attempt (login/password prompts are re-issued — the authentication process is not passed to RADIUS).

TACACS+ architecture

You can configure TACACS+ on the Ethernet Routing Switch 8300 using the following methods:

- Connect the TACACS+ server through a local interface (see [Figure 14 on page 68](#)). Management PCs can reside on the out-of-band management port, serial port, or on the corporate network. The TACACS+ server is placed on the corporate network so that it can be routed to the Ethernet Routing Switch 8300.
- Connect the TACACS+ server through the management interface using an out-of-band management network (see [Figure 15 on page 68](#)).

Figure 14 Connecting the TACACS+ server through a local interface

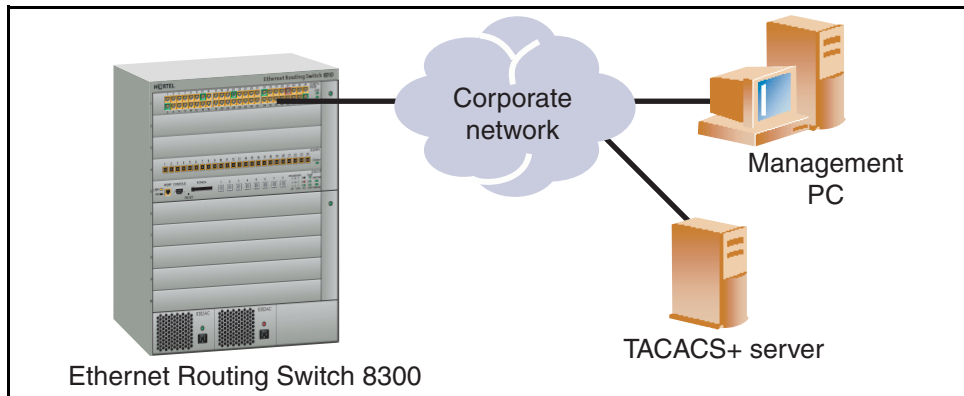
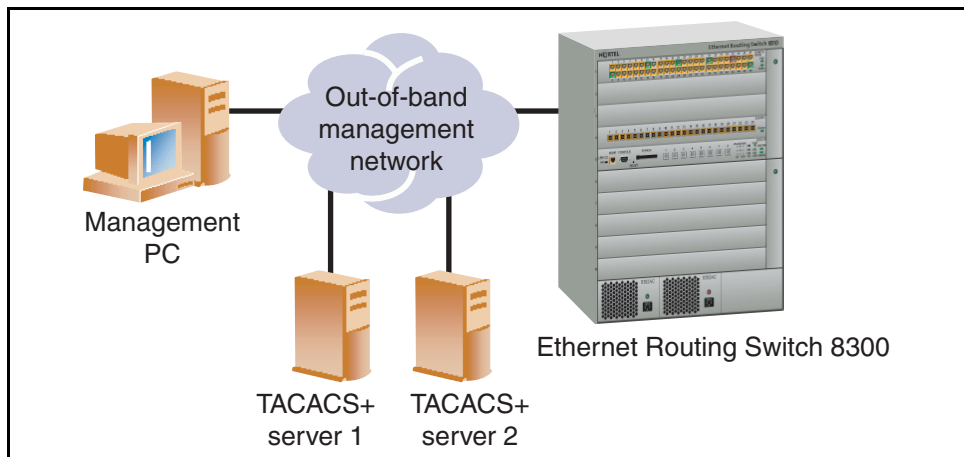


Figure 15 Connecting the TACACS+ server through the management interface



Multiple TACACS+ servers can be configured for backup authentication in both the local interface and out-of-band management network scenarios. The primary authentication server will be determined by server priority.

TACACS+ authentication

TACACS + authentication offers complete control of authentication through login/password dialog and response. The authentication session provides username/password functionality.

TACACS+ authorization

The transition from TACACS+ authentication to authorization phase is transparent to the user. Upon successful completion of the authentication session, an authorization session starts with the authenticated username. The authorization session provides access level functionality.

TACACS+ access levels

TACACS+ supports six Ethernet Routing Switch 8300 access levels. [Table 4](#) shows the scheme used to map the access levels to TACACS+ privilege levels.

Table 4 Ethernet Routing Switch 8300 access levels

Ethernet Routing Switch 8300 access level	Privilege level
None (0)	0
READ ONLY (1)	1
L1 READ WRITE (2)	2
L2 READ WRITE (3)	3
L3 READ WRITE (4)	4
READ WRITE (5)	5
READ WRITE ALL (6)	6



Note: This version of TACACS+ does not support any other TACACS+ arguments in authorization requests, such as `cmd`, `cmd-arg`, `acl`, `zonelist`, `addr`, `routing`, and so on. If you attempt to configure any argument in authorization requests (other than access level and privilege level), the TACACS+ request is dropped by the switch and an error is recorded to system log.

Chapter 2

Setting passwords, locking ports, and viewing SNMP errors

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

Topic	Page
Controlling access to the CLI	71
Locking a port	75
Viewing SNMP errors	75

Controlling access to the CLI

If you have read/write/all access authority using SNMPv1 or SNMPv2c, you can use Device Manager to change the passwords for access to the CLI through a console or Telnet session. Please note that the user name and password fields are blank for security reasons.



Note: With SNMPv3, read/write/all access level does not exist. If you attempt to change a user name and password, an Authorization error appears. You can change the following fields: MaxTelnet Sessions, MaxRloginSessions, and Timeout.



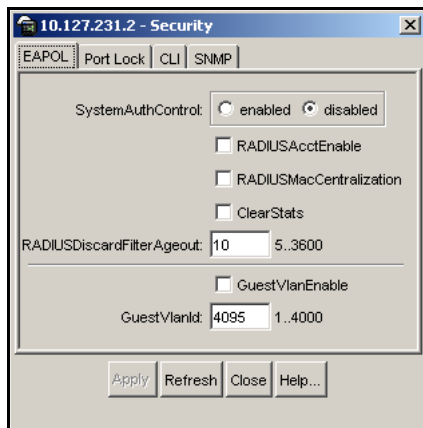
Caution: For security reasons, Nortel recommends that you set the passwords to values other than the factory defaults.

To change passwords for access to the CLI:

- 1 Select **Edit > Security > General** from the Device Manager menu bar.

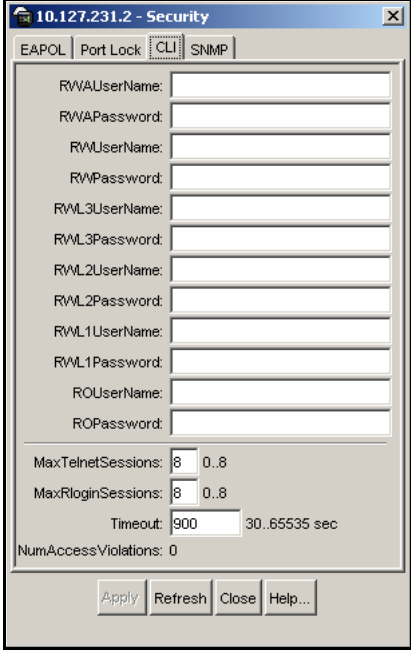
The **Security** dialog box opens with the **EAPOL** tab selected. (Figure 16).

Figure 16 Security dialog box—EAPOL tab



- 2 Click the **CLI** tab.

The **CLI** tab opens (Figure 17 on page 73).

Figure 17 Security dialog box—CLI tab top part

The screenshot shows a window titled "10.127.231.2 - Security" with a close button (X) in the top right corner. The window has four tabs: "EAPOL", "Port Lock", "CLI", and "SNMP". The "CLI" tab is selected. The dialog box contains several text input fields for usernames and passwords, followed by numeric input fields for session limits and a timeout value, and a read-only field for access violations. At the bottom, there are four buttons: "Apply", "Refresh", "Close", and "Help...".

RWAUserName:	<input type="text"/>
RWAPassword:	<input type="text"/>
RWUserName:	<input type="text"/>
RWPassword:	<input type="text"/>
RWL3UserName:	<input type="text"/>
RWL3Password:	<input type="text"/>
RWL2UserName:	<input type="text"/>
RWL2Password:	<input type="text"/>
RWL1UserName:	<input type="text"/>
RWL1Password:	<input type="text"/>
ROUserName:	<input type="text"/>
ROPassword:	<input type="text"/>
MaxTelnetSessions:	<input type="text" value="8"/> 0..8
MaxRloginSessions:	<input type="text" value="8"/> 0..8
Timeout:	<input type="text" value="900"/> 30..65535 sec
NumAccessViolations:	0

Buttons:

[Table 5 on page 74](#) describes the **CLI** tab fields.

Table 5 CLI tab fields

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

Locking a port

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

To lock and unlock specific ports:

- 1 Select **Edit > Security > General** from the Device Manager menu bar.

The **Security** dialog box opens with the **EAPOL** tab selected (Figure 16 on page 72).

- 2 Click the **Port Lock** tab.

The **Port Lock** tab opens (Figure 18).

Figure 18 Security dialog box—Port Lock tab

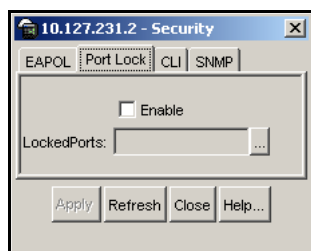


Table 6 describes the **Port Lock** tab fields.

Table 6 Port Lock tab fields

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

Viewing SNMP errors

To view SNMP errors:

- 1 Select **Edit > Security > General** from the Device Manager menu bar.
The **Security** dialog box opens with the **EOPOL** tab selected.
- 2 Click the **SNMP** tab.
The **SNMP** tab opens ([Figure 19](#)).

Figure 19 Security dialog box—SNMP tab



Table 7 describes the SNMP tab fields.

Table 7 SNMP tab fields

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

Table 7 SNMP tab fields (continued)

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

Chapter 3

Configuring access policies

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

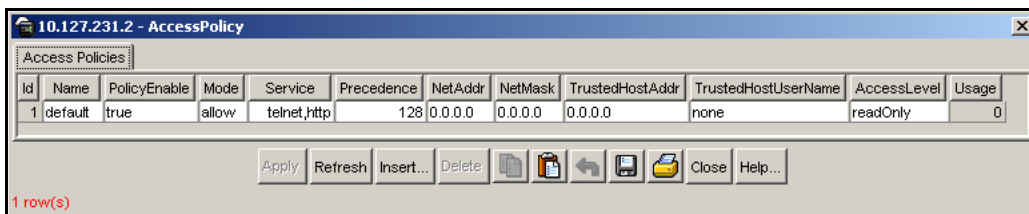
This chapter includes the following topics:

Topic	Page
Creating a new access policy	79
Enabling access policy for rlogin or rsh access	82

Creating a new access policy

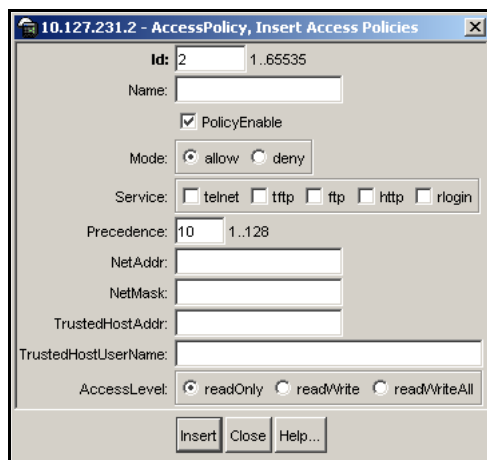
To create a new access policy:

- 1 Select **Edit > Security > Access Policies** from the Device Manager menu bar. The **AccessPolicy** dialog box opens (see [Figure 20 on page 80](#)).

Figure 20 AccessPolicy dialog box — Access Policies tab

2 Click **Insert**.

The **AccessPolicy, Insert Access Policies** dialog box opens (Figure 21).

Figure 21 AccessPolicy, Insert Access Policies dialog box

- 3 Ensure the **PolicyEnable** check box is enabled.
- 4 Identify the mode for a service by selecting the **allow** or **deny** option button.
- 5 Indicate the services by selecting one or more of the following option buttons: **telnet**, **tftp**, **ftp**, **http**, or **rlogin**.
- 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 network mask used for the **NetAddr** field.
- 9 Enter an IP address for the trusted host in the **TrustedHostAddr** field.

- 10 Enter a username in the **TrustedHostUserName** field.
- 11 Identify the access level for the service by selecting the **readOnly**, **readWrite**, or **readWriteAll** option button.
- 12 Click **Insert**.

[Table 8](#) describes the fields in the AccessPolicy and Insert Access Policies dialog boxes.

Table 8 AccessPolicy and Insert 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 or protocols to which this entry should be applied.
Precedence	Indicates the precedence of the policy. The lower the number, the higher the precedence (1 to 128).
NetAddr	Indicates the source network IP address. An address of 0.0.0.0 specifies any address on the network.
NetMask	Indicates the source network masks.
TrustedHostAddr	Indicates the trusted IP address of the host performing rlogin or rsh into the device. Applies only to rlogin and rsh. Note: You cannot use wildcard entries.
TrustedHostUserName	Specifies the user name assigned to the trusted host. Applies only to rlogin and rsh. This name is the same user name that you used to log on to the network (not the switch user name, such as rwa). Note: You cannot use wildcard entries. The user must already be logged in with the user name to be assigned to the trusted host. For example, using "rlogin -l newusername xx.xx.xx.xx" will not work from a UNIX workstation.
AccessLevel	Specifies the access level of the trusted host (readOnly, readWrite, or readWriteAll).
Usage	Indicates the number of times the access policy has been used.

