Part No. 316343-B Rev 00
May 2004

4655 Great America Parkway
Santa Clara, CA 95054

Configuring Internet Membership Group Authentication Protocol (IGAP)

Passport 8000 Series Software Release 3.7

NORTEL NETWORKS™

Copyright © 2004 Nortel Networks

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

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

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and [other Nortel trademarked product names] are trademarks of Nortel Networks.

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

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 MERCHANTABLITITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

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

4. General

a) If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

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

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

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

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

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

Contents

Figures

Tables

Preface

This manual describes the IGMP for Internet Membership Group Authentication Protocol (IGAP) and how it is implemented in the Passport* 8000 Series switches. This includes how to configure an IGAP-enabled RADIUS server.

This manual consists of the following three chapters:

- Chapter 1 provides an overview of IGAP and describes its basic concepts. It also explains how IGAP works with other multicast protocols.

- Chapter 2 describes how to configure IGAP and RADIUS using the Device Manager graphical user interface (GUI).

- Chapter 3 describes how to configure IGAP and RADIUS using the command line interface (CLI).

Before you begin

This document is intended for network administrators who have:

- A basic knowledge of networks and IP routing
- Some familiarity with networking concepts and terminology
- A basic knowledge of network topologies
- Experience with windowing systems or GUIs

Text conventions

This guide uses the following text conventions:

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

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

Acronyms

This guide uses the following acronyms:

CHAP	Challenge Handshake Authentication Protocol for PPP
IETF	Internet Engineering Task Force
IGAP	IGMP for user Authentication Protocol
IGMP	Internet Group Management Protocol
MAC	media access control
PAP	Password Authentication Protocol for PPP
PIM-SM	Protocol Independent Multicast - Sparse Mode
RADIUS	Remote Access Dial-In User Services
VLAN	virtual LAN

Hard-copy technical manuals

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

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

How to get help

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

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

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

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

Chapter 1
IGAP concepts

IGMP for Internet Membership Group Authentication Protocol (IGAP) is an authentication and accounting protocol for clients receiving multicast streams. With IGMP and existing multicast protocols, users can join an IP multicast group and receive all the multicast traffic that any other member in the group had access to. With IGAP's authentication and accounting features, service providers and enterprises have more control over their networks and can better manage the multicast groups on their networks.

IGAP is an IETF Internet draft that extends the functionality of the Internet Group Management Protocol (IGMPv2), and uses a standard authentication server like RADIUS with extensions for IGAP. This manual describes IGAP concepts and explains how to configure IGAP services. For more information about other multicast protocols and to learn how to configure them, refer to the publication, *Configuring IP Multicast Protocols.*

This chapter discusses the following topics:

Overview

In traditional *shared access* IP multicast networks, service providers have no control over user access (authentication) and no means of generating revenue (accounting). Users can join an IP multicast group and receive all the multicast traffic that any other member in the group has access to. Now that many service providers and enterprises have their own *non-shared* access networks such as dial, DSL or switched Ethernet, providers have more control over their networks.

IGAP extends that control by using RADIUS to add authentication and accounting functionality. Unlike with other multicast protocols, members cannot join an IGAP host group simply by sending a join message in a report.

Joining an IGAP multicast group

The following process describes how an IP host (IGAP member) interacts with an authentication gateway (Passport 8600) and a RADIUS server to join an IGAP multicast group:

1. IGAP member, who wants to join a specific multicast group, sends an IGAP Report message to a Passport 8600 switch.
2. Passport 8600 checks to see if authentication is needed to join this VLAN.
   a. If authentication **is not required**, the Passport 8600 grants immediate access and the join process stops. For example, authentication is not required for a member that has already been authenticated. This is called a Solicited PAP Join (without authentication ticket), which is sent in response to the basic and general Query message to renew membership.
   b. If authentication **is required**, the Passport 8600 forwards the join request to a RADIUS server for processing. For example, when authentication is required in order to access multicast traffic, any Unsolicited PAP Join (with authentication ticket) received by the Passport 8600 requires authentication. Go on to Step 3.
3. RADIUS server sends authentication results to Passport 8600.

4. Passport 8600 grants or denies the join request based on the authentication results from the RADIUS server. The Passport 8600 informs the IGAP member of the authentication results by sending an IGAP Authentication Query message.

   a. If authentication is **denied**, the Passport 8600 rejects the join request (IGAP report) and does not forward traffic to the user for that group. In cases where a re-authentication (or second join) is denied, the Passport 8600 rejects the join request and stops any traffic that might have been flowing up to this point.

   b. If authentication is **granted**, the Passport 8600 starts sending multicast traffic. Go on to Step 5.

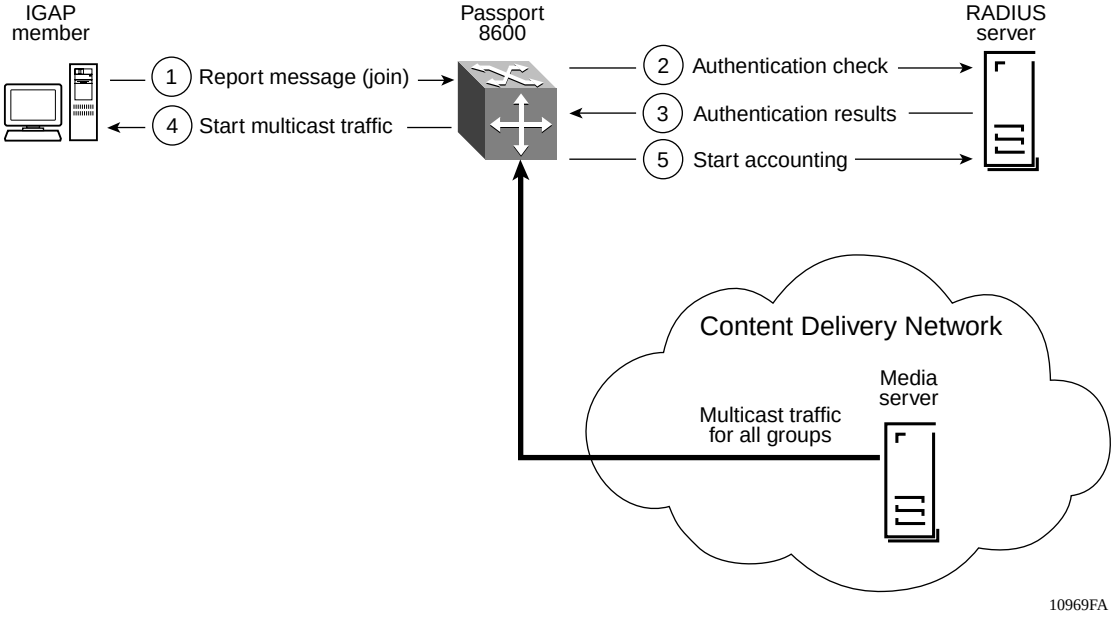
5. If traffic for the requested group is available, the Passport 8600 sends a message to the RADIUS server to start accounting immediately. After the Passport 8600 receives an accounting success message from the RADIUS server, it informs the IGAP member that accounting is starting by sending an IGAP Accounting Query message.

   If traffic is not available, the Passport 8600 waits until traffic starts before sending the accounting start messages to the RADIUS server and to the IGAP member.

   RADIUS server starts the accounting process to track how long the IGAP client receives multicast traffic.

Figure 1 shows an example of how an IGAP member joins a multicast group.

Figure 1 Joining an IGAP multicast group



Leaving an IGAP multicast group

IGAP uses the Passport 8600 Fast Leave feature to terminate members from a multicast group. This feature is useful for multicast-based TV distribution applications. Fast Leave is an alternative leave process in which the switch stops sending traffic to the member or client *immediately* after receiving a leave message, without issuing a group-specific query to check if other group members are present on the interface port.

Nortel Networks extended the Fast Leave feature to support more than one user per interface port so that traffic will not stop if there is more than one user listening to the same group. Fast Leave alleviates the network from additional bandwidth demand when changing TV channels.

