

HP Route Analytics Management Software

Software Version 9.00

Administrator Guide

Document Release Date: March 2010
Software Release Date: March 2010



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2005–2010 Hewlett-Packard Development Company, L.P.

Contains software from Packet Design, Inc.

© Copyright 2008 Packet Design, Inc.

Trademark Notices

Linux is a U.S. Registered trademark of Linus Torvalds.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Unix® is a registered trademark of The Open Group.

Support

You can visit the HP software support web site at:

<http://h20230.www2.hp.com/selfsolve/manuals>

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels and HP Passport, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1	Introduction	11
	About Route Analytics Management Software	11
	How Route Analytics Management Software Products Operate	12
	Key Components of Route Analytics Management Software	13
	Using Route Analytics Management Software	17
	The Web Interface	17
	The Application Interface	19
2	Configuration and Management	21
	Configuration Overview	21
	Connecting to the Web Interface Home Page	22
	Logging In	23
	Setting the Time and Date	26
	Applying License Keys	28
	Designating the Master and Clients	32
	Assigning the Master Role to an Appliance	33
	Adding Clients to the Configuration	34
	Adding a Second Modeling Engine to the Configuration