Enabling access policy for rlogin or rsh access

To enable access policy for rlogin or rsh access:

- 1 Select **Edit > Chassis** from the Device Manager menu bar.

The **Chassis** dialog box opens with the **System** tab selected. (See [Figure 22](#).)

Figure 22 Chassis dialog box—System tab

10.127.231.2 - Chassis

System Chassis Boot Config Trap Receivers Performance User Set Time PoE

sysDescr: Passport-8310 (2.2.0.0)
sysUpTime: 8 days, 12h:18m:07s
sysContact: support@nortelnetworks.com
sysName: Passport-8310
sysLocation: 4655 Great America Parkway, Santa Clara, CA 95054
VirtualIpAddr: 0.0.0.0
VirtualNetMask: 0.0.0.0
ReadWriteLevel: ReadWriteAll

AuthenticationTraps
 EnableWebServer
 EnableAccessPolicy
 MrouteStreamLimit

LastChange: 0 day, 21h:12m:39s
LastVlanChange: 8 days, 12h:17m:11s
LastStatisticsReset: none
LastRunTimeConfigSave: 3 days, 00h:16m:44s
LastRunTimeConfigSaveToSlave: none
LastBootConfigSave: none
LastBootConfigSaveOnSlave: none

DefaultRuntimeConfigFileName: /flash/config.cfg
DefaultBootConfigFileName: /flash/boot.cfg
ConfigFileName:

Action: hardReset softReset resetCounters
 cpuSwitchOver resetConsole saveRuntimeConfig
 saveRuntimeConfigToSlave saveBootConfig saveSlaveBootConfig

LastActionResult: success

Apply Refresh Close Help...

- 2 Select the **EnableAccessPolicy** check box.

- 3 Click **Apply**.

4 Click **Close**.

Chapter 4

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.

This chapter includes the following topics:

Topic	Page
Loading the encryption module	85
Logging on using SNMPv3	87
Creating a user security model	89
Assigning MIB view access for an object	97
Creating a community	99

Loading the encryption module

Before you access the switch using SNMPv3 with DES encryption, you must load the encryption module, p83c2200.des, which allows you to use the Privacy protocol.

- 1 Open www.nortel.com/support in your browser.
- 2 Log in.
- 3 Ensure the **Browse product support** tab is selected.
- 4 Select **Passport** from the list in box 1.
- 5 Select **Ethernet Routing Switch 8300** from the list in box 2.
- 6 Select **Software** from the list in box 3.

- 7 Click **Go**.
- 8 Click on the **Ethernet Routing Switch 8300 SNMPv3 & 3DES** link.
- 9 Answer the questions on the questionnaire.
- 10 Click **Submit**.
- 11 Right-click on the file download link and enter a file location in which to copy the DES encryption module.
- 12 Click **OK**.
- 13 The file is downloaded.



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

- 14 Use FTP to copy this file to the switch.
- 15 Open the DOS window.
- 16 Use FTP to connect to the Ethernet Routing Switch 8300.

Figure 23 shows sample output from an FTP session.

Figure 23 FTP sample output from DOS window

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

- 17 Load the module on the switch:

```
config load-module DES /flash/p83c2200.des
```

Logging on using SNMPv3

To log on to Device Manager using SNMPv3, a valid SNMPv3 user must exist. If you have not yet configured SNMPv3 users, use the default user **initial** to log on to Device Manager. (To log on using the default user, **Authentication Protocol** must be set to **NONE**.) To configure users for your network using Device Manager, see “[Creating a user security model](#)” on [page 89](#) for instructions.

- 1 Launch the Device Manager.


The Device Manager opens — no devices are selected. See [Figure 24](#).

Figure 24 Device Manager window



- 2 Select **Device > Open** in the Device Manager window.

The **Open Device** dialog box opens ([Figure 25 on page 88](#)). [Table 9 on page 89](#) contains descriptions of the **Open Device** dialog box fields.

Figure 25 Open Device dialog box

The screenshot shows a dialog box titled "Device Manager 577b02 - Open Device". It has a standard Windows-style title bar with a close button. The dialog contains the following fields and controls:

- Device Name:** An empty text input field.
- Read Community:** A text input field containing six asterisks (*****).
- Write Community:** A text input field containing six asterisks (*****).
- SNMPv3 Section:**
 - v3 Enabled
 - User Name:** An empty text input field.
 - Authentication Protocol:** A dropdown menu currently showing "NONE".
 - Authentication Password:** An empty text input field.
 - Privacy Protocol:** A dropdown menu currently showing "NONE".
 - Privacy Password:** An empty text input field.
- Buttons:** Four buttons at the bottom: "Open", "Ping...", "Telnet...", and "Close".

- 3** Enter the device IP address in the **Device Name** field.
- 4** Select the **v3 Enabled** check box.
- 5** Enter a username in the **User Name** field.
- 6** Select the authentication protocol (if configured) for the user from the **Authentication Protocol** drop-down list.
- 7** Enter the password (if necessary) in the **Authentication Password** field.
- 8** Select the privacy protocol (if configured) for the user from the **Privacy Protocol** drop-down list.
- 9** Enter a password (if necessary) in the **Privacy Password** field.
- 10** Click **Open**.

Device Manager opens with the specified device selected.

Table 9 Open Device box fields

Field	Description
Device Name	Identifies the DNS name or IP address of the device.
Read Community	Indicates the length of the read community password string.
Write Community	Indicates the length of the write community password string.
v3 Enabled	Enables (the check box is selected) or disables (the check box is cleared) SNMP version 3.
User Name	Indicates the user's security name. If the v3 Enabled check box is selected, this name appears in the SNMPv3 tables.
Authentication Protocol	Identifies the authentication protocol used. Select the value (from the drop-down list) that is configured for this user. The valid values are NONE, MD5, and SHA-96.
Authentication Password	The password that is configured for the user for authentication purposes.
Privacy Protocol	Identifies the privacy protocol used. Select the value (from the drop-down list) that is configured for this user. The valid values are NONE, DES, and AES. If you select NONE, you do not enter a password.
Privacy Password	The password that is configured for this user for privacy purposes. (Note: Privacy must be set with authentication.)

Creating a user security model

The following sections describe the process for creating a user Security model (USM).

- [“Creating a user security model” on page 90](#)
- [“Creating membership for a group” on page 93](#)
- [“Creating access for a group” on page 94](#)

Creating a user security model



Note: To access the SNMPv3 USM, VACM, and Community tables, you must log on to Device Manager with SNMPv3 enabled (see [“Logging on using SNMPv3”](#) on page 87).

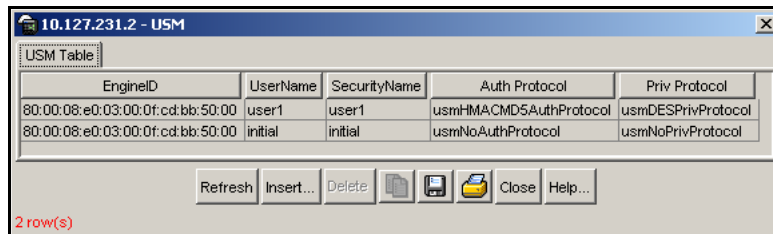
You can also use the NNCLI or CLI to configure SNMPv3 users. Refer to *Configuring and Managing Security using the NNCLI and CLI* (316804-C) for instructions.

To create a user security model (USM):

- 1 Select **Edit > SntpV3 > USM Table** from the Device Manager menu bar.

The USM dialog box opens ([Figure 26](#)).

Figure 26 USM dialog box



[Table 10](#) describes the USM tab fields.

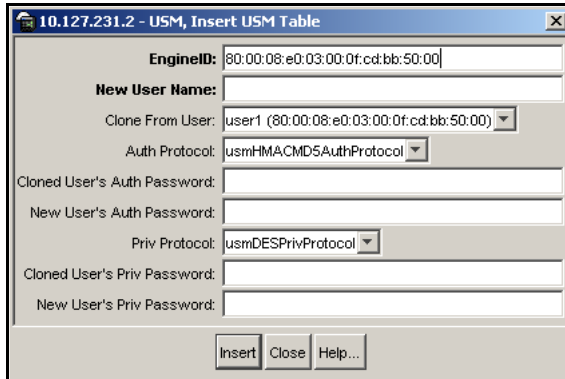
Table 10 USM dialog box fields

Field	Description
EngineID	Read-only field that indicates the SNMP engine's administratively-unique identifier.
New User Name	Indicates the name of the user in usmUser.
Security Name	Creates the name used as an index to the table. The range is 1 to 32 characters.
Auth Protocol	Identifies the Authentication protocol used.
Priv Protocol	Identifies the privacy protocol used.

2 Click **Insert**.

The **USM, Insert USM Table** dialog box opens (Figure 27).

Figure 27 USM, Insert USM Table dialog box

**3** Enter a name.**4** Select a security name from the **Clone From User** drop-down list.

The new user entry copies authentication data and private data from the user entry you select here.

5 Select an authentication protocol.**6** Enter the cloned user's authentication password.**7** Enter the new user's authentication password for this user model.**8** Select a privacy protocol.**9** Enter the cloned user's privacy password (if one exists).**10** Enter a new privacy password for this user model (if desired).**11** Click **Insert**.

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



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 11](#) describes the USM, Insert USM Table dialog box fields.

Table 11 USM—Insert USM Table dialog box fields

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

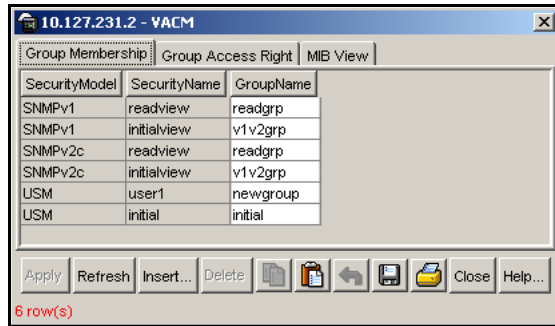
Creating membership for a group

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

- 1 Select **Edit > SnmpV3 > VACM table** from the Device Manager menu bar.

The **VACM** dialog box opens with the **Group Membership** tab displayed. See [Figure 28](#).

Figure 28 VACM dialog box



[Table 12](#) describes the VACM tab fields.

Table 12 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 1–32 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 29 on page 94](#)).

Figure 29 VACM, Insert Group Membership dialog box

- 3 Identify the security model by selecting the **SNMPv1**, **SNMPv2c**, or **USM** option button.
- 4 Enter a name in the **SecurityName** field.
- 5 Enter a name in the **GroupName** field.
- 6 Click **Insert**.

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

[Table 13](#) describes the VACM, Insert Group Membership tab fields.

Table 13 VACM dialog box—Insert Group Membership tab fields

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

Creating access for a group

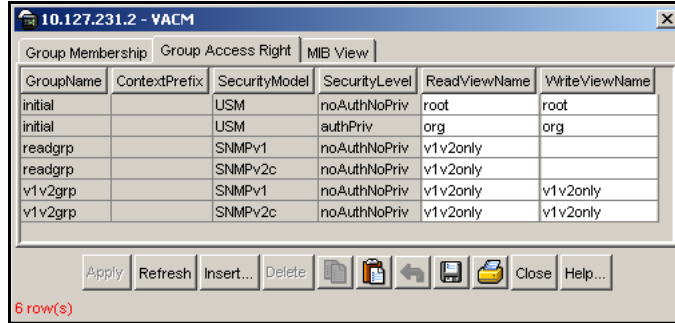
To create new access for a group:

- 1 Select **Edit > SntpV3 > VACM table** from the Device Manager menu bar. The **VACM** dialog box opens with the **Group Membership** tab displayed ([Figure 28 on page 93](#)).

- Click the **Group Access Right** tab.

The **Group Access Right** tab opens (Figure 30).

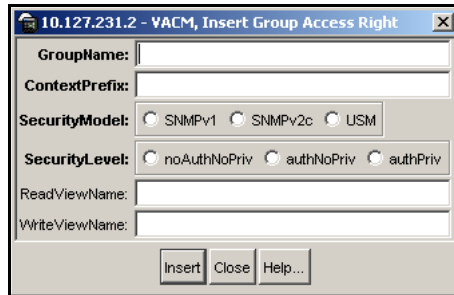
Figure 30 VACM dialog box — Group Access Right tab



- Click **Insert**.

The **VACM, Insert Group Access Right** dialog box opens (Figure 31).

Figure 31 VACM, Insert Group Access Right dialog box



- Enter a name in the **GroupName** field.
- Enter a value in the **ContextPrefix** field.



Note: The only supported context prefix is the empty string (“”).

- 6 Identify the security model by selecting the **SNMPv1**, **SNMPv2c**, or **USM** option button.
- 7 Identify the security level by selecting the **noAuthNoPriv**, **authNoPriv**, or **authPriv** option button.
- 8 Enter the MIB view name, in the **ReadViewName** field, to which you want the group to have read access (for example, **org**).
- 9 Enter the MIB view name, in the **WriteViewName** field, to which you want the group to have write access (for example, *org*).
- 10 Click **Insert**.

The **VACM Group Access Right** dialog box updates with the new group access added to the list.

Table 14 describes the Insert Group Access tab fields.

Table 14 VACM dialog box—Insert Group Access Right tab fields

Field	Description
GroupName	The name of the new group in the VACM table. The name is a numeral. The range is 1 to 32 characters.
ContextPrefix	The contextPrefix name must match exactly or partially to the value of the instance of this object. The range is an SnmpAdminString, 1 to 32 characters. Currently, only the empty string prefix is supported.
SecurityModel	The authentication checking to communicate to the switch. The security models are: <ul style="list-style-type: none"> • SNMPv1 • SNMPv2c • USM
SecurityLevel	The minimum level of security required to gain the access rights allowed. The security levels are: <ul style="list-style-type: none"> • noAuthNoPriv • authNoPriv • authPriv
ReadViewName	Identifies the MIB view (for example, <i>org</i>) to which you want the group to have read access.
WriteViewName	Identifies the MIB view (for example, <i>org</i>) to which you want the group to have write access.