The IGAP Fast Leave process consists of the following steps:

1 IGAP member sends an IGAP Leave message to the Passport 8600.

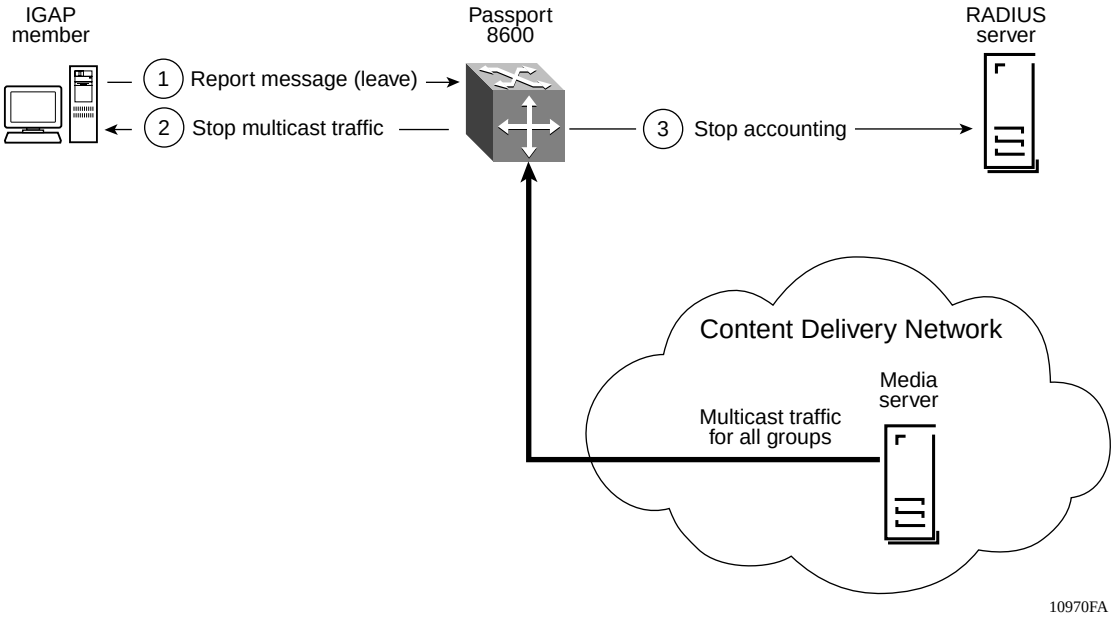
2 Passport 8600 stops sending multicast traffic to the IGAP member. This assumes that no other group members are on the same interface.

3 Passport 8600 directs the RADIUS server to stop accounting.

4 Passport 8600 receives an accounting success response from the RADIUS server and informs the IGAP member that accounting is stopping by sending an IGAP Accounting Query message.

Figure 2 shows an example of how an IGAP member leaves a multicast group.

Figure 2 Leaving an IGAP multicast group



If several receivers are present on the same interface, the Passport 8600 ensures that all receivers have left the group before stopping the traffic. The Passport 8600 performs accounting based on user ID, member IP address and the group joined, but stops the traffic only when all users leave the group. For this process to operate properly, it is expected that every IGAP receiver issues join reports and does not do any report suppression. The advantage of this process is the efficient use of bandwidth and the support of several IGAP clients at the same interface.

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 Passport 8000 Series switch, RADIUS performs the following functions:

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

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.

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, the RADIUS client software resides on the Passport 8600.

For more information about RADIUS, refer to *Configuring and Managing Security.*

Authentication

IGAP uses RADIUS to restrict access to multicast groups by requiring users to be authenticated. Users have to be authorized to get access to a group. For example, employees may have access to a company's network, but they will not be able to attend a restricted video conference unless they have specific access rights.

The Passport 8600 sends periodic *IGAP Query messages* to IGAP hosts on a local network for updates on the current status of members. Hosts respond by issuing *IGAP Report messages* listing their current members that want to receive multicast traffic.

The Passport 8600 uses the Query/Report mechanism to periodically re-authenticate all the host members access to a group. Host members also use this mechanism to join a multicast group. If a member has already been authenticated, you can skip the re-authentication process by excluding the PAP ticket information. This alleviates the authentication process and is called a Solicited PAP Join.

The Passport 8600 identifies each host member with a key, which consists of a combination of the user ID and IP address. If authentication fails, the Passport 8600 automatically terminates access to the multicast group for that member. However, keep in mind that there are situations where you may *not* want to restrict access. For example, a CEO may want all employees to watch a video conference. To facilitate that, IGAP allows you to disable authentication.

To add the authentication functionality, IGAP incorporates an authentication protocol into IGMPv2 that uses a simple password such as the Password Authentication Protocol (PAP).

PAP provides network security by sending a plain text user ID and password to the authenticating/accounting (RADIUS) server. If the RADIUS server doesn't recognize the user, it denies the user access to the network resource. The user ID and password are text strings that identify the ID and password for a specific interface. All authentication requests must contain this ID and password to access the network.

Accounting

IGAP uses the RADIUS accounting feature to track how long an individual user or group of users maintain access to a particular multicast group. IGAP tracks the IGMP leaves and joins per interface or VLAN. This usage tracking enables providers to accurately bill for services or to monitor the popularity of specific programs. For example, Internet TV service providers can collect information on individual users so that they can charge them only for the time they watch a specific TV channel. Providers can also use accounting to monitor overall TV usage and for a specific program. This information will help them with their future programming plans.

The Passport 8600 identifies each host member with a key, which consists of a combination of the user ID and IP address. If accounting fails, the Passport 8600 sends a message notifying the member that accounting (start/stop) failed. However, keep in mind that there are situations where you may *not* want to track usage. For example, if a TV station has to broadcast public service messages periodically, the station management cannot charge for the service and may not be interested in tracking how many users were watching. IGAP allows you to disable accounting.

Using IGAP with other multicast features

IGAP is an extension of IGMPv2 so, naturally, you can use many of the other IGMPv2 parameters. In addition to IGMP, you can use other multicast features to customize your network, including the following:

- IGMP Access Control
- Channel limitation

The following sections summarize these features. For more information and to learn how to configure them, refer to *Configuring IP Multicast Protocols*.

Multicast access control

Multicast access control enhances the security and control you have over your multicast network. It enables you to restrict users from sending or receiving traffic from specific multicast groups. For example, in a TV channel distribution network, you can restrict users from getting TV channels that they are not authorized to watch.

Channel limitation

Channel limitation refers to limiting the number of multicast streams that a user can receive at one time. This limitation allows you to set the maximum number of multicast streams on a VLAN for a given interface. This limitation protects the bandwidth and controls access to multicast streams.

Where IGMP access control places limits on specific channels; channel limitation places limits on the number of multicast channels. You can use this feature in any environment where users should not be getting more than a certain number of concurrent multicast streams. For example, if a customer has a service contract for two TVs and attempts to turn on three TVs at the same time, the Passport 8600 blocks the customer from receiving multicast streams on the third TV.

Chapter 2
Configuring IGAP using Device Manager

IGAP is an authentication and accounting protocol for clients receiving multicast streams. IGAP extends the functionality of the Internet Group Management Protocol (IGMPv2) by giving providers more control over their networks. With IGAP, service providers and enterprises can authenticate users before granting access to their networks and track how long users receive multicast traffic.

This chapter describes how to use Device Manager to configure IGAP. It also describes the commands that display information about the current IGAP configuration. For more information about IGAP concepts, see Chapter 1, "IGAP concepts."

This chapter includes the following topics:

Configuration considerations

- IGAP can be enabled on IGMPv2 interfaces *only.*
- IGAP uses the Fast Leave feature *exclusively* to save bandwidth and enhance the network's efficiency. This feature cannot be disabled.
- Since IGAP uses Fast Leave, it never sends group-specific Query messages in response to a Leave message or use the IGMP Last Member Query Interval (LMQI) parameter.
- Nortel Networks does not recommend using static IGMP members on IGAP-enabled interfaces. Functionally, this means that the Passport 8600 will still send traffic to the member ports of the static multicast group, but it will not authenticate users or account for their traffic usage.
- The Passport 8600 supports IGAP in PIM-SM (sparse mode) only, and not for PIM-SSM (source specific multicast) or DVMRP.
- IGAP does not support spanning VLANs.
- IGAP does not support static port members.
- Nortel Networks recommends that you do not use static (or block) IGMP member ports.

Configuration prerequisites and notes

Before you can configure IGAP, you must create the VLANs that you want to enable with IGAP. Then you must enable PIM-SM globally and on the VLANs you created. For more information on VLANs, refer to the publication, *Configuring IP Routing Operations*.

Creating VLANs

To create a VLAN on the switch, complete the following steps:

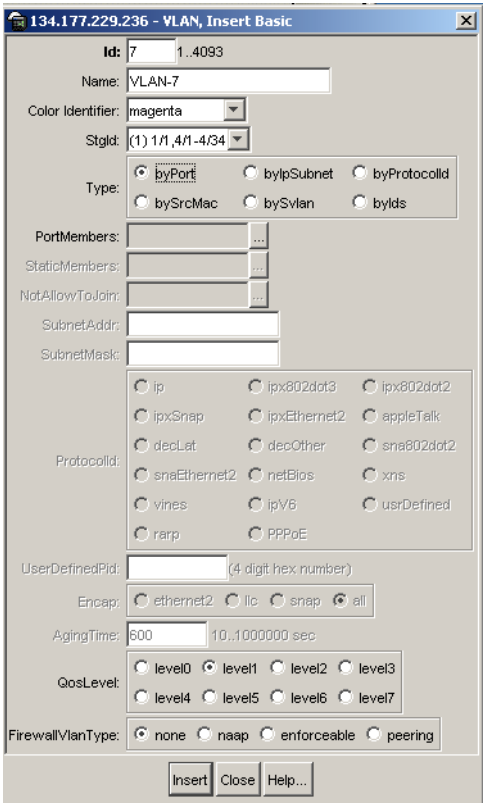
1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens with the Basic tab displayed.

2 Click Insert.

The VLAN, Insert Basic dialog box opens (Figure 3).

Figure 3 VLAN, Insert Basic dialog box



3 Configure the VLAN and click the Insert button.

The new VLAN is displayed in the VLAN dialog box.

4 Select the new VLAN.

The IP button becomes available.

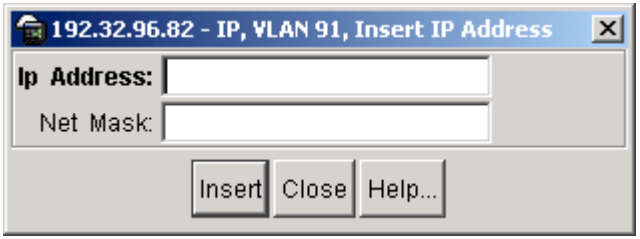
5 Click the IP button.

The IP, VLAN dialog box opens with the IP Address tab displayed.

6 Click Insert.

The IP, VLAN Insert IP Address dialog box opens (Figure 4).

Figure 4 IP, VLAN Insert IP Address dialog box



7 Enter the IP address and network mask you want to assign to this VLAN.

8 Click Insert.

Configuring PIM-SM globally

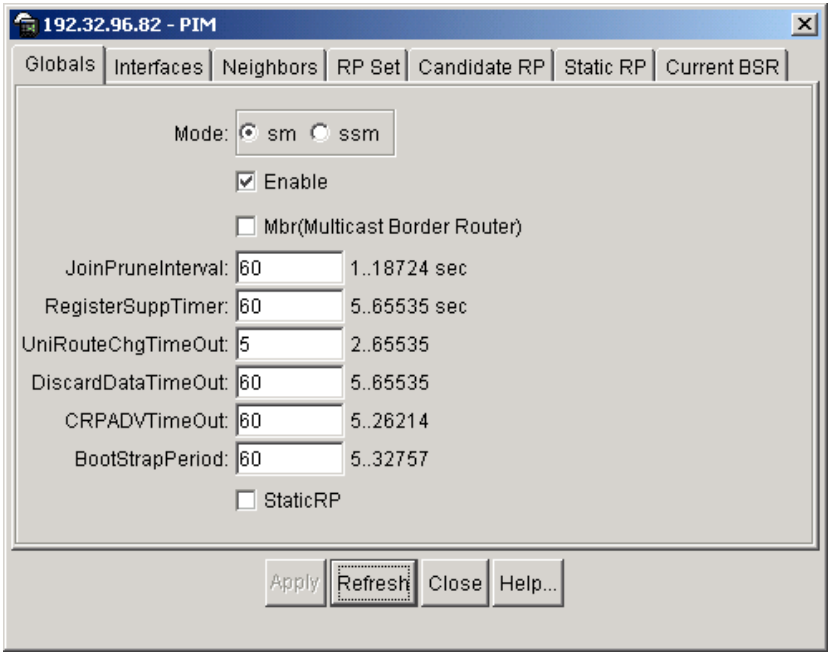
In order for the IGMP and IGAP parameters to take effect, you must enable PIM-SM.

To enable PIM-SM globally:

1 From the Device Manager menu bar, choose IP Routing > PIM.

The PIM dialog box opens with the Globals tab displayed (Figure 5).

Figure 5 PIM dialog box—Globals tab



2 Click Mode: sm (sparse mode).

3 Click Enable.

4 Click Apply.

Configuring PIM-SM on a VLAN

To enable PIM-SM on a specific VLAN:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens with the Basic tab displayed.

2. Select the VLAN ID that you want to configure with PIM-SM.

   Several buttons on the bottom of the dialog box become available.

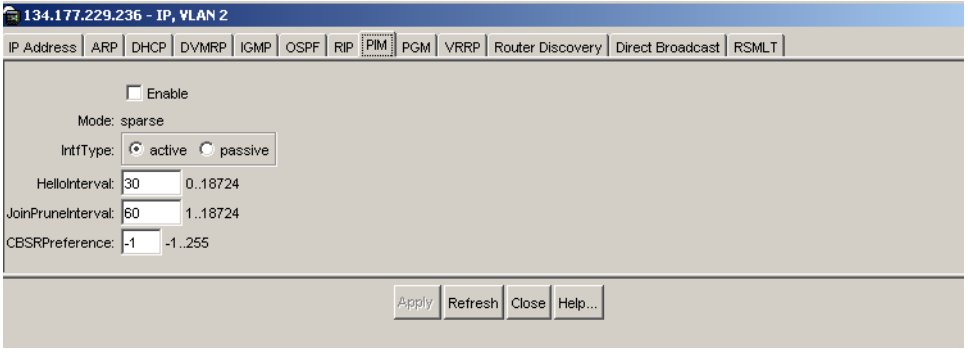
3. Click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.

4. Click the PIM tab.

   The PIM tab opens (Figure 6).

Figure 6 IP VLAN dialog box—PIM tab



5. Check the Enable box.
6. Click Apply.

Configuring IGAP on a VLAN

To configure IGAP on a VLAN:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens, with the Basic tab displayed.

2. Select a VLAN.

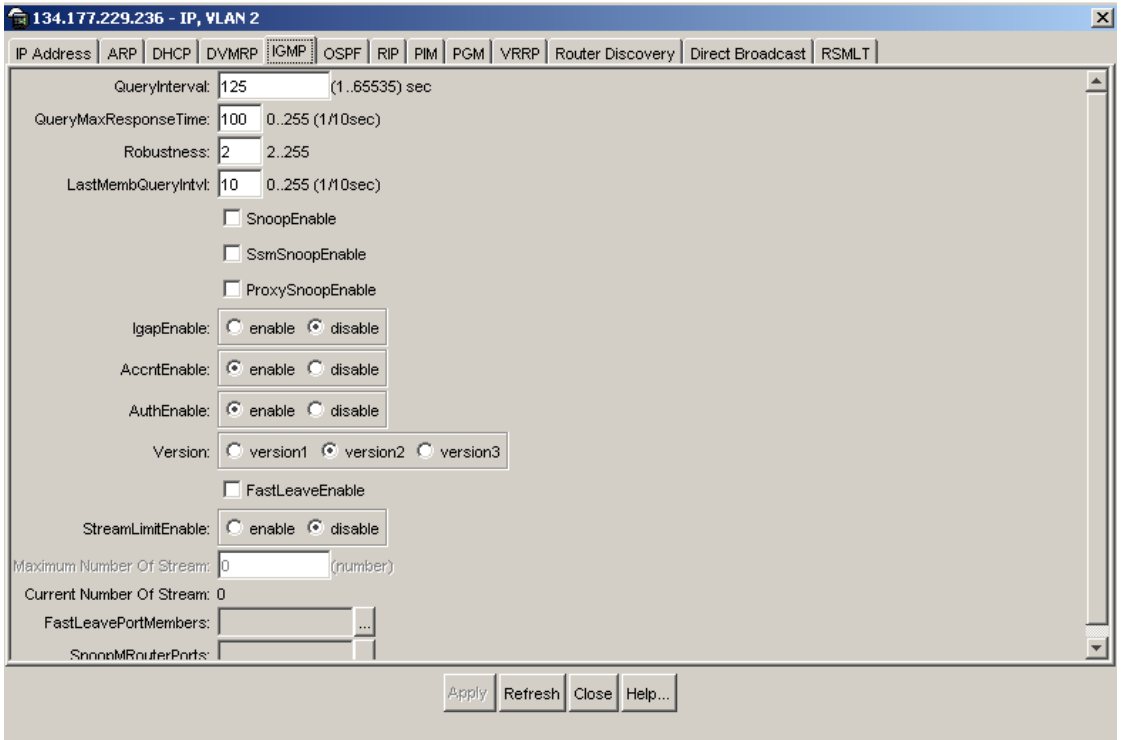
3. Click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.