Assigning MIB view access for an object

To assign MIB view access for an object:

- 1 Select **Edit > SnmpV3 > VACM table** from the Device Manager menu bar.
The **VACM** dialog box opens (see [Figure 28 on page 93](#)).
- 2 Select the **MIB View** tab.
The **MIB View** tab opens ([Figure 32](#)).

Figure 32 VACM dialog box—MIB View tab

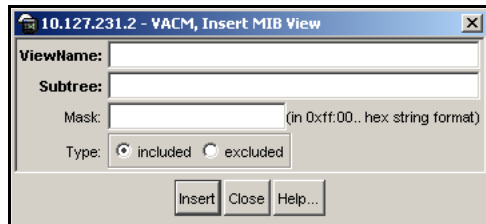
ViewName	Subtree	Mask	Type
org	iso		included
root	iso		included
snmp	snmpModules		included
snmp	system		included
layer1	org		excluded
layer1	system		included
layer1	ifAdminStatus		included
layer1	rcSys.Action		included
layer1	rcPortLockLockedPorts		included
layer1	rcPortAutoNegotiate		included
layer1	rcPortAdminDuplex		included
layer1	rcPortAdminSpeed		included
layer1	rcPortEntry 50		included
layer2	org		included
layer2	rcIp		excluded
layer2	rcArp		excluded
layer2	rcMlt		excluded
layer2	rcCli		excluded
layer2	rcIpx		excluded
layer2	rcLinkFlapDetect		excluded
layer2	rcRadius		excluded
layer2	rcUserSetTime		excluded
layer2	rcSsh		excluded
layer2	rcMgmt 40		excluded
layer2	rcRec		excluded
layer2	rcLacp		excluded
layer2	rcSys.AccessPolicyEnable		excluded
layer2	rcSys.AccessPolicyTable		excluded
layer2	rcChasDiffServEcnCompatibilityEnable		excluded
layer2	rcIpRouteTable		excluded
layer2	rcDiag.15		excluded
layer2	rcIcmp.9		excluded
layer2	rcIcmp.10		excluded
layer2	rc2kCpuEthernetPortTable		excluded
layer2	rc2kCpuEthernetPortRouteTable		excluded

48 row(s)

3 Click **Insert**.

The **VACM, Insert MIB View** dialog box opens (Figure 33).

Figure 33 VACM—Insert MIB View dialog box



4 Enter a name in the **ViewName** field.

5 Enter a subtree value.

6 Enter a mask value.

7 Identify the type of MIB view by selecting the **included** or **excluded** option button.

8 Click **Insert**.

The **MIB View** tab updates with the new MIB view added to the list.

Table 15 describes the VACM, Insert MIB View tab fields.

Table 15 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 (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). The default is included.

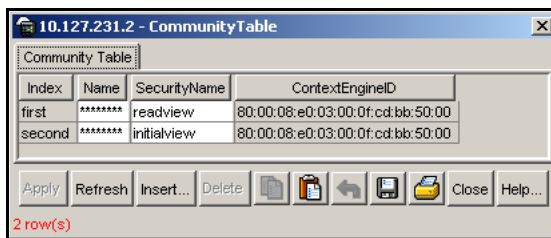
Creating a community

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

- 1 Select **Edit > SnmpV3 > Community Table** from the Device Manager menu bar.

The **Community Table** dialog box opens (Figure 34).

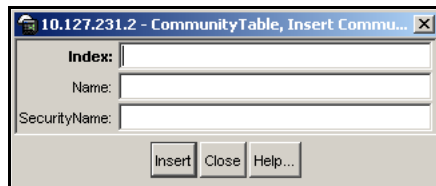
Figure 34 Community Table dialog box



- 2 Click **Insert**.

The **Community Table, Insert Community Table** dialog box opens (Figure 35).

Figure 35 Community Table, Insert Community Table dialog box



- 3 Enter an index.
- 4 Enter a name that is a community string.
- 5 Enter a security name.
- 6 Click **Insert**.

The **Community Table** tab updates with the new community name added to the list.

Table 16 describes the Community Table, Insert Community Table dialog box fields.

Table 16 Community Table, Insert Community Table dialog box fields

Field	Description
Index	Specifies the unique index value of a row in this table.
Name	Specifies the community string for which a row in this table represents a configuration.
SecurityName	Specifies the security name assigned to this entry in the Community table. The range is 1 to 32 characters.

Chapter 5

Configuring SSH

This chapter includes the following topics:

Topic	Page
Changing Secure Shell configuration parameters	101
Supported SSH and SCP clients	104
Using DSA authentication	105
Using RSA authentication	106

Changing Secure Shell configuration parameters

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



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

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

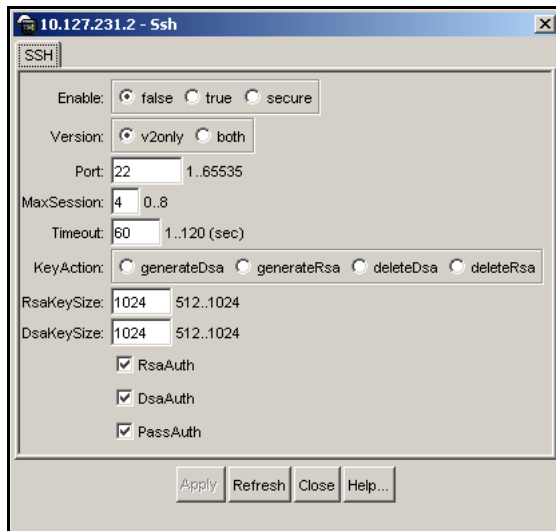
- The user access level is set to read/write/all community strings.
- The SNMP protocol is enabled.

To change SSH parameters:

- 1 Select **Edit > Security > SSH** from the Device Manager menu bar.

The **Ssh** dialog box opens. The **SSH** tab is selected. (See [Figure 36](#).)

Figure 36 Ssh dialog box — SSH tab



- 2 Enter information.

- 3 Click **Apply**.

[Table 17](#) describes the **SSH** tab fields.

Table 17 Ssh 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 non-secure 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.

Table 17 Ssh dialog box — SSH tab fields (continued)

Field	Description
Port	Sets the SSH connection port number. The default value is 22. Note: SSH session is not established for reserved ports. If you attempt to configure a reserved port (for example, port 23 (Telnet)) as an SSH connection port, the SSH session will not be established. Furthermore, you cannot later change the port number or any other parameters, even if you disable SSH. The default SSH connection port is 22. To configure additional SSH connection ports, use port numbers greater than 1024 (up to 65535).
MaxSession	Sets the maximum number of SSH sessions allowed. The value is in the range 0–8. Default is 4.
Timeout	Set the SSH authentication connection timeout in seconds. Default is 60 seconds. The timeout value is in the range 1–120.
KeyAction	Set the SSH key action.
RsaKeySize	RSA key size. Value is in the range 512–1024. Default is 1024.
DsaKeySize	DSA key size. Value is in the range 512–1024. 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 18 describes the third party SSH and SCP client software that have been tested, but are not included with this release.

Table 18 Third party SSH and SCP client software

SSH Client	Secure Shell (SSH)	Secure Copy (SCP)
Tera Term (Pro) Windows 2000/XP	<ul style="list-style-type: none"> • Supports SSH-1 client only. • Authentication: <ul style="list-style-type: none"> - RSA - Password • Does not include a keygen tool. • A separate key generation tool such as PuTTYgen must be used to generate an RSA key in SSHv1 format. 	<ul style="list-style-type: none"> • Client distribution does not include SCP client. • Tested on the Ethernet Routing Switch 8300 with the following applications: <ul style="list-style-type: none"> - Pageant (authentication agent holding private keys in memory) - PSCP (secure copy client)
Secure Shell Client Window 2000/XP	<ul style="list-style-type: none"> • Supports SSH-2 client. • Authentication: <ul style="list-style-type: none"> - DSA - Password • Provides a keygen tool. • It creates a DSA key in SSHv2 format. 	<ul style="list-style-type: none"> • Client distribution includes an SCP client which is not compatible with the Ethernet Routing Switch 8300.
OpenSSH Unix Solaris 3.9	<ul style="list-style-type: none"> • Supports SSH-1 and SSH-2 clients. • Authentication: <ul style="list-style-type: none"> - RSA - DSA - Password • Provides a keygen tool. • It creates both RSA and DSA keys in SSH v1 format. 	<ul style="list-style-type: none"> • Client distribution includes an SCP client that is supported on the Ethernet Routing Switch 8300.

After you have installed one of the SSH clients, 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.

Using DSA authentication

The Ethernet Routing Switch 8300 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 Ethernet Routing Switch 8300 generates one automatically, 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 Ethernet Routing Switch 8300.

[Table 19](#) describes access levels and filenames used for storing the SSH client authentication information using DSA.

Table 19 DSA authentication access level and filename

Client key format or WSM	Access Level	File name
Client key in IETF format (SSHv2)	RWA	<code>/flash/.ssh/dsa_key_rwa_ietf</code>
	RW	<code>/flash/.ssh/dsa_key_rw_ietf</code>
	RO	<code>/flash/.ssh/dsa_key_ro_ietf</code>
	L3	<code>/flash/.ssh/dsa_key_rwl3_ietf</code>
	L2	<code>/flash/.ssh/dsa_key_rwl2_ietf</code>
	L1	<code>/flash/.ssh/dsa_key_rwl1_ietf</code>
Client key in non IETF format	RWA	<code>/flash/.ssh/dsa_key_rwa</code>
	RW	<code>/flash/.ssh/dsa_key_rw</code>
	RO	<code>/flash/.ssh/dsa_key_ro</code>
	L3	<code>/flash/.ssh/dsa_key_rwl3</code>
	L2	<code>/flash/.ssh/dsa_key_rwl2</code>
	L1	<code>/flash/.ssh/dsa_key_rwl1</code>

Table 19 DSA authentication access level and filename (continued)

Client key format or WSM	Access Level	File name
WSM	14admin	<i>/flash/.ssh/dsa_key_14admin</i>
	slbadmin	<i>/flash/.ssh/dsa_key_slbadmin</i>
	oper	<i>/flash/.ssh/dsa_key_oper</i>
	14oper	<i>/flash/.ssh/dsa_key_14_oper</i>
	slboper	<i>/flash/.ssh/dsa_key_slboper</i>
	ssladmin	<i>/flash/.ssh/dsa_key_ssladmin</i>

Using RSA authentication

The Ethernet Routing Switch 8300 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 Ethernet Routing Switch 8300 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 Ethernet Routing Switch 8300.

[Table 20](#) describes the access level and filename used for storing the SSH client authentication information using RSA.

Table 20 RSA authentication access level and file name

Client key format or WSM	Access level	File name
Client key in IETF format	RWA	<i>/flash/.ssh/rsa_key_rwa</i>
	RW	<i>/flash/.ssh/rsa_key_rw</i>
	RO	<i>/flash/.ssh/rsa_key_ro</i>
	L3	<i>/flash/.ssh/rsa_key_rwl3</i>
	L2	<i>/flash/.ssh/rsa_key_rwl2</i>
	L1	<i>/flash/.ssh/rsa_key_rwl1</i>

Table 20 RSA authentication access level and file name (continued)

Client key format or WSM	Access level	File name
WSM	14admin	<i>/flash/.ssh/rsa_key_14admin</i>
	slbadmin	<i>/flash/.ssh/rsa_key_slbadmin</i>
	oper	<i>/flash/.ssh/rsa_key_oper</i>
	14oper	<i>/flash/.ssh/rsa_key_14_oper</i>
	slboper	<i>/flash/.ssh/rsa_key_slboper</i>
	ssladmin	<i>/flash/.ssh/rsa_key_ssladmin</i>

Chapter 6

Setting up RADIUS servers

Nortel recommends that you configure at least two RADIUS servers in the network to provide redundancy. You can configure a maximum of 10 RADIUS servers in a single network.

The Ethernet Routing Switch 8300 software supports BaySecure Access Control (BSAC*), Merit Network, and freeRadius servers. For instructions on installing the BSAC, Merit Network, or freeRadius server software on the server that you will use, see the installation manual that came with your software.



Note: The BSAC server is now known as the Steel-Belted Radius server (SBR). The SBR Version 4.0 and higher includes a module that supports EAP. The procedures in this chapter for preparing a BSAC server to support RADIUS authentication are valid for the SBR.

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

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

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

Topic	Page
Updating files for the BSAC RADIUS server	110
Updating the dictionary file for a Merit Network server	112
Updating files for the freeRadius server	113
Using a third-party RADIUS server	115
Enabling EAP authentication	116

Updating files for the BSAC RADIUS server

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

- The main dictionary (radius.dct). This file must be edited to contain an entry of parameters from the newly created Passport dictionary.
- A private dictionary (pprt8300.dct). This file, which is specific to the Ethernet Routing Switch 8300, must be generated. It will be sourced and used by dictiona.dcm and vendor.ini.
- The vendor.ini file. This file must contain an entry for the Ethernet Routing Switch 8300 in order for the file to acknowledge the model/type during the client configuration.
- The account.ini file. This file must contain the CLI-Command= entry.

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

- 1 Add the following lines in files `radius.dct` and `pprt8300.dct`:

```

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

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

```



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

- 2 Add the following lines in `vendor.ini`:

```

vendor-product = Nortel Passport 8300
dictionary = pprt8300
ignore-ports = no
port-number-usage = per-port-type
help-id = 0

```

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

```
Cli-Command=
```

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

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

- 5 Restart the server to activate the changes.