4. Select IGMP.

   The IGMP tab opens (Figure 7).

Figure 7 IP, VLAN dialog box—IGMP tab



5. Click enable in the IgapEnable field. (The default is disable.)

6 Click enable in the AccntEnable field, if desired. (The default is enable.)

7 Click enable in AuthEnable field, if desired. (The default is enable.)

8 Click version2 in the Version field. (The default is version2.)

9 Check FastLeaveEnable. (When you enable IGAP and click Apply, this field is automatically enabled.)

10 Click Apply.

Configuring IGAP interfaces

To view information about all the IGAP interfaces configured on the switch or to modify their configuration:

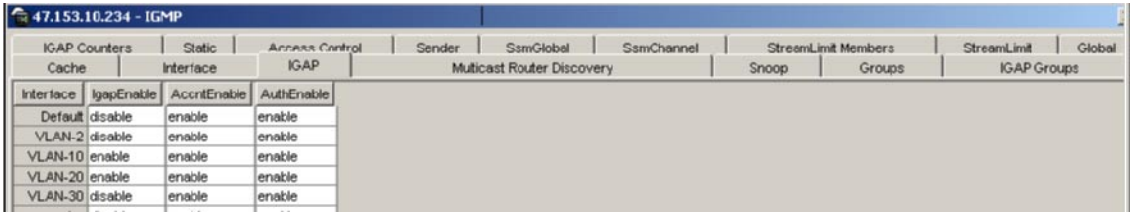
1 From the Device Manager menu bar, choose IP Routing > IGMP.

The IGMP dialog box opens with the Global tab displayed.

2 Click the IGAP tab.

The IGAP tab opens (Figure 8).

Figure 8 IGMP dialog box—IGAP tab



3 Double-click on any interface parameter that you want to modify.

Table 1 describes the IGAP tab fields.

Table 1 IGAP tab fields

Field	Description
IgapEnable	Enables or disables IGAP on this interface.
AccntEnable	Enables or disables IGAP Accounting on this interface.
AuthEnable	Enables or disables IGAP Authentication on this interface.

Displaying IGAP groups

To see how all the IGAP groups on the switch are configured:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Global tab displayed.

2. Click the IGAP Groups tab.

   The IGAP Groups tab opens (Figure 9).

Figure 9 IGMP dialog box—IGAP Groups tab

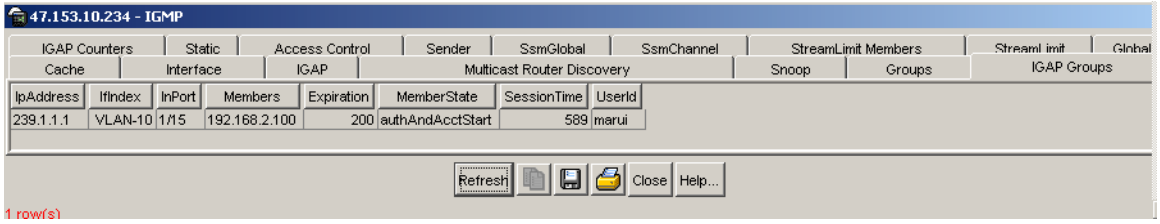


Table 2 describes the IGAP Groups tab fields.

Table 2 IGAP Groups tab fields

Field	Description
IpAddress	Indicates the IP address of this IGAP group.
IfIndex	Displays the VLAN name that uniquely identifies the interface.
InPort	Displays the ingress port of the IGAP report.
Members	Indicates the IP address of this IGAP group member.
Expiration	Specifies how much time is left (in seconds) before the Group Report for this interface expires. This timer is restarted when the RADIUS server receives a new group report.
MemberState	Displays the state of this IGAP group member. • **Auth** indicates that the member was authenticated by a RADIUS server. • **Acct** indicates that a RADIUS server successfully started accounting for this member's session.
SessionTime	Displays the accounting time (in seconds) for the duration of the multicast session for this IGAP group member.
UserId	Displays the user ID for this interface.

Troubleshooting IGAP network connectivity

IGAP counters provide network connectivity information that you can use to monitor and troubleshoot IGAP interfaces.

To display the counter information:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

2. Click the IGAP Counters tab.

   The IGAP Counters tab opens (Figure 10).

Figure 10 IGMP dialog box—IGAP Counters tab

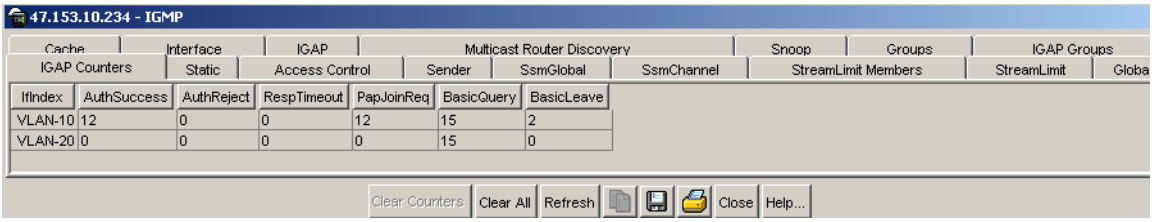


Table 3 describes the IGAP Groups tab fields.

Table 3 IGAP Counters tab fields

Field	Description
IfIndex	Displays the VLAN name that uniquely identifies the interface.
AuthSuccess	Displays the number of authentication success messages received from the RADIUS server on this interface.
AuthReject	Displays the number of authentication fail messages received from the RADIUS server on this interface.
RespTimeout	Displays the number of times that the Authentication Timer timed out. This timer controls the waiting time from sending an Authentication request to receiving an Authentication response.
PapJoin Req	Displays the number of Password Authentication Protocol (PAP) Join requests received for members of this interface.
BasicQuery	Displays the number of Basic Query messages sent by the Passport 8600 on an IGAP-enabled interface.
BasicLeave	Displays the number of Basic Leave messages received by this interface.

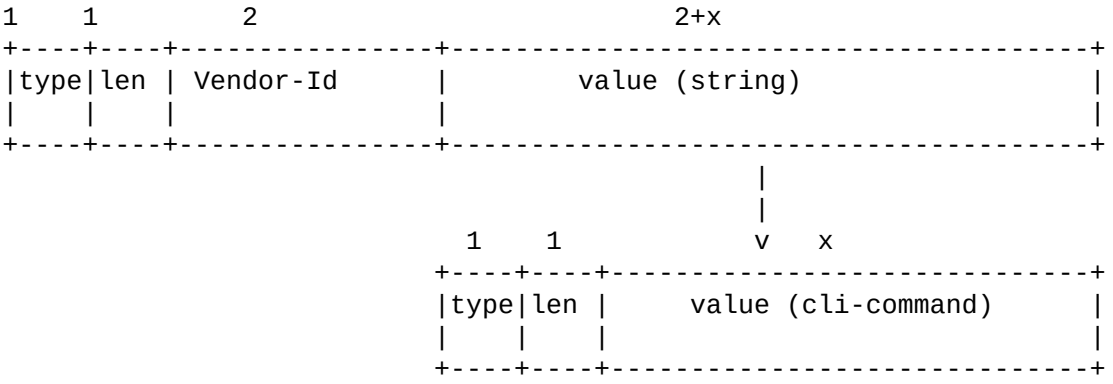
Configuring IGAP with RADIUS

IGAP uses RADIUS servers to authenticate users and account for how long they use the multicast services. This section describes the IGAP-specific RADIUS parameters. For information about the complete set of RADIUS parameters, refer to the publication, *Configuring and Managing Security.*

Setting VSAs for Nortel Networks and third-party servers

Vendor-specific attributes (VSAs) enable the server to recognize RADIUS clients. The Passport 8000 Series software supports BaySecure Access Control (BSAC*) and the Merit Network servers. To use these servers, you must first obtain the software for the server you will use. Also, you must make changes to one or more configuration files for these servers. For detailed information about the changes that must be made for the BSAC server, refer to *Configuring and Managing Security.*

The Nortel Networks vendor ID is 1584, as allocated by the Internet Assigned Numbers Authority. Use this ID in the header when using VSAs. 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:



If you do not have a Nortel Networks server, use the RADIUS dictionary file as a reference to change your existing RADIUS dictionaries. Because this file is in the format of some popular RADIUS servers, you may be able to use it as a direct replacement. However, you should review the dependencies and make a decision on how to apply the differences.

Setting the VSA for the multicast address

To set the vendor-specific attribute (VSA) for the multicast address on an IGAP-enabled RADIUS server:

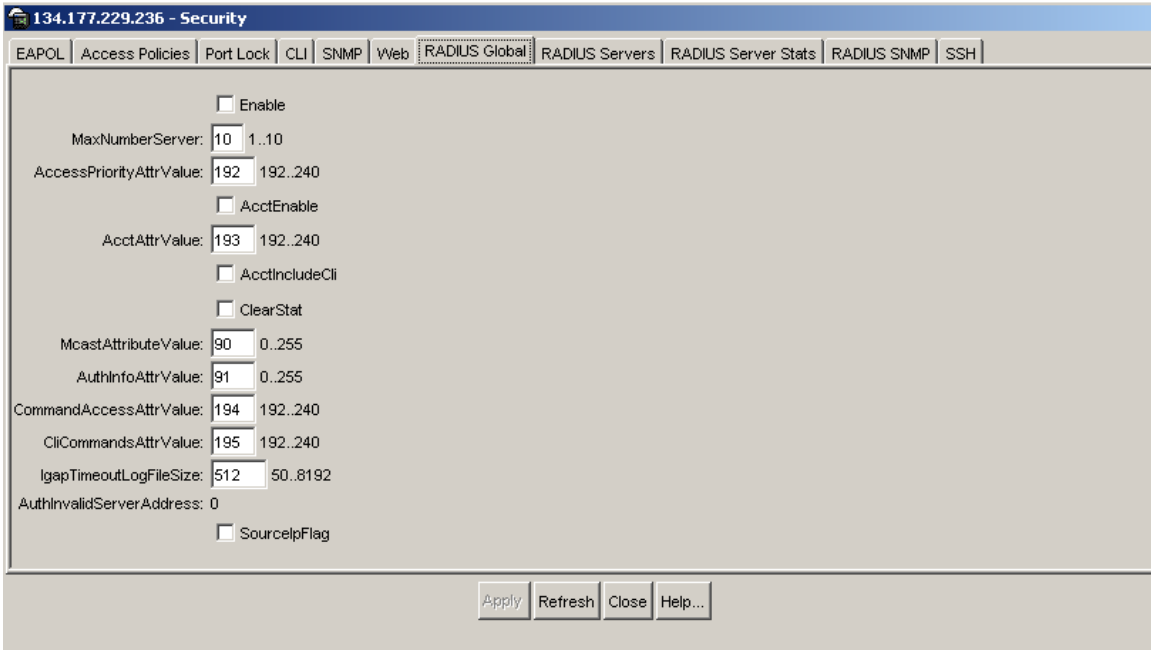
1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the EAPOL tab displayed.

2. Click the RADIUS Global tab.

   The RADIUS Global tab opens (Figure 11).

Figure 11 Security dialog box—RADIUS Global tab



3. Set the vendor-specific McastAttributeValue, which must be in the range from 0 to 255. The default is 90.

4. Set the vendor-specific AuthInfoAttrValue, which must be in the range from 0 to 255. The default is 91.

5 Click Apply.

Note: Do not select the Enable and AcctEnable check boxes. IGAP ignores these check boxes because they are only used when you configure the server for CLI authentication and accounting.

Setting the timeout log file size

The Passport 8600 captures authentication and accounting information in an IGAP timeout log for each session. The timeout log records information such as when the Passport 8600 sent an accounting start request to the RADIUS server, what the server's response was and when accounting started.

To set the size of the timeout log file for an IGAP-enabled RADIUS server:

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

The Security dialog box opens with the EAPOL tab displayed.

2 Click the RADIUS Global tab.

The RADIUS Global tab opens (Figure 11).

3 Set the IgapTimeoutLogFileSize (in KB), which must be in the range from 50 to 8192. The default is 512.

4 Click Apply.

Storing IGAP timeout logs

The Passport 8600 stores the timeout log in a PCMCIA file, which uses the following naming convention:

```
vendorname_nasIPaddress_type_version.log
```

where:
vendorname is a two-character symbol representing the vendor.
In the example shown below, **nr** represents a specific Nortel Networks project.

nasIPaddress identifies the network access server (NAS) by its IP address. In the example shown below, **192168010001** represents the edge node at IP address 192.168.10.1. Note that when there are less than three digits in an octet such as the 10 and 1, leading zeroes fill in to make up the 12 digits. If the Passport 8600 cannot determine NAS IP address, create a file corresponding to NAS IP "0.0.0.0" such as:

```
7672 MAR-17-2003 11:42:20 /pcmcia/nr_000000000000_rac_01.log
```

type uses three characters to represent the kind of log.
In the example shown below, **rac** stands for radius accounting.

version uses two digits to represent the version number.

Separate the four parts of the name with underscores and use the file extension **.log**. An example of a log file name is **nr_192168010001_rac_01.log**

The following is a sample PCMCIA file, along with its authentication timeout and accounting timeout contents:

```
6902    MAR-31-2003  11:51:02   /pcmcia/nr_140007008002_rac_01.log

[03/27/03 14:48:51] auth-req   vlan: 1001 group: 224.10.0.1
receiver: 141.1.1.10 user: nttproject

[03/27/03 14:52:36] auth-req   vlan: 1001 group: 224.10.0.1
receiver: 141.1.1.10 user: nttproject

[03/27/03 14:54:40] acct-stop  sess id: 13000000 vlan: 1001 group:
224.10.0.1 receiver: 141.1.1.10 user: nttproject

[03/27/03 14:54:40] acct-stop  sess id: 13000001 vlan: 1001 group:
224.10.0.1 receiver: 141.1.1.10 user: mmaproject
```

Working with IGAP timeout logs

When an IGAP timeout log file reaches its maximum size, the Passport 8600 performs the following tasks:

- Sends a trap. To see information about these traps, select Device > Trap Log from the Device Manager menu bar.

- Prints an SNMP warning on the console such as:

  ```
  bwA07-1:6# CPU6 [04/03/03 09:02:14] SNMP WARNING Log file for
  IGAP Radius timeout logs has exceeded the maximumlimit
  ```

- Logs the event and sends it to DRAM. To display the event, enter the following command:

  ```
  show log file tail
  ```

  The switch displays an SNMP warning such as:

  ```
  CPU6 [04/03/03 09:02:14] SNMP WARNING Log file for IGAP Radius
  timeout logs has exceeded the maximumlimit
  ```

Working with PCMCIA files

When the PCMCIA reaches its limit, you have to make more room by deleting files. However, before deleting the files, you may want to copy them to another location. To copy PCMCIA files, select Edit > File System from the Device Manager menu bar. For more information on displaying and copying PCMCIA files, refer to the publication, *Configuring Network Management*.

How the Passport 8600 reports that there is no PCMCIA card present depends on whether or not the authentication or accounting time out occurred.