Updating the dictionary file for a Merit Network server

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

```
VENDOR          Nortel  1584  
  
ATTRIBUTE       Access-Priority 192 integer  Nortel  
  
VALUE  Access-Priority      None-Access          0  
VALUE  Access-Priority      Read-Only-Access     1  
VALUE  Access-Priority      L1-Read-Write-Access 2  
VALUE  Access-Priority      L2-Read-Write-Access 3  
VALUE  Access-Priority      L3-Read-Write-Access 4  
VALUE  Access-Priority      Read-Write-Access     5  
VALUE  Access-Priority      Read-Write-All-Access 6  
  
ATTRIBUTE       Cli-Command  192 string  Nortel
```

You must restart the server to activate the changes.

Updating files for the freeRadius server

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

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

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

- 1 Add the following lines in the dictionary file:

```
VENDOR          Nortel 1584

BEGIN-VENDOR Nortel

ATTRIBUTE       Access-Priority 192 integer

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

#CLI profile
ATTRIBUTE       Command-Access 194 integer

#CLI Commands
ATTRIBUTE       Cli-Commands 193 string

#CLI Commands
ATTRIBUTE       Commands 195 string

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

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

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

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

3 Add the following lines in users.

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

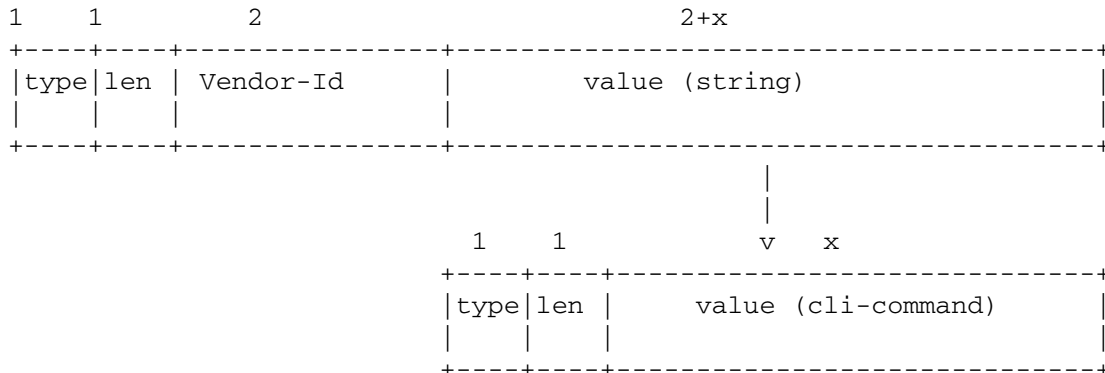
DOMAIN2\eap_user    Auth-Type := EAP, User-Password == "eap_password"
                    Reply-Message = "You're authenticated, %u !!",

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

You must restart the server to activate the changes.

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:



Enabling EAP authentication

To enable EAP authentication:

- 1** Ensure the RADIUS authentication and accounting ports match between the SBR server and the 8300 switch.
- 2** Edit the eap.ini file in the SBR's "Radius\Service" directory to accommodate the authentication paradigm.
- 3** Update 5 files for the SBR server:
 - a** The main dictionary (radius.dct). This file must be edited to contain an entry of parameters from the newly-created Passport dictionary.
 - b** A private dictionary (pprt8300.dct). This file, which is specific to the Ethernet Routing Switch 8300, must be generated. It will be sourced and used by (dictiona.dcm) and (vendor.ini).
 - c** The vendor.ini file. This file must contain an entry for the Ethernet Routing Switch 8300 in order for the file to acknowledge the model/type during the client configuration.
 - d** The account.ini file. This file must contain the CLI Command = entry.
 - e** The eap.ini file for SBR Ver4.0 and above for EAP authentication.

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

- a** Add the following lines in files radius.dct and pprt8300.dct:

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

```
VALUE Access-Priority Read-Write-Access 5
VALUE Access-Priority Read-Write-All-Access 6
ATTRIBUTE Cli-Command 26 [vid=1584 type1=193 len1=+2
data=string]
```



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

- b** Add the following lines in vendor.ini:

```
vendor-product = Nortel Passport 8300
dictionary = pprr8300
ignore-ports = no
port-number-usage = per-port-type
help-id = 0
```

- c** Add the following entry to the account.ini file:

```
Cli-Command=
```

- d** In the account.ini file, ensure that the following lines are present:

```
vendor-product = Nortel Passport 8300
dictionary = pprr8300
ignore-ports = no
port-number-usage = per-port-type
help-id = 0
```

- e** To enable EAP authentication, for the SBR Server Version 4.0 and above, uncomment the line in the eap.ini file.
- f** Save changes and restart the server to activate the changes.

Chapter 7

Configuring RADIUS authentication and accounting

This chapter describes how to configure RADIUS authentication and accounting using the Device Manager, and includes the following topics:

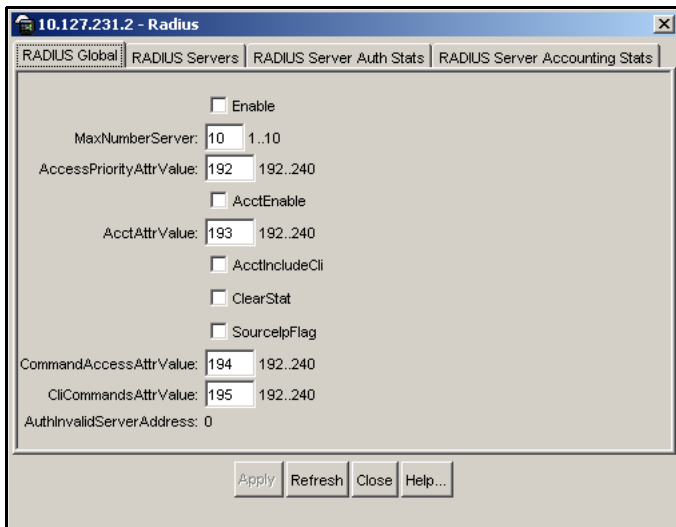
Topic	Page
Enabling RADIUS authentication	119
Enabling RADIUS accounting	122
Adding a RADIUS server	122
Showing RADIUS server authentication statistics	125
Showing RADIUS server accounting statistics	126
Modifying a RADIUS configuration	127
Deleting a RADIUS configuration	128

Enabling RADIUS authentication

To enable RADIUS authentication globally:

- 1 Select **Edit > Security > RADIUS** from the Device Manager menu bar.

The **Radius** dialog box opens with the **RADIUS Global** tab selected. (see [Figure 37 on page 120](#)).

Figure 37 Radius dialog box — RADIUS Global tab

- 2 Select the **Enable** check box to enable RADIUS authentication services.
- 3 Enter a value for the maximum number of servers in the **MaxNumberServer** field.
- 4 Enter an access priority value in the **AccessPriorityAttrValue** field (the default value is 192).
- 5 Click **Apply**.

[Table 21](#) describes the **RADIUS Global** tab fields.

Table 21 RADIUS dialog box — RADIUS Global tab fields

Fields	Description
Enable	Enables (checked) or disables (cleared) the RADIUS authentication feature globally.
MaxNumberServer	Specifies the maximum number of servers to be used (in the range 1–10).

Table 21 RADIUS dialog box — RADIUS Global tab fields (continued)

Fields	Description
AccessPriorityAttrValue	Specific to RADIUS authentication. Sets this vendor-specific attribute value to match the type value set in the dictionary file on the RADIUS server. Values are in the range 192–240. Nortel recommends the default setting of 192 for the Ethernet Routing Switch 8300.
AcctEnable	Enables (selected) or disables (cleared) the RADIUS accounting feature.
AcctAttrValue	Specific to RADIUS accounting. This is a vendor-specific attribute. Values are in the range 192–240. This value must be different from the access-priority attribute value configured for authentication. The default value is 193.
AcctIncludeCli	Specifies whether the user wants CLI commands to be included in the RADIUS accounting requests. By default, CLI commands are not included.
ClearStat	Select the check box to clear RADIUS statistics from the switch.
SourceIpFlag	Enable (select the check box) to include the IP address of the gateway or router in the RADIUS packet.
CommandAccessAttrValue	Specifies the value of the CLI/NNCLI command access attribute. Attribute values configured at the switch must match those configured at the server. The value range is 192 to 240. Check with your network administrator to verify attribute values. Note: The attribute value for CLI access must be different from the attribute value for NNCLI access so that the server can distinguish between the two types of commands.
CliCommandsAttrValue	Specifies the value of the CLI command attribute. Values are in the range 192–240. The default value is 195.
AuthInvalidServerAddress	Specifies the number of RADIUS Access-Response packets received from invalid or unknown servers.
Note: When configuring RADIUS services, no two attributes can have the same value. For example, if acct-attribute-value is set to 194, no other attribute can have that same value.	

Enabling RADIUS accounting

To enable RADIUS accounting globally:

- 1 Select **Edit > Security > RADIUS** from the Device Manager menu bar.
The **Radius** dialog box opens with the **RADIUS Global** tab selected (see [Figure 37 on page 120](#)).
- 2 Select the **AcctEnable** check box to enable RADIUS accounting services.



Note: When RADIUS accounting is enabled, expect a delay in the CLI login process. When accounting is enabled, the switch must attempt to connect to all RADIUS servers individually (there are three retries for each server), and if a server responds, the switch must send the accounting-start message. This creates the delay. If you are not using RADIUS accounting, ensure it is disabled to prevent the login delays.

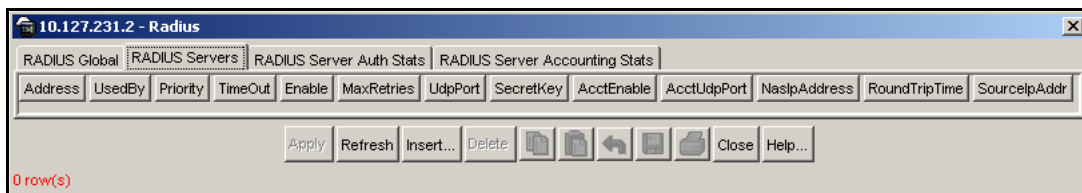
- 3 Enter an attribute value in the **AcctAttrValue** field (the default value is 193).
- 4 Click **Apply**.

[Table 21 on page 120](#) describes the **RADIUS Global** tab fields.

Adding a RADIUS server

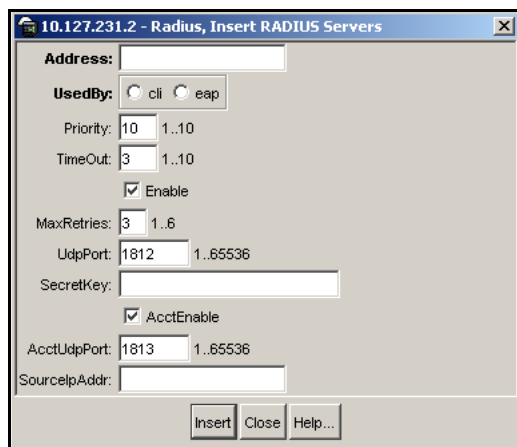
To add a RADIUS server:

- 1 Select **Edit > Security > RADIUS** from the Device Manager menu bar.
The **Radius** dialog box opens with the **RADIUS Global** tab selected (see [Figure 37 on page 120](#)).
- 2 Click the **RADIUS Servers** tab.
The **RADIUS Servers** tab opens ([Figure 38 on page 123](#)).

Figure 38 Radius dialog box — RADIUS Servers tab

3 Click **Insert**.

The **Radius, Insert RADIUS Servers** dialog box opens ([Figure 39](#)).

Figure 39 Radius, Insert RADIUS Servers dialog box

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

5 Select a service in the **Usedby** field.

Select either the **cli** or **eap** option button.

6 Enter a secret key.

7 Click **Insert**.

The information for the configured RADIUS server appears in the **RADIUS Servers** tab of the **Radius** dialog box.

[Table 22 on page 124](#) describes the fields on the **RADIUS Servers** tab and the **Radius, Insert RADIUS Servers** dialog box.

Table 22 RADIUS Servers tab and Insert RADIUS Servers dialog box fields

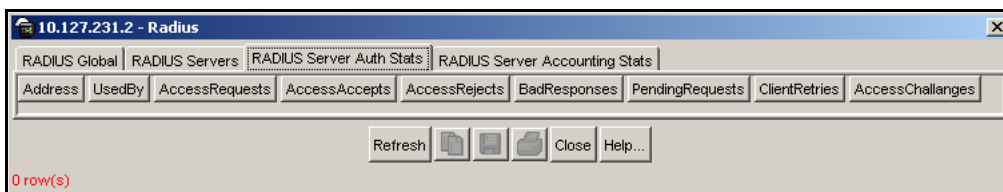
Fields	Description
Address	The IP address of the RADIUS server.
UsedBy	Specifies the service that uses this device. The options are CLI or EAP.
Priority	Specifies the priority of each server (that is, the order in which authentication is sent to servers when more than one is configured). The range is 1–10. The default is 10.
TimeOut	Specifies the time interval, in seconds, before the client retransmits the packet (in the range 1–10). The default value is 3 seconds.
Enable	Enables or disables authentication on the server. The default is true (the check box is selected).
MaxRetries	Specifies the maximum number of retransmissions allowed (in the range 1–6). The default value is 3.
UdpPort	Specifies the UDP port that the client uses to send requests to the server (in the range 1–65536). The default value is 1812. Note: The UDP port value set for the client must match the UDP value set for the RADIUS server.
SecretKey	Specifies the RADIUS server secret key. The secret key is the client password that must be validated by the server.
AcctEnable	Enables RADIUS accounting.
AcctUdpPort	The UDP port the client uses to send accounting requests to the server (in the range 1–65536). The default value is 1813. Note: The UDP port value set for the client must match the UDP value set for the RADIUS server.
SourceIpAddr	IP address of the gateway or router.
NasIpAddress	IP address of the NAS used in RADIUS requests sent to the server.
RoundTripTime	Time difference between the instant when a RADIUS Request is sent to the server and the instant when the RADIUS Response is received from the server.

Showing RADIUS server authentication statistics

To display RADIUS server authentication statistics on the switch:

- 1 Select **Edit > Security > RADIUS** from the Device Manager menu bar.
The **Radius** dialog box opens with the **RADIUS Global** tab selected (see [Figure 37 on page 120](#)).
- 2 Click the **RADIUS Server Auth Stats** tab.
The **RADIUS Server Auth Stats** tab opens ([Figure 40](#)).

Figure 40 Radius dialog box — RADIUS Server Auth Stats tab



[Table 23](#) describes the **RADIUS Server Auth Stats** tab fields.

Table 23 Radius dialog box — RADIUS Server Auth Stats tab fields

Item	Description
Address	The IP address of the RADIUS server.
UsedBy	The service that uses the RADIUS server (CLI or EAP).
AccessRequests	Number of RADIUS access-response packets sent to this server. This does not include retransmissions.
AccessAccepts	Number of RADIUS access-accept packets, valid or invalid, received from this server.
AccessRejects	Number of RADIUS access-reject packets, valid or invalid, received from this server.
BadResponses	Number of RADIUS invalid access-response packets received from this server.

Table 23 Radius dialog box — RADIUS Server Auth Stats tab fields (continued)

Item	Description
PendingRequests	Number of RADIUS access-request packets sent to this server that have not yet received a response, or have timed out. This variable is increased when an access-request is sent. The variable is decreased due to receipt of an access-request, access-reject, a timeout, or retransmission.
ClientRetries	Number of authentication retransmissions to the server.
AccessChallenges	Authentication parameter that indicates the number of access-challenges sent by the RADIUS server.

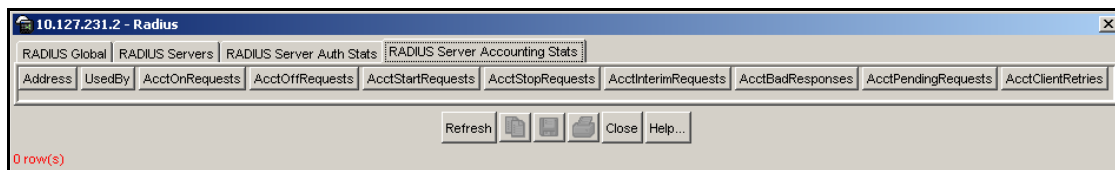


Note: To clear server statistics, select the **ClearStat** check box located on the **RADIUS Global** tab (see [Figure 37 on page 120](#)), and click **Apply**.

Showing RADIUS server accounting statistics

To display RADIUS server accounting statistics on the switch:

- 1 Select **Edit > Security > RADIUS** from the Device Manager menu bar.
The **Radius** dialog box opens with the **RADIUS Global** tab selected (see [Figure 37 on page 120](#)).
- 2 Click the **RADIUS Server Accounting Stats** tab.
The **RADIUS Server Accounting Stats** tab opens ([Figure 41](#)).

Figure 41 Radius dialog box — RADIUS Server Accounting Stats tab

[Table 23 on page 125](#) describes the **RADIUS Server Accounting Stats** tab fields.

Table 24 Radius dialog box — RADIUS Server Accounting Stats tab fields

Item	Description
Address	The IP address of the RADIUS server.
UsedBy	The service that uses the RADIUS server (CLI or EAP).
AcctOnRequests	Number of accounting-on requests sent to the server.
AcctOffRequests	Number of accounting-off requests sent to the server.
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.
AcctBadResponses	Number of invalid accounting responses from the server that are discarded.
AcctPendingRequests	Number of accounting requests waiting to be sent to the server.
AcctClientRetries	Number of accounting retries made to this server.



Note: To clear server statistics, select the **ClearStat** check box located on the **RADIUS Global** tab (see [Figure 37 on page 120](#)), and click **Apply**.

Modifying a RADIUS configuration

To modify an existing RADIUS configuration:

- 1 Select **Edit > Security > RADIUS** from the Device Manager menu bar.
The **Radius** dialog box opens with the **RADIUS Global** tab selected (see [Figure 37 on page 120](#)).
- 2 Click the **RADIUS Servers** tab.
The **RADIUS Servers** tab opens (see [Figure 38 on page 123](#)).

- 3 Type new information in the row you want to modify, or use the lists to make a selection.
Access the lists by left-clicking in a field.
- 4 Click **Apply**.

Deleting a RADIUS configuration

To delete an existing RADIUS configuration:

- 1 Select **Edit > Security > RADIUS** from the Device Manager menu bar.
The **Radius** dialog box opens with the **RADIUS Global** tab selected (see [Figure 37 on page 120](#)).
- 2 Click the **RADIUS Servers** tab.
The **RADIUS Servers** tab opens (see [Figure 38 on page 123](#)).
- 3 Identify the configuration to delete by clicking anywhere in the row.
- 4 Click **Delete**.

Chapter 8

Configuring EAPoL

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access control protocol. EAPoL provides security to your network by preventing users from accessing network resources before they are authenticated.

EAPoL allows you to set up network access control on internal LANs and to exchange authentication information between any end station or server connected to the Ethernet Routing Switch 8300 and an authentication server (such as a RADIUS server). Commands for configuring the RADIUS MAC centralization feature are also included.

EAPoL extends the benefits of remote authentication to internal LAN clients. For example, if a new client PC fails the authentication process, EAPoL prevents it from accessing the network.

This chapter includes the following topics:

Topic	Page
Configuration prerequisites	130
Configuring EAPoL globally	130
Configuring EAPoL on a port	132
Changing the authentication status of a port	148
Graphing EAPoL statistics	149

Configuration prerequisites

Use the following configuration rules when using EAPoL:

- Before configuring your switch, you must configure at least one EAPoL RADIUS Server and Shared Secret field.