- If there is no PCMIA present and no authentication or accounting time out, the Passport 8600 prints an information and a warning message on the console such as,

  ```
  bwA07-1:6# CPU6 [04/03/03 09:02:14] SW INFO PCMCIA card removed
  from Master CPU “bwA07-1” slot 6, Chassis S/N SSNM00009I
  bwA07-1:6# CPU6 [04/03/03 09:02:14] SNMP WARNING PCMCIA is
  removed, Logging resumes on DRAM
  ```

- If there is no PCMIA present, but there is an authentication or accounting time out, the Passport 8600 sends information and a warning messages to DRAM (not the console).
  To display these messages, enter the following command:

  ```
  show log file tail
  ```

The switch displays messages such as,

```
CPU6 [04/03/03 09:04:43] RADIUS INFO unable to write to IGAP
radius billing log:please verify that PCMCIA has enough free
space.log message:  [04/03/03 09:04:43] auth-req   vlan: 1001
group: 224.10.0.1 receiver: 141.1.1.10 user: nttproject
CPU6 [04/03/03 09:04:17] SNMP WARNING PCMCIA is removed, Logging
resumes on DRAM
CPU6 [04/03/03 09:04:17] SW INFO PCMCIA card removed from Master
CPU "bwA07-1" slot 6, Chassis S/N SSNM00009I
```

Adding an IGAP-enabled RADIUS server

To add an IGAP-enabled RADIUS server:

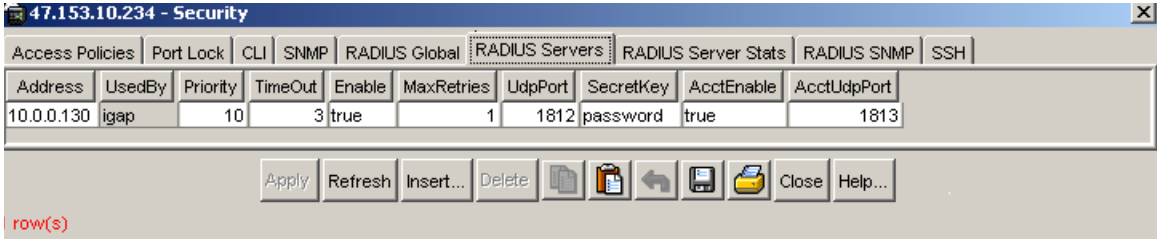
1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the EAPOL tab displayed.

2. Click the RADIUS Servers tab.

   The RADIUS Servers tab opens (Figure 12).

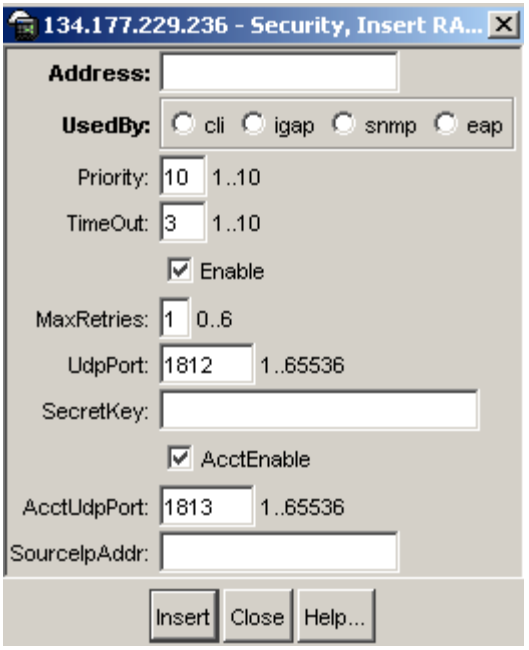
Figure 12 Security dialog box—RADIUS Servers tab



3. Click Insert.

   The Security, Insert RADIUS Servers dialog box opens (Figure 13).

Figure 13 RADIUS Servers tab - Security, Insert RADIUS Servers dialog box



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

5 Select igap in the UsedBy field. The `usedby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`igap` - configures the server for IGAP authentication.
`snmp` - configures the server for SNMP authentication.

6 Enter a secret key.

7 Click Insert.

The information for the configured RADIUS server appears in the RADIUS Servers tab of the Security dialog box (Figure 12).

Deleting an IGAP-enabled RADIUS server

To delete an IGAP-enabled RADIUS server:

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

   The Security dialog box opens with the EAPOL tab displayed.

2. Click the RADIUS Servers tab.

   The RADIUS Servers tab opens (Figure 12).

3. Select the RADIUS server that you want to delete by the IP address shown in the first column.

   The Delete button becomes available.

4. Click Delete.

   The selected RADIUS server is deleted from the dialog box.

Troubleshooting IGAP-enabled RADIUS servers

RADIUS server statistics are available to assist you in troubleshooting the IGAP interfaces. The RADIUS server statistics help you identify where problems are occurring on your network.

To see the IGAP-enabled RADIUS server statistics:

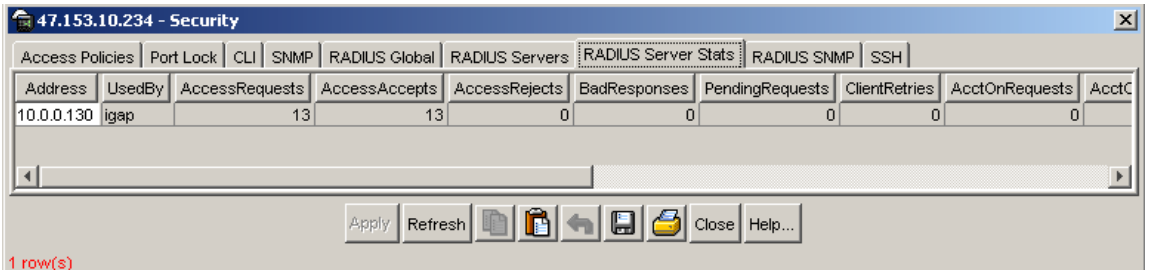
1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the EAPOL tab displayed.

2. Click the RADIUS Server Stats tab.

   The RADIUS Server Stats tab opens (Figure 14).

Figure 14 Security dialog box—RADIUS Server Stats tab



3 Look for “igap” in the UsedBy column to find the IGAP-enabled RADIUS servers

Note: To clear server statistics, select ClearStat from the RADIUS Global tab (Figure 11) and click Apply.

Chapter 3
Configuring IGAP using the CLI

IGAP is an authentication and accounting protocol for clients receiving multicast streams. IGAP extends the functionality of the Internet Group Management Protocol (IGMPv2) by giving providers more control over their networks. With IGAP, service providers and enterprises can authenticate users before granting access to their networks and track how long users receive multicast traffic.

This chapter describes how to use the CLI to configure IGAP. It also describes the commands that display information about the current IGAP configuration. For more information about IGAP concepts, see Chapter 1, “IGAP concepts.”

This chapter includes the following topics:

Roadmap of IGAP commands

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

Command	Parameter
config ip igmp interface <ipaddr> igap	info
	enable
	disable
	authentication <enable|disable>
	accounting <enable|disable>
	clear-counters
config vlan <vid> ip igmp igap	info
	enable
	disable
	authentication <enable|disable>
	accounting <enable|disable>
	clear-counters
config ip igmp igap clear-counters	
config radius mcast-addr-attr-value <value>	
config radius auth-info-attr-value <value>	
config radius igap-timeout-log-fsize <value>	
config radius server create <ipaddr> secret <value> usedby igap	
config radius server delete <ipaddr> usedby igap	

Command	Parameter
`config radius server set <ipaddr> usedby igap`	
`show ip igmp igap`	
`show ip igmp igap-group [count] [memb-subnet <value>] [grp <value>]`	
`show ip igmp igap-counters [vlan <value>]`	

Configuration considerations

- IGAP can be enabled on IGMPv2 interfaces *only*.
- The Passport 8600 processes messages according to the following rules:
  - On IGAP-enabled interfaces, the Passport 8600 processes IGAP messages and ignores all others.
  - On non-IGAP interfaces, the Passport 8600 processes non-IGAP messages and ignores IGAP messages.
- IGAP uses the Fast Leave feature *exclusively* to save bandwidth and enhance the network's efficiency. This feature cannot be disabled.
- Since IGAP uses Fast Leave, it never sends group-specific Query messages in response to a Leave message or use the IGMP Last Member Query Interval (LMQI) parameter.
- IGAP does not support the Passport 8600 static mroute feature. Functionally, this means that the Passport 8600 will still send traffic to the member ports of the static multicast group, but it will not authenticate users or account for their traffic usage.
- IGAP does not support spanning VLANs.
- IGAP does not support static port members.

- Nortel Networks recommends that you do not use static (or block) IGMP member ports.

- Nortel Networks recommends setting the activity check interval to 30 seconds or less. The lower the value means the more often the switch checks the S,G activity for a multicast group. When there is a traffic interruption, IGAP accounting stops and re-starts based on this activity check. For example, a 30 second activity check interval provides for an accounting stop within 60 seconds of a traffic interruption, and an accounting start within 30 seconds after traffic re-starts.