- You cannot configure EAPoL on ports that are currently configured for:
 - shared segments
 - multilink trunking (MLT)
 - tagging



Note: Although you can enable both port mirroring and EAPoL on a port, Nortel does not recommend it.

- You can enable EAPoL in any order; that is, you do not have to enable EAPoL locally before you can enable it globally.
- You can connect up to eight clients on each EAPoL-enabled port if you enable the Multiple Host feature.

EAPoL uses the RADIUS protocol to authenticate EAPoL logins. See [Chapter 7, “Configuring RADIUS authentication and accounting,”](#) on page 119 for more information on using the RADIUS protocol.

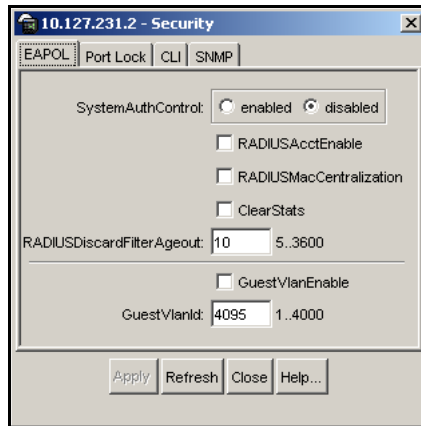
Configuring EAPoL globally

The **SystemAuthControl** field globally enables or disables EAPoL on the switch. (By default, EAPoL is disabled.) You enable EAPoL on all the controlled ports of the switch with this command.

To enable EAPoL globally on the switch:

- 1 Select **Edit > Security > General** from the Device Manager main menu.

The **Security** dialog box opens with the **EAPoL** tab selected (see [Figure 42 on page 131](#)).

Figure 42 Security dialog box — EAPOL tab

- 2 Select the **enabled** option button.
- 3 Select the **RADIUSAcctEnable** check box to enable RADIUS accounting.
- 4 Select the **RADIUSMacCentralization** check box to enable RADIUS MAC centralization.
- 5 Select the **ClearStats** check box to clear RADIUS statistics from the switch.
- 6 Enter an integer value (in the range 5–3600 seconds) in the **RADIUSDiscardFilterAgeout** field to globally set the ageout period for pending (due to server timeout or the server is unreachable) non-eap-macs.
- 7 Select the **GuestVlanEnable** check box to enable Guest VLANs on the switch.
- 8 Enter an integer value (in the range 1–4000) in the **GuestVlanId** field to identify the Guest VLAN.
- 9 Click **Apply** to save your changes.

Configuring EAPoL on a port

This section describes how to configure EAPoL on your switch ports, and includes the following topics:

- [“Configuring general authenticator port settings,”](#) next
- [“Configuring non-EAPoL clients on a port”](#) on page 136
- [“Configuring non-EAPoL MAC addresses on a port”](#) on page 137
- [“Viewing the status of non-EAPoL clients that use RADIUS”](#) on page 139
- [“Configuring EAPoL multihosts on a port”](#) on page 141
- [“Enabling or disabling Guest VLANs on a port”](#) on page 147

Configuring general authenticator port settings

To configure general EAPoL settings on one or more ports:

- 1 Select the port you want to edit.



Note: To select multiple ports, press and hold the **Ctrl** key, then left-click the ports you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

- Double-click the selected port.
- Select **Edit** from the shortcut menu.
- Select **Edit > Port** from the Device Manager main menu.
- Click **Edit** on the toolbar.

The **Port** dialog box for a single port opens with the **Interface** tab selected (see [Figure 43](#) on page 133).

Figure 43 Port dialog box — Interface tab

192.168.1.1 - Port 1/3

Interface | VLAN | STG | MAC Learning | Rate Limiting | Test | Router Discovery | VCT | PoE | QOS | TxQueue | EAPOL | Mroute Stream Limit

Index: 66
Name:
Descr: Port 1/3
Type: rc100BaseTXPOE
Mtu: 1522
PhysAddress: 00:0f:cd:bb:50:42
VendorDescr:

AdminStatus: up down testing
OperStatus: up
LastChange: 4 days, 03h:54m:32s
LinkTrap: enabled disabled

AutoNegotiate: true false
AdminDuplex: half full
OperDuplex: full
AdminSpeed: mbps10 mbps100 mbps1000
OperSpeed: 100
AutoNegAdCapability: 10Half,10Full,100Half,100Full
AutoNegAd: 10Half 10Full 100Half
 100Full 1000Half 1000Full

MIItd: 0
Locked: false
 UnknownMacDiscard

Action: none flushMacFdb flushAll
Result: none

Apply Refresh Close Help...

3 Click the **EAPOL** tab.

The EAPoL tab opens (see Figure 44).

Figure 44 Port dialog box — EAPoL tab

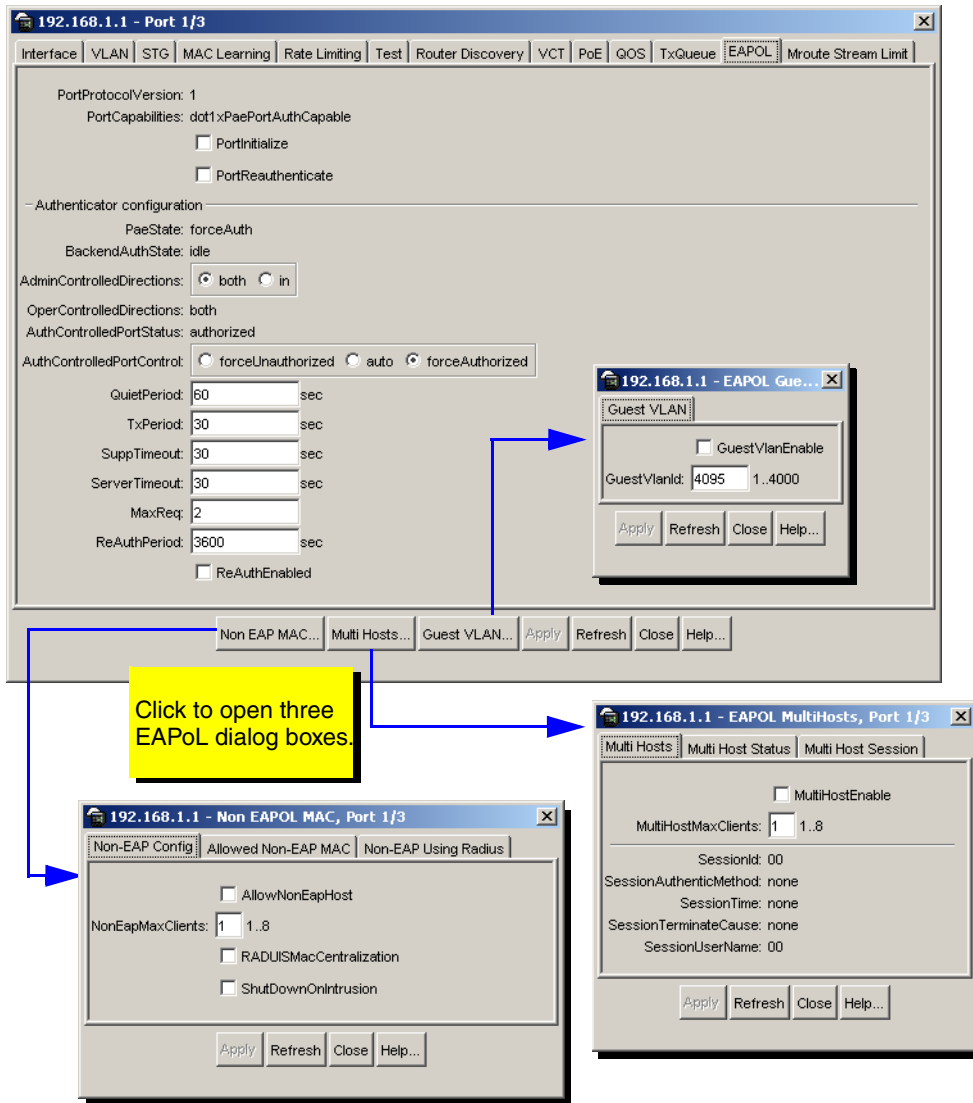


Table 25 on page 135 describes the EAPoL tab fields.

Table 25 Port dialog box — EAPoL tab fields

Field	Description
PortProtocolVersion	Read-only field that indicates the protocol version number.
PortCapabilities	Read-only field that indicates that PAE is supported on this port.
PortInitialize	When checked, initializes EAPoL authentication on this port. After the port initializes, this field reverts to its default, which is disabled.
PortReauthenticate	When checked, re-authenticates the Supplicant connected to this port immediately. The default is disabled.
PaeState	Displays the current Authenticator PAE state. The possible states are: initialized disconnected connecting authenticating authenticated aborting held forceAuth forceUnauth
BackendAuthState	Displays the current state of Backend Authentication. The possible states are: request response success fail timeout idle initialize
AdminControlledDirections	Indicates the control direction. Control direction can be either in (incoming-only) or both (incoming-and-outgoing). If the port is unauthorized, traffic is blocked, based on this setting. If AdminControlledDirections is set to in , ingressing traffic is blocked; egress traffic is forwarded normally. If AdminControlledDirections is set to both , traffic is blocked in both directions.
OperControlledDirections	Read-only field that indicates the current control direction. The options are in and both .
AuthControlledPortStatus	Displays the port's current state: unauthorized, auto, or authorized.
AuthControlledPortControl	Sets the authentication status for this port. The default is <i>forceAuthorized</i> . <i>forceUnauthorized</i> - port is always unauthorized. <i>auto</i> - port authorization depends on the results of the EAPoL authentication by the RADIUS server. <i>forceAuthorized</i> - port is always authorized.

Table 25 Port dialog box — EAPoL tab fields (continued)

Field	Description
QuietPeriod	Sets the time interval (in seconds) between authentication failure and the start of a new authentication. The allowed range is 1 to 65535, and the default is 60.
TxPeriod	Sets the time (in seconds) to wait for a response from a Supplicant for EAP Request/Identity packets. The allowed range is 1 to 65535, and the default is 30.
SuppTimeout	Sets the time (in seconds) to wait for a response from a Supplicant for all EAP packets except EAP Request/Identity packets. The allowed range is 1 to 65535, and the default is 30.
ServerTimeout	Sets the time (in seconds) to wait for a response from the RADIUS server. The allowed range is 1 to 65535, and the default is 30.
MaxReq	Sets the maximum number of times to retry sending packets to the Supplicant. The allowed range is 1 to 10, and the default is 2.
ReAuthPeriod	Sets the time interval (in seconds) between successive re-authentications (see “ReAuthEnabled”). The allowed range is 1 to 2147483647, and the default is 3600 (1 hour).
ReAuthEnabled	When checked, re-authenticates an existing Supplicant at the time interval specified in ReAuthPeriod .

Configuring non-EAPoL clients on a port

To configure non-EAPoL MAC addresses on one or more ports:

- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click the selected port.
 - Select **Edit** from the shortcut menu.
 - Select **Edit > Port** from the Device Manager main menu.
 - Click **Edit** on the toolbar.

The **Port** dialog box for a single port opens with the **Interface** tab selected (see [Figure 43](#) on page 133).

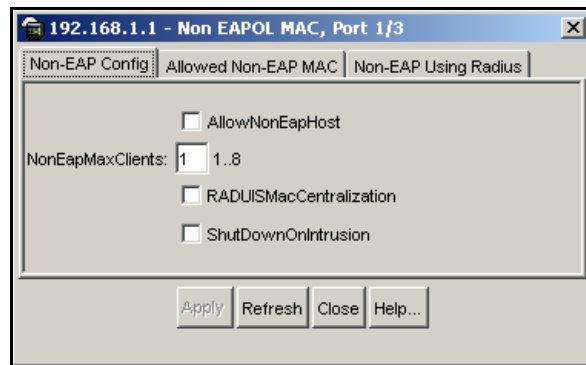
- 3 Click the **EAPoL** tab.

The **EAPoL** tab opens (see [Figure 44](#) on page 134).

- 4 Click **Non EAP MAC...**

The **Non EAP MAC** dialog box opens with the **Non-EAP Config** tab selected ([Figure 45](#)).

Figure 45 Non EAPoL MAC dialog box — Non-EAP Config tab



- 5 Select the **AllowNonEapHost** check box to allow a mix of EAPoL clients on the port.
- 6 Enter an integer value (in the range 1–8) in the **NonEAPMaxClients** field to specify the maximum number of non-EAPoL clients that can reside on this port.
- 7 Select the **RADIUSMacCentralization** check box to enable this feature.
- 8 Select the **ShutDownOnIntrusion** check box to shut down the port when the maximum non-EAP clients limit is reached.
- 9 Click **Apply** to save your configuration.

Configuring non-EAPoL MAC addresses on a port

To configure non-EAPoL MAC addresses on one or more ports:

- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click the selected port.

- Select **Edit** from the shortcut menu.
- Select **Edit > Port** from the Device Manager main menu.
- Click **Edit** on the toolbar.

The **Port** dialog box for a single port opens with the **Interface** tab selected (see [Figure 43 on page 133](#)).

- 3 In the **Port** dialog box, click the **EAPOL** tab.

The **EAPOL** tab opens (see [Figure 44 on page 134](#)).

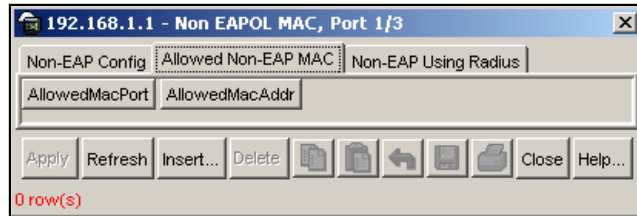
- 4 Click **Non EAP MAC...**

The **Non EAP MAC** dialog box opens with the **Non EAP Config** tab selected ([Figure 45 on page 137](#)).

- 5 Click the **Allowed Non-EAP MAC** tab.

The **Allowed Non-EAP MAC** tab opens and displays currently configured MAC addresses that are allowed ([Figure 46](#)).

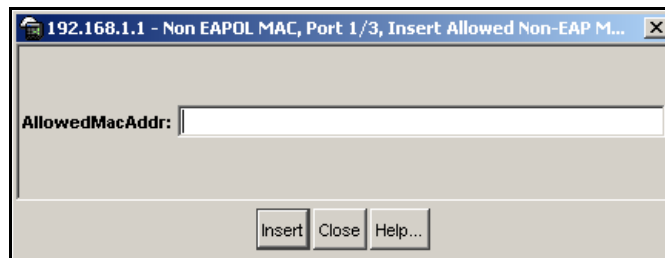
Figure 46 Non EAPOL MAC dialog box — Allowed Non-EAP MAC tab



- 6 Click **Insert**.

The **Insert Allowed Non-EAP MAC** dialog box opens ([Figure 47](#)).

Figure 47 Insert Allowed Non-EAP MAC dialog box



- 7 Enter a MAC address you want to add to the non-EAPoL MAC list in the **AllowedMacAddr** field.



Note: Non-Eap-Mac addresses can be added only when allow-non-eap-clients is disabled.

- 8 Click **Insert**.

The new MAC address is added to the **AllowedMACAddr** list in the **Allowed Non-EAP MAC** tab.

- 9 Click **Apply** to save your configuration.

Viewing the status of non-EAPoL clients that use RADIUS

To view information about non-EAPoL clients using RADIUS on one or more ports:

- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click the selected port.
 - Select **Edit** from the shortcut menu.
 - Select **Edit > Port** from the Device Manager main menu.
 - Click **Edit** on the toolbar.

The **Port** dialog box for a single port opens with the **Interface** tab selected (see [Figure 43 on page 133](#)).

- 3 Click the **EAPOL** tab.

The **EAPOL** tab opens (see [Figure 44 on page 134](#)).

- 4 Click **Non EAP MAC...**

The **Non EAP MAC** dialog box opens with the **Non EAP Config** tab selected ([Figure 45 on page 137](#)).

- 5 Click the **Non-EAP Using Radius** tab.

The **Non-EAP Using Radius** tab opens ([Figure 46 on page 138](#)).

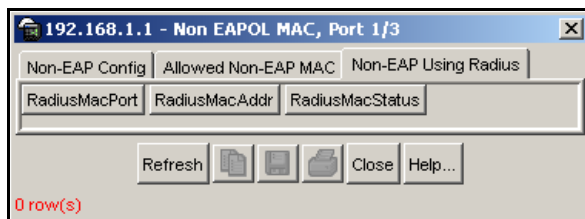
Figure 48 Non EAPOL MAC dialog box — Non-EAP Using Radius tab

Table 25 describes the **Non-EAP Using Radius** tab fields.

Table 26 Non EAPOL MAC dialog box — Non-EAP using Radius tab fields

Field	Description
RadiusMacPort	Read-only field that displays the port number.
RadiusMacAddr	Read-only field that displays the non-EAP MAC address.
RadiusMacStatus	Read-only field that displays the RADIUS authentication status of the learned MAC addresses. There are five possible status options: Pending Rejected Authenticated Request dropped Server not reachable



Note: Non-EAP clients are not authenticated if the RADIUS queue is full, or if the RADIUS server cannot process the requests. For example, when the RADIUS server is down during the STP convergence, a discard filter is added for non-EAP clients. The RADIUS request for the non-EAP clients times out and is dropped. That is, the non-EAP clients are discarded and never get a chance to be authenticated. In addition, if the RADIUS queue is full and more RADIUS requests come in, all those additional RADIUS requests are dropped.

To solve this issue, in Ethernet Routing Switch 8300 software release 2.2 the authentication status of the non-EAP client changes from pending to radius-server-not-reachable when the RADIUS request of a non-EAP client times out. Also, when the RADIUS request of a non-EAP client is dropped due to insufficient space in the RADIUS queue, the authentication status of the non-EAP client is changed to radius-request-dropped.

The discarded RADIUS non-EAP clients (with an authentication status of radius-request-dropped or radius-server-not-reachable) receive another chance to be authenticated when one of the following occurs:

- The discard-filter-ageout timer (configured by the user) expires. By default, the discard-filter-ageout value is 10 seconds. The user can configure it to a value in the range of 5–3600 seconds.
- Traffic from the RADIUS server is received.

In addition, a consistency check prevents enabling EAP and unknown-mac-discard together.

Configuring EAPoL multihosts on a port