  The command is `config ip pim activity-chk-interval {15|30|210}`. For more information, refer to the publication, *Configuring IP Multicast Routing Operations.*

Configuration prerequisites and notes

Before you can configure IGAP, you must configure the switch as follows:

1. Create the VLANs that you want to enable with IGAP and assign IP addresses to them. For more information on VLANs, refer to the publication, *Configuring IP Routing Operations.*

   ```
   config vlan <vid> ip create <ipaddr/mask> [mac_offset <value>]
   ```

   where:
   vid is the VLAN ID (from 1 to 4094). VLAN 1 is the default VLAN.
   ipaddr/mask is the IP address and network mask you want to assign to this VLAN.
   mac_offset <*value*> is the MAC address you want to assign to this VLAN. This is an optional parameter that, if used, replaces the default MAC address.

2. Set the version of IGMP on each VLAN to version 2. For more information, refer to the publication, *Configuring IP Multicast Routing Operations.*

   ```
   config vlan <vid> ip igmp version 2
   ```

3. Enable PIM-SM globally on the switch. For more information, refer to the publication, *Configuring IP Multicast Routing Operations.*

   ```
   config ip pim mode sparse
   ```

4. Enable PIM-SM on the VLAN that you want IGAP-enabled.

   ```
   config vlan <vid> ip pim enable
   ```

Configuring IGAP on an interface

To configure IGAP on a specific interface, use the following command:

`config ip igmp interface <ipaddr> igap`

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip igmp interface <*ipaddr*> igap followed by:	
`info`	Displays information about the IGAP interface.
`enable`	Enables IGAP on this interface.
`disable`	Disables IGAP on this interface.
`authentication <enable|disable>`	Enables or disables authentication on the specified interface. The default is enable.
`accounting <enable|disable>`	Enables or disables accounting on the specified interface. The default is enable.
`clear-counters`	Clears the IGAP counters for this interface. To see IGAP counters, use the show ip igmp igap-counters [vlan <value>] command.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Enable IGAP on the interface at IP address 142.1.1.254.
- Enable authentication.
  The RADIUS server authenticates users on this interface before granting access to join the multicast group.
- Enable accounting.
  The RADIUS server starts accounting on this session as soon as a user on this interface joins the multicast group, and stops accounting when they leave the multicast group.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
bwA09-1:5/config/ip/igmp/interface/142.1.1.254/igap# enable
bwA09-1:5/config/ip/igmp/interface/142.1.1.254/igap# authentication enable
bwA09-1:5/config/ip/igmp/interface/142.1.1.254/igap# accounting enable
bwA09-1:5/config/ip/igmp/interface/142.1.1.254/igap# info

             Sub-Context:
             Current Context:

                                        IGAP       Info :
                                         If Index : 2053
                                    IGAP-enable : enable
                                Authentication : enable
                                    Accounting : enable
```

Configuring IGAP on a VLAN

To configure IGAP on a VLAN, use the following command:

`config vlan <vid> ip igmp igap`

where:
vid is a VLAN ID from 1 to 4092.

This command includes the following parameters:

`config vlan <vid> ip igmp igap` followed by:	
`info`	Displays IGAP settings on the VLAN.
`enable`	Enables IGAP on this VLAN.
`disable`	Disables IGAP on this VLAN.
`authentication <enable|disable>`	Enables or disables authentication on this VLAN.

config vlan <*vid*> ip igmp igap followed by:	
`accounting <enable|disable>`	Enables or disables accounting on this VLAN.
`clear-counters`	Clears the IGAP counters for this VLAN. To see IGAP counters, use the show ip igmp igap-counters [vlan <value>] command.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Enable IGAP on VLAN 1001.
- Enable authentication.
  The RADIUS server authenticates users on this VLAN before granting access to join the multicast group.
- Enable accounting.
  The RADIUS server starts accounting the session as soon as a user on this VLAN joins the multicast group, and stops accounting when they leave the multicast group.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
bwA09-1:5/config/vlan/1001/ip/igmp/igap# enable
bwA09-1:5/config/vlan/1001/ip/igmp/igap# authentication enable
bwA09-1:5/config/vlan/1001/ip/igmp/igap# accounting enable
bwA09-1:5/config/vlan/1001/ip/igmp/igap# info

Sub-Context:
Current Context:

                              IGAP       Info :
                            If Index : 2053
                         IGAP-enable : enable
                      Authentication : enable
                          Accounting : enable
```

Clearing IGAP counters

IGAP counters provide information that you can use to monitor and troubleshoot IGAP interfaces. See “Troubleshooting IGAP network connectivity” on page 61. To help you isolate a problem, you may want to clear one or all of the counters to observe traffic behavior.

There are three commands that you use to clear counters

- To clear all counters, use the following command:

```
config ip igmp igap clear-counters
```

- To clear counters on a specific interface, use the following command:

```
config ip igmp interface <ipaddr> igap clear-counters
```

- To clear counters on a specific VLAN, use the following command:

```
config vlan <vid> ip igmp igap clear-counters
```

Configuring IGAP with RADIUS

IGAP uses RADIUS servers to authenticate users and account for how long they use the multicast services. This section describes the IGAP-specific RADIUS commands. For information about the complete set of RADIUS parameters, refer to the publication, *Configuring and Managing Security.*

Setting vendor-specific attributes

The following two sections describe the RADIUS commands that set vendor-specific attributes (VSAs) for IGAP.

Setting the multicast address attribute

To set the vendor-specific attribute for the multicast address on an IGAP-enabled RADIUS server, use the following command:

```
config radius mcast-addr-attr-value <value>
```

where:
value indicates an integer assigned to this vendor-specific attribute, which must be in the range from 0 to 255. The default is 90.

Setting the authentication information attribute

To set the vendor-specific attribute for the authentication information on an IGAP-enabled RADIUS server, use the following command:

```
config radius auth-info-attr-value <value>
```

where:
value indicates an integer assigned to this vendor-specific attribute, which must be in the range from 0 to 255. The default is 91.

Setting the timeout log file size

The Passport 8600 captures authentication and accounting information in an IGAP timeout log for each session. The timeout log records information such as when the Passport 8600 sent an accounting start request to the RADIUS server, what the server's response was and when accounting started.

To set the maximum size of the RADIUS timeout log file, use the following command:

```
config radius igap-timeout-log-fsize <value>
```

where:
value indicates an integer (in KB), which must be in the range from 50 to 8192. The default is 512.

Storing IGAP timeout logs

The Passport 8600 stores the timeout log in a PCMCIA file, which uses the following naming convention:

```
vendorname_nasIPaddress_type_version.log
```

where:

vendorname is a two-character symbol representing the vendor.
In the example shown below, **nr** represents a specific Nortel Networks project.

nasIPaddress identifies the network access server (NAS) by its IP address.
In the example shown below, **192168010001** represents the edge node at IP address 192.168.10.1. Note that when there are less than three digits in an octet such as the 10 and 1, leading zeroes fill in to make up the 12 digits. If the Passport 8600 cannot determine NAS IP address, create a file corresponding to NAS IP "0.0.0.0" such as:

```
7672 MAR-17-2003 11:42:20 /pcmcia/nr_000000000000_rac_01.log
```

type uses three characters to represent the kind of log.
In the example shown below, **rac** stands for radius accounting.

version uses two digits to represent the version number.

Separate the four parts of the name with underscores and use the file extension **.log**. An example of a log file name is **nr_192168010001_rac_01.log**

The following is a sample PCMCIA file, along with its authentication timeout and accounting timeout contents:

```
6902    MAR-31-2003  11:51:02   /pcmcia/nr_140007008002_rac_01.log

[03/27/03 14:48:51] auth-req   vlan: 1001 group: 224.10.0.1
receiver: 141.1.1.10 user: nttproject

[03/27/03 14:52:36] auth-req   vlan: 1001 group: 224.10.0.1
receiver: 141.1.1.10 user: nttproject

[03/27/03 14:54:40] acct-stop  sess id: 13000000 vlan: 1001 group:
224.10.0.1 receiver: 141.1.1.10 user: nttproject

[03/27/03 14:54:40] acct-stop  sess id: 13000001 vlan: 1001 group:
224.10.0.1 receiver: 141.1.1.10 user: mmaproject
```

Working with IGAP timeout logs

When an IGAP timeout log file reaches its maximum size, the Passport 8600 performs the following tasks:

- Sends a trap. To see information about these traps, select Device > Trap Log from the Device Manager menu bar.

- Prints an SNMP warning on the console such as:

  ```
  bwA07-1:6# CPU6 [04/03/03 09:02:14] SNMP WARNING Log file for
  IGAP Radius timeout logs has exceeded the maximumlimit
  ```

- Logs the event and sends it to DRAM. To display the event, enter the following command:

  ```
  show log file tail
  ```

  The switch displays an SNMP warning such as:

  ```
  CPU6 [04/03/03 09:02:14] SNMP WARNING Log file for IGAP Radius
  timeout logs has exceeded the maximumlimit
  ```

Working with PCMCIA files

When the PCMCIA reaches its limit, you have to make more room by deleting files. However, before deleting the files, you may want to copy them to another location. To copy PCMCIA files, select Edit > File System from the Device Manager menu bar. For more information on displaying and copying PCMCIA files, refer to the publication, *Configuring Network Management*.

How the Passport 8600 reports that there is no PCMCIA card present depends on whether or not the authentication or accounting time out occurred.

- If there is no PCMIA present and no authentication or accounting time out, the Passport 8600 prints an information and a warning message on the console such as,

  ```
  bwA07-1:6# CPU6 [04/03/03 09:02:14] SW INFO PCMCIA card removed
  from Master CPU “bwA07-1” slot 6, Chassis S/N SSNM00009I
  bwA07-1:6# CPU6 [04/03/03 09:02:14] SNMP WARNING PCMCIA is
  removed, Logging resumes on DRAM
  ```

- If there is no PCMIA present, but there is an authentication or accounting time out, the Passport 8600 sends information and a warning messages to DRAM (not the console).
  To display these messages, enter the following command:

  ```
  show log file tail
  ```

The switch displays messages such as,

```
CPU6 [04/03/03 09:04:43] RADIUS INFO unable to write to IGAP
radius billing log:please verify that PCMCIA has enough free
space.log message:  [04/03/03 09:04:43] auth-req   vlan: 1001
group: 224.10.0.1 receiver: 141.1.1.10 user: nttproject
CPU6 [04/03/03 09:04:17] SNMP WARNING PCMCIA is removed, Logging
resumes on DRAM
CPU6 [04/03/03 09:04:17] SW INFO PCMCIA card removed from Master
CPU "bwA07-1" slot 6, Chassis S/N SSNM00009I
```

Adding an IGAP-enabled RADIUS server

To add an IGAP-enabled RADIUS server, use the following command:

```
config radius server create <ipaddr> secret <value> usedby
igap
```

where:
ipaddr indicates the IP address of the selected interface and
value specifies the secret key, which is a string of up to 20 characters. The RADIUS server uses this password to validate the IGAP client.

Note: The `usedby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`igap` - configures the server for IGAP authentication.
`snmp` - configures the server for SNMP authentication.

The other parameters that you can use with this command are:

```
[port <value>] [priority <value>] [retry <value>]
[timeout <value>] [enable <value>] [acct-port <value>]
[acct-enable <value>]
```

Deleting an IGAP-enabled RADIUS server

To delete an IGAP-enabled RADIUS server, use the following command:

```
config radius server delete <ipaddr> usedby igap
```

where:
ipaddr indicates the IP address of the selected interface.

Note: The `usedby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`igap` - configures the server for IGAP authentication.
`snmp` - configures the server for SNMP authentication.

Setting IGAP-enabled RADIUS server parameters

To set IGAP-enabled RADIUS server parameters, use the following command:

```
config radius server set <ipaddr> usedby igap
```

where:
ipaddr indicates the IP address of the selected interface.

Note: The `usedby` parameter determines how the server functions:

`cli` - configures the server for CLI authentication.
`igap` - configures the server for IGAP authentication.
`snmp` - configures the server for SNMP authentication.

The other parameters that you can set with this command are:

```
[secret <value>] [port <value>] [priority <value>]
[retry <value>] [timeout <value>] [enable <value>]
[acct-port <value>] [acct-enable <value>]
```

Showing IGAP interface information

To display information on IGAP-enabled interfaces, use the following command:

```
show ip igmp igap
```

Figure 15 shows sample output for this command.

Figure 15 Show IGAP command output

```
bwA09-1:5# show ip igmp igap

================================================================================
                                    Igmp IGAP
================================================================================
VLAN ID         IGAP            ACCOUNTING      AUTHENTICATION
--------------------------------------------------------------------------------
91              Disable         Enable          Enable
92              Disable         Disable         Enable
1001            Enable          Disable         Disable
1002            Enable          Enable          Disable
1003            Enable          Enable          Enable
1004            Enable          Enable          Enable
1005            Enable          Enable          Enable
```

Showing IGAP group information

To display information on IGAP groups, use the following command:

`show ip igmp igap-group [count] [memb-subnet <value>] [grp <value>]`

where the optional parameter:
`count` indicates the number of entries to show.
`memb-subnet <value>` is a specific IP address and network mask that you want to show.
`grp <value>` is the IP address of a specific group that you want to show.

Figure 16 shows sample output for this command.

Figure 16 Show IGAP Group command output

```
bwA07-1:5# show ip igmp igap-group

================================================================================
                                Igap Group
================================================================================
GRPADDR     INPORT       MEMBER    MEMBER_STATE  ACCT_TIME EXPIRATION USER_ID
--------------------------------------------------------------------------------
224.10.0.1   V1001-1/1 141.1.1.10   Auth+Acct      5        254      proj1
224.10.0.1   V1001-1/1 141.1.1.11   Auth+Acct      5        254      proj1
224.10.0.1   V1001-1/1 141.1.1.12   Auth+Acct      5        254      proj1
224.10.0.1   V1001-1/1 141.1.1.13   Auth+Acct      5        254      proj1

Total number of groups 4
Total number of unique groups 1
```

Table 4 describes the IGAP group parameters.

Table 4 Show IGAP Group parameters

Field	Description
GRPADDR	Indicates the IP address of this IGAP group.
INPORT	Displays the ingress port and VLAN of the IGAP report.
MEMBER	Indicates the IP address of this IGAP group member.
MEMBER_STATE	Displays the state of this IGAP group member. • **Auth** indicates that the member was authenticated by a RADIUS server. • **Acct** indicates that a RADIUS server successfully started accounting for this member's session.
ACCT_TIME	Displays the accounting time (in seconds) for the duration of the multicast session for this IGAP group member.
EXPIRATION	Specifies how much time is left (in seconds) before the Group Report for this interface expires. This timer is restarted when the RADIUS server receives a new group report.
USER_ID	Displays the User ID for this IGAP member.

Troubleshooting IGAP network connectivity

IGAP counters provide network connectivity information that you can use to monitor and troubleshoot IGAP interfaces. To display the counter information, use the following command:

```
show ip igmp igap-counters [vlan <value>]
```

where:
`vlan <value>` indicates the ID number of the VLAN you want to show.

Figure 17 shows sample output for this command.

Figure 17 Show IGAP Counters command output

```
bwA09-1:5# show ip igmp igap-counters

================================================================================
                              IGAP Counters
================================================================================
INTERFACE     AUTH-SUCCESS        AUTH-REJECT         RESP-TIMEOUT
                        PAPJOINREQ        BASIC-QUERY         BASIC-LEAVE
--------------------------------------------------------------------------------
Vlan 1001        0                    0                   0
                             0                   0                   0
Vlan 1002        0                    0                   0
                             0                   0                   0
Vlan 1003        0                    0                   0
                             0                   0                   0
Vlan 1004        0                    0                   0
                             0                   0                   0
Vlan 1005        0                    0                   0
                             0                   0                   0
Vlan 1006        0                    0                   0
                             0                   0                   0
Vlan 1007        0                    0                   0
                             0                   0                   0
Vlan 1008        0                    0                   0
                             0                   0                   0
```

Note: To clear the counters, see "Clearing IGAP counters" on page 53.

Table 5 describes the IGAP Serviceability Counters parameters.

Table 5 Show IGAP Counter parameters

Field	Description
INTERFACE	Indicates the VLAN ID of this IGAP interface.
AUTH-SUCCESS	Displays the number of authentication success messages received from the RADIUS server on this interface.
AUTH-REJECT	Displays the number of authentication fail messages received from the RADIUS server on this interface.
RESP-TIMEOUT	Displays the number of times that the Authentication Timer timed out. This timer controls the waiting time from sending an Authentication request to receiving an Authentication response.
PAPJOINREQ	Displays the number of Password Authentication Protocol (PAP) Join requests received for members of this interface.
BASIC-QUERY	Displays the number of Basic Query messages sent by the Passport 8600 on an IGAP-enabled interface.
BASIC-LEAVE	Displays the number of Basic Leave messages received by this interface.

Index

V