You can configure up to eight EAPoL clients (hosts) on each of your switch ports. You can display status and session information about the clients on each of the configured ports.

This section includes the following topics:

- [“Enabling or disabling multiple clients on switch ports,”](#) next
- [“Displaying multiple clients statistics”](#) on page 143
- [“Displaying multiple clients session information”](#) on page 145

Enabling or disabling multiple clients on switch ports

To configure EAPoL multihosts on one or more ports:

- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click the selected port.
 - Select **Edit** from the shortcut menu.
 - Select **Edit > Port** from the Device Manager main menu.
 - Click **Edit** on the toolbar.

The **Port** dialog box for a single port opens with the **Interface** tab selected (see [Figure 43 on page 133](#)).

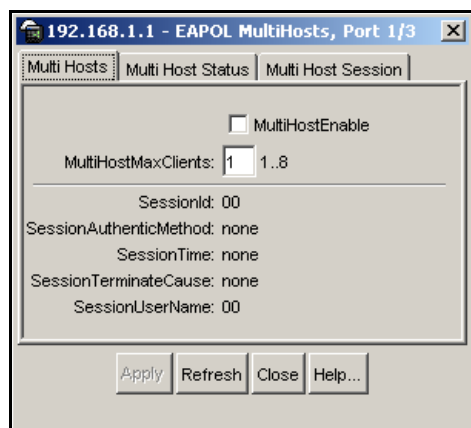
- 3 Click the **EAPOL** tab.

The **EAPOL** tab opens (see [Figure 44 on page 134](#)).

- 4 Click **Multi Hosts**.

The **EAPOL MultiHosts** dialog box opens with the **Multi Hosts** tab selected ([Figure 49](#)).

Figure 49 EAPOL MultiHosts dialog box — Multi Hosts tab



[Table 27 on page 143](#) describes the **Multi Hosts** tab fields.

Table 27 Port dialog box — Multi Hosts tab fields

Field	Description								
MultiHostEnable	Allows you to enable or disable multiple EAPoL clients on the port. Click in the field to enable the feature. <ul style="list-style-type: none"> The default setting is disable (unchecked). Click the checkbox (enter a checkmark) to enable the feature. 								
MultiHostMaxClients	Sets the maximum number of EAPoL hosts for the port. <ul style="list-style-type: none"> 1..8 indicates that you enter an integer value in the range 1 and 8, which specifies the maximum number of hosts that can reside on this port. 								
SessionId	Read-only field—displays a unique identifier for the session that is at least three characters.								
SessionAuthenticMethod	Read-only field—displays the authentication method (remote or local RADIUS server) used to establish the session.								
SessionTime	Read-only field—displays the duration of the session (in days, hours, minutes, and seconds).								
SessionTerminateCause	Read-only field—displays the reason for the session being terminated. The possible reasons are: <table style="margin-left: 20px; border: none;"> <tr> <td>Supplicant logoff</td> <td>Port failure</td> </tr> <tr> <td>Supplicant restart</td> <td>Re-authentication failed</td> </tr> <tr> <td>Control force unauthorized</td> <td>Port re-initialized</td> </tr> <tr> <td>Port admin disabled</td> <td>Not terminated</td> </tr> </table>	Supplicant logoff	Port failure	Supplicant restart	Re-authentication failed	Control force unauthorized	Port re-initialized	Port admin disabled	Not terminated
Supplicant logoff	Port failure								
Supplicant restart	Re-authentication failed								
Control force unauthorized	Port re-initialized								
Port admin disabled	Not terminated								
SessionUserName	Read-only field—displays the user name of the Supplicant PAE.								

Displaying multiple clients statistics

To display statistics about multiple clients configured on one or more ports:

- 1 Select the port you want to display.
- 2 Do one of the following:
 - Double-click the selected port.
 - Select **Edit** from the shortcut menu.
 - Select **Edit > Port** from the Device Manager main menu.

- Click **Edit** on the toolbar.

The **Port** dialog box for a single port opens with the **Interface** tab selected (see [Figure 43 on page 133](#)).

- 3 Click the **EAPOL** tab.

The **EAPOL** tab opens (see [Figure 44 on page 134](#)).

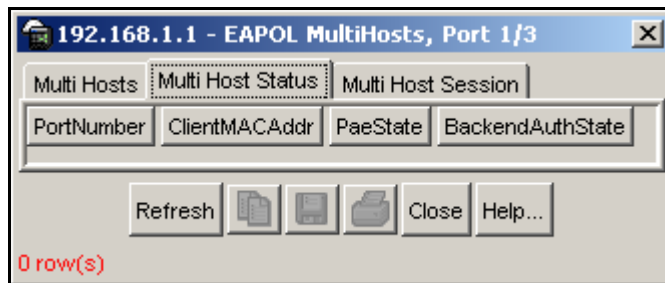
- 4 Click **Multi Hosts**.

The **EAPOL MultiHosts** dialog box opens, with the **Multi Hosts** tab selected ([Figure 49 on page 142](#)).

- 5 Click the **Multi Host Status** tab.

The **Multi Host Status** tab opens and displays statistics about clients configured on each switch port ([Figure 50](#)).

Figure 50 EAPOL MultiHosts dialog box — Multi Hosts Status tab



- 6 Click **Refresh** to display current information about your switch ports.

[Table 28](#) describes the **Multi Host Status** tab fields.

Table 28 Port dialog box — Multi Host Status tab fields

Field	Description
PortNumber	Lists the port number for the displayed statistics.
ClientMACAddr	Displays the client's MAC address.

Table 28 Port dialog box — Multi Host Status tab fields (continued)

Field	Description
PAEState	Displays the current Authenticator PAE state. The possible states are: initialized disconnected connecting authenticating authenticated aborting held forceAuth forceUnauth
BackendAuthState	Displays the current state of Backend Authentication. The possible states are: request response success fail timeout idle initialize

Displaying multiple clients session information

To display information about multiple client sessions configured on one or more ports:

- 1 Select the port you want to display.
- 2 Do one of the following:
 - Double-click the selected port.
 - Select **Edit** from the shortcut menu.
 - Select **Edit > Port** from the Device Manager main menu,.
 - Click **Edit** on the toolbar.

The **Port** dialog box for a single port opens with the **Interface** tab selected (see [Figure 43 on page 133](#)).

- 3 Click the **EAPOL** tab.

The **EAPOL** tab opens (see [Figure 44 on page 134](#)).

- 4 Click **Multi Hosts**.

The **EAPOL MultiHosts** dialog box opens with the **Multi Hosts** tab selected ([Figure 49 on page 142](#)).

- 5 Click the **Multi Host Session** tab.

The **Multi Hosts Session** tab opens and displays session information about clients configured on each switch port ([Figure 51 on page 146](#)).

Enabling or disabling Guest VLANs on a port

To enable or disable Guest VLANs on one or more ports:

- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click the selected port.
 - Select **Edit** from the shortcut menu.
 - Select **Edit > Port** from the Device Manager main menu.
 - Click **Edit** on the toolbar.

The **Port** dialog box for a single port opens with the **Interface** tab selected (see [Figure 43 on page 133](#)).

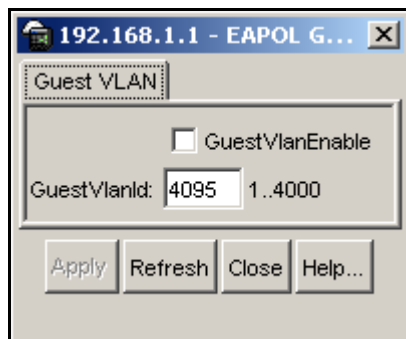
- 3 Click the **EAPOL** tab.

The **EAPOL** tab opens (see [Figure 44 on page 134](#)).

- 4 Click **Guest VLAN**.

The **EAPOL Guest VLAN** dialog box opens with the **Guest VLAN** tab selected ([Figure 52](#)).

Figure 52 EAPOL Guest VLAN dialog box — Guest VLAN tab



- 5 Enter an integer value in the **GuestVlanId** field (in the range 1–4000) that represents the unique VLAN identification.



Note: You cannot modify the **GuestVlanId** field when the **GuestVlanEnable** field is enabled.

- 6 Select the **GuestVlanEnable** check box to enable Guest VLAN on the switch port. Clear the **GuestVlanEnable** check box to disable Guest VLAN.
The default setting is disable (unchecked).
- 7 Click **Apply** to save your configuration.

Changing the authentication status of a port

By default, ports are **forceAuthorized**. This means that the ports are always authorized and are not authenticated by the RADIUS server.

You can change this setting so that the ports are always unauthorized (**forceUnauthorized**). You can also make the ports controlled so that they are automatically authenticated when you globally enable EAPoL (**auto**). The **auto** setting automatically authenticates the port according to the results of the RADIUS server.

To change the authentication status:

- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click the selected port.
 - Select **Edit** from the shortcut menu.
 - Select **Edit > Port** from the Device Manager main menu.
 - Click **Edit** on the toolbar.

The **Port** dialog box for a single port opens with the **Interface** tab selected ([Figure 43 on page 133](#)).

- 3 Click the **EAPOL** tab.
The **EAPOL** tab opens ([Figure 44 on page 134](#)).
- 4 Select one of the following in the **AuthControlledPortControl** field:
 - **forceUnauthorized** — sets the port so it is always unauthorized.
 - **auto** — sets the port to match the global EAPoL authentication setting.
 - **forceAuthorized** — sets the port so it is always authorized (default).

Graphing EAPoL statistics

The Ethernet Routing Switch 8300 provides the following graphing tools to help you monitor and troubleshoot your switch:

- [Graphing EAPoL Authenticator statistics](#)
- [Graphing EAPoL diagnostic statistics](#)
- [Graphing EAPoL session statistics](#)

Graphing EAPoL Authenticator statistics

To display the Authenticator PAE statistics for each selected port:

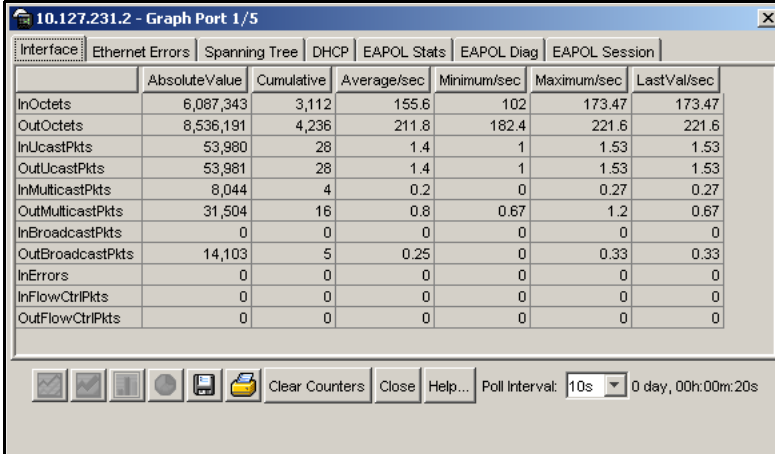
- 1 Select the port or ports you want to graph.



Note: To select multiple ports, press and hold the **Ctrl** key while left-clicking the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:
 - Select **Graph > Port** from the Device Manager main menu.
 - Select **Graph** from the shortcut menu.
 - Click **Graph** on the toolbar.

The **Port** dialog box for a single port or for multiple ports opens with the **Interface** tab selected ([Figure 53 on page 150](#)).

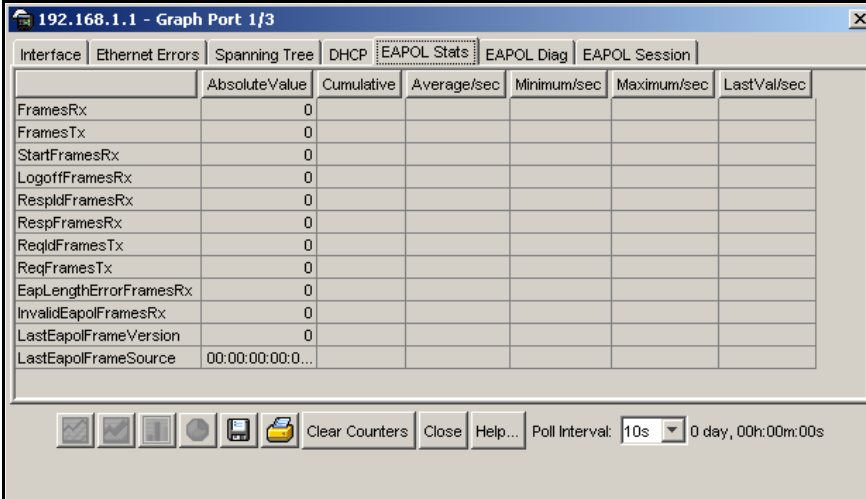
Figure 53 Graph Port dialog box — Interface tab


	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
InOctets	6,087,343	3,112	155.6	102	173.47	173.47
OutOctets	8,536,191	4,236	211.8	182.4	221.6	221.6
InUcastPkts	53,980	28	1.4	1	1.53	1.53
OutUcastPkts	53,981	28	1.4	1	1.53	1.53
InMulticastPkts	8,044	4	0.2	0	0.27	0.27
OutMulticastPkts	31,504	16	0.8	0.67	1.2	0.67
InBroadcastPkts	0	0	0	0	0	0
OutBroadcastPkts	14,103	5	0.25	0	0.33	0.33
InErrors	0	0	0	0	0	0
InFlowCtrlPkts	0	0	0	0	0	0
OutFlowCtrlPkts	0	0	0	0	0	0

Clear Counters Close Help... Poll Interval: 10s 0 day, 00h:00m:20s

3 Click **EAPOL Stats**.

The **EAPOL Stats** tab opens (Figure 54). In this example, port 1/3 has been selected.

Figure 54 Graph Port dialog box — EAPOL Stats tab


	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
FramesRx	0					
FramesTx	0					
StartFramesRx	0					
LogoffFramesRx	0					
RespldFramesRx	0					
RespFramesRx	0					
ReqldFramesTx	0					
ReqFramesTx	0					
EapLengthErrorFramesRx	0					
InvalidEapolFramesRx	0					
LastEapolFrameVersion	0					
LastEapolFrameSource	00:00:00:00:0...					

Clear Counters Close Help... Poll Interval: 10s 0 day, 00h:00m:00s

Table 30 on page 151 describes the **EAPOL Stats** tab fields.

Table 30 Graph Port dialog box — EAPoL Stats tab fields

Field	Description
FramesRx	Displays the number of valid EAPoL frames of any type that have been received by this Authenticator.
FramesTx	Displays the number of EAPoL frame types of any type that have been transmitted by this Authenticator.
StartFramesRx	Displays the number of EAPoL start frames that have been received by this Authenticator.
LogoffFramesRx	Displays the number of EAPoL Logoff frames that have been received by this Authenticator.
RespIdFramesRx	Displays the number of EAPoL Resp/Id frames that have been received by this Authenticator.
RespFramesRx	Displays the number of valid EAP Response frames (Other than Resp/Id frames) that have been received by this Authenticator.
ReqIdFramesTx	Displays the number of EAPoL Req/Id frames that have been transmitted by this Authenticator.
ReqFramesTx	Displays the number of EAP Req/Id frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
EapLengthErrorFramesRx	Displays the number of EAPoL frames that have been received by this Authenticator in which the packet body length field is not valid.
InvalidEapolFramesRx	Displays the number of EAPoL frames that have been received by this Authenticator in which the frame type is not recognized.
LastEapolFrameVersion	Displays the protocol version number that was in the most recently received EAPoL frame.
LastEapolFrameSource	Displays the source MAC address that was in the most recently received EAPoL frame.

Graphing EAPoL diagnostic statistics

To display the Authenticator PAE diagnostic statistics for each selected port:

- 1 Select the port or ports you want to graph.



Note: To select multiple ports, press and hold the **Ctrl** key while left-clicking the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- Select **Graph > Port** from the Device Manager main menu.
- Select **Graph** from the shortcut menu.
- Click **Graph** on the toolbar.

The **Port** dialog box for a single port, or for multiple ports, opens with the **Interface** tab selected (Figure 53 on page 150).

3 Click **EAPOL Diag**.

The **EAPOL Diag** tab opens (Figure 55). In this example, port 1/3 is selected.

Figure 55 Graph Port dialog box — EAPOL Diag tab

	Absolute Value	Cumulative	Average/sec	Minimum/sec	Maximum/sec	Last Val/sec
EntersConnecting	0					
EapLogoffsWhileConnecting	0					
EntersAuthenticating	0					
AuthSuccessWhileAuthenticating	0					
AuthTimeoutsWhileAuthenticating	0					
AuthFailWhileAuthenticating	0					
AuthReauthsWhileAuthenticating	0					
AuthEapStartsWhileAuthenticating	0					
AuthEapLogoffWhileAuthenticating	0					
AuthReauthsWhileAuthenticated	0					
AuthEapStartsWhileAuthenticated	0					
AuthEapLogoffWhileAuthenticated	0					
BackendResponses	0					
BackendAccessChallenges	0					
BackendOtherRequestsToSupplicant	0					
BackendNonNakResponsesFromSupplicant	0					
BackendAuthSuccesses	0					
BackendAuthFails	0					

Table 31 on page 153 describes the **EAPOL Diag** tab fields.

Table 31 Graph Port dialog box — EAPoL Diag tab fields

Field	Description
EntersConnecting	Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPoL-Logoff message.
EntersAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/Identity message being received from the Supplicant.
AuthSuccessWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the Supplicant.
AuthTimeoutsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout.
AuthFailWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure.
AuthReauthsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPoL-Start message being received from the Supplicant.
AuthEapLogoffWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPoL-Logoff message being received from the Supplicant.
AuthReauthsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of a reauthentication request.

Table 31 Graph Port dialog box — EAPoL Diag tab fields (continued)

Field	Description
AuthEapStartsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of an EAPoL-Start message being received from the Supplicant.
AuthEapLogoffWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Disconnected as a result of an EAPoL-Logoff message being received from the Supplicant.
BackendResponses	Counts the number of times that the Backend Authentication state machine sends an Initial-Access request packet to the Authentication server.
BackendAccessChallenges	Counts the number of times that the Backend Authentication state machine receives an Initial-Access challenge packet from the Authentication server.
BackendOtherRequestsToSupplicant	Counts the number of times that the Backend Authentication state machine sends an EAP request packet (other than an Identity, Notification, failure, or success message) to the Supplicant.
BackendNonNakResponsesFromSupplicant	Counts the number of times that the Backend Authentication state machine receives a response from the Supplicant to an initial EAP request and the response is something other than EAP-NAK.
BackendAuthSuccesses	Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server.
BackendAuthFails	Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server.

Graphing EAPoL session statistics

To display the Authenticator PAE statistics for each session that is still in progress, and the final values for ports where there is no currently active session:

- 1 Select the port or ports you want to graph.



Note: To select multiple ports, press and hold the **Ctrl** key while left-clicking the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- Select **Graph > Port** from the Device Manager main menu.
- Select **Graph** from the shortcut menu.
- Click **Graph** on the toolbar.

The **Port** dialog box for a single port, or for multiple ports, opens with the **Interface** tab selected (Figure 53 on page 150).

3 Click **EAPOL Session**.

The **EAPOL Session** tab opens (Figure 56). In this example, ports 8/25, 8/27, and 8/29 are selected.

Figure 56 Graph Port dialog box — EAPOL Session tab

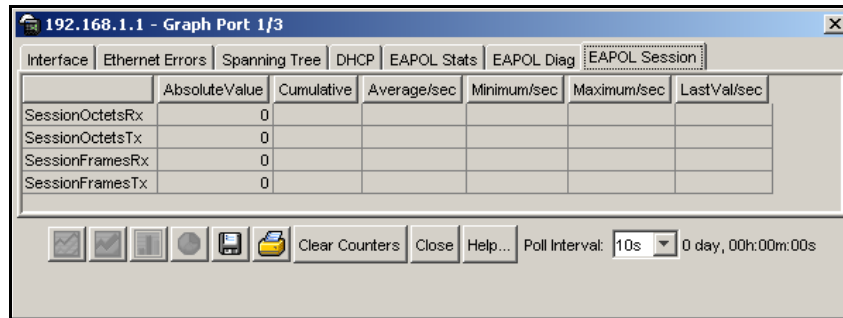


Table 32 describes the **EAPOL Session** tab fields.

Table 32 Graph Port dialog box—EAPOL Session tab fields

Field	Description
SessionOctetsRx	Displays the number of octets received in user data frames on this port during the session.
SessionOctetsTx	Displays the number of octets transmitted in user data frames on this port during the session.
SessionFramesRx	Displays the number of user data frames received on this port during the session.
SessionFramesTx	Displays the number of user data frames transmitted on this port during the session.

Table 32 Graph Port dialog box—EAPoL Session tab fields (continued)

Field	Description
SessionId	Displays a unique identifier for the session that is at least three characters.
SessionAuthenticMethod	Displays the authentication method (remote or local RADIUS server) used to establish the session.
SessionTime	Displays the duration of the session (in seconds).
SessionTerminateCause	Displays the reason for the session being terminated. The possible reasons are: 1=supplicantLogoff 2=portFailure 3=supplicantRestart 4=reauthFailed 5=authControlForceUnauth 6=portReinit 7=portAdminDisabled 999=notTerminatedYet
SessionUserName	Displays the user name of the Supplicant PAE.

Chapter 9

Configuring TACACS+

This chapter describes how to configure TACACS+ using Device Manager. For more information about TACACS+, see [Chapter 1, “Overview of security features,” on page 19](#).

This chapter includes the following topics:

Topic	Page
Configuration prerequisites	157
Configuring TACACS+ globally	157
Adding a TACACS+ server	158
Modifying a TACACS+ configuration	160
Deleting a TACACS+ configuration	161

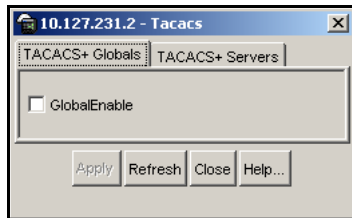
Configuration prerequisites

Before configuring your switch, you must configure at least one TACACS+ server (and shared secret).

Configuring TACACS+ globally

To enable TACACS+ globally on the switch:

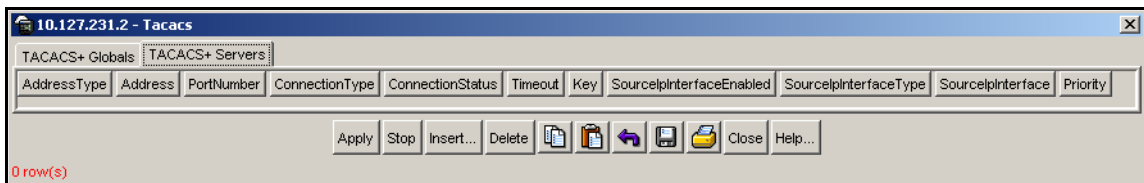
- 1 Select **Edit > Security > TACACS+** from the Device Manager main menu. The **Tacacs** dialog box opens with the **TACACS+ Globals** tab selected (see [Figure 57 on page 158](#)).

Figure 57 Tacacs dialog box — TACACS+ Globals tab

- 2 Select the **GlobalEnable** check box to enable TACACS+ globally on the switch.
- 3 Click **Apply** to save your changes.

Adding a TACACS+ server

- 1 Select **Edit > Security > TACACS+** from the Device Manager menu bar.
The **Tacacs** dialog box opens with the **TACACS+ Globals** tab selected (see [Figure 57](#)).
- 2 Click the **TACACS+ Servers** tab.
The **TACACS+ Servers** tab opens ([Figure 58](#)).

Figure 58 Tacacs dialog box — TACACS+ Servers tab

- 3 Click **Insert**.
The **Tacacs, Insert TACACS+ Servers** dialog box opens ([Figure 59 on page 159](#)).

Figure 59 Tacacs, Insert TACACS+ Servers dialog box

4 Enter the appropriate values.

5 Click **Apply**.

The information for the configured TACACS+ server appears on the **TACACS+ Servers** tab of the **Tacacs** dialog box.

6 Save your configuration.

[Table 33](#) describes the fields on the **TACACS+ Servers** tab and the **Tacacs, Insert TACACS+ Servers** dialog box.

Table 33 TACACS+ Servers tab and Insert TACACS+ Servers dialog box fields

Field	Description
AddressType	Specifies the type of IP address (IPv4 or IPv6) used on the TACACS+ server. Note: For the current software release, you must set the value to IPv4.
Address	The IP address of the TACACS+ server.
PortNumber	The TCP port on which the client establishes a connection to the server. The default is port number 49.

Table 33 TACACS+ Servers tab and Insert TACACS+ Servers dialog box fields

Field	Description
ConnectionType	Specifies the TCP connection type between a device and the TACACS+ server. Either a single open connection between a device and server (singleConnection), or open/close connection per communication session (perSessionConnection)
ConnectionStatus	Specifies the status of the TCP connection between a device and the TACACS+ server. Note: For the current software release, this field is unavailable.
Timeout	The maximum time (in seconds) to wait for this TACACS+ server to reply.
Key	The secret key to be shared with the TACACS+ server. String length is a 1–128 characters.
SourceIpInterfaceEnabled	Enables the source address specification. If SourceIpInterfaceEnabled is true (the check box is selected), and you change SourceIpInterfaceEnabled to false (the check box is cleared), the SourceIpInterface is reset to 0.0.0.0.
SourceIpInterfaceType	Specifies the type of IP address (IPv4 or IPv6) used on the interface that connects to the TACACS+ server. Note: For the current software release, you must set the value to IPv4.
SourceIpInterface	The IP address of the interface to use with the server. A value of 0.0.0.0 for this object disables the source address specification.
Priority	Determines the order in which the TACACS+ servers are used, where 1 is the highest priority. The priority value must be unique for each server.

Modifying a TACACS+ configuration

To modify an existing TACACS+ configuration:

- 1 Select **Edit > Security > TACACS+** from the Device Manager menu bar.
The **Tacacs** dialog box opens with the **TACACS+ Globals** tab selected (see [Figure 57 on page 158](#)).
- 2 Click the **TACACS+ Servers** tab.

The **TACACS+ Servers** tab opens (see [Figure 58 on page 158](#)).

- 3 Type new information in the row you want to modify, or use the lists to make a selection.

Access the lists by double-clicking in a field.

- 4 Click **Apply**.
- 5 Save your configuration, if necessary.

Deleting a TACACS+ configuration

To delete an existing TACACS+ configuration:

- 1 Select **Edit > Security > TACACS+** from the Device Manager menu bar.
The **Tacacs** dialog box opens with the **TACACS+ Globals** tab selected (see [Figure 57 on page 158](#)).
- 2 Click the **TACACS+ Servers** tab.
The **TACACS+ Servers** tab opens (see [Figure 58 on page 158](#)).
- 3 Identify the configuration to delete by clicking anywhere in the row.
- 4 Click **Delete**.

Index

Numbers

3DES encryption 27

A

access policies

 configuring 79

 overview of 20

authentication

 DSA 27

 RSA 27

authentication server 37

authenticator 36

B

BSAC RADIUS servers

 configuring 111, 113

 updating files for 110

C

Community Table dialog box 99

Community Table tab fields 100

controlled port 37

conventions, text 14

customer support 17

D

dialog box

 Community Table 99

 Group Access Right 95

 Group Membership 93

 Insert Community Table 99

 MIB View 97

 USM Table 90

 VACM Table 93

DSA authentication 27

E

EAPoL

 AuthControlledPortControl 135

 AuthControlledPortStatus 135

 authentication server 37

 authenticator 36

 BackendAuthState 135

 configuration example 38

 configuration prerequisites 130

 configuration process 37

 configuring authentication status 148

 configuring globally 130

 configuring ports 132, 136, 142, 143, 145, 147

 configuring RADIUS 61

 controlled port 37

 description 36

 graphing AuthStats 149

 graphing DiagStats 151

 graphing SessionStats 154

 MaxReq 136

 PaeState 135

 port access entity (PAE) 37

 PortInitialize 135

 PortReauthenticate 135

 QuietPeriod 136

 ReAuthEnabled 136

 ReAuthPeriod 136

 ServerTimeout 136

 supplicant 36

- SuppTimeout 136
- system requirements 66
- TxPeriod 136
- VLANs, dynamic assignment 56

encryption

- 3DES 27

Extensible Authentication Protocol over LAN. *See* EAPoL

F

freeRadius servers, configuring 113

G

graphing

- Authenticator statistics 149
- Diagnostic statistics 151
- EAPoL session statistics 154

Group Access Right dialog box 95

Group Access tab fields 96

Group Membership dialog box 93

Group Membership tab fields 94

I

initialize EAPoL port 135

Insert Community Table dialog box 99

IP Globals tab

- fields 92

M

Merit Network servers, configuring 112

MIB View dialog box 97

MIB View tab fields 98

P

passwords, setting 71

port access entity (PAE) 37

port lock feature

configuring 75

- overview of 20

product support 17

publications

- hard copy 16

R

RADIUS

accounting

- overview of 34

authentication

- enabling 119, 122
- overview of 34

client 61

deleting the configuration, using Device Manager 128, 161

modifying the configuration, using Device Manager 127

overview of 31

servers

- adding, using Device Manager 122
- using third party 110, 115
- vendor-specific attributes 61

RADIUS, configuring for EAPoL 61

reauthenticate EAPoL port 135

Remote Access Dial-In User Services, *see* RADIUS

RSA authentication 27

S

Secure Shell

- supported clients 104

Secure Shell version 2 (SSH-2)

- overview 28

servers

- configuring BSAC RADIUS 111, 113
- freeRadius, configuring 113
- Merit Network, configuring 112
- using third-party RADIUS 110, 115

SSH version 2 (SSH-2)

- overview 28

supplicant 36
support, Nortel 17

T

TACACS+
 configuration prerequisites 157
 modifying the configuration, using Device
 Manager 160
technical publications 16
technical support 17
text conventions 14

U

USM dialog box 90
USM tab fields 90

V

VACM tab fields 93
VACM Table dialog box 93
vendor-specific attributes 61
VLANs, EAPoL dynamic assignment 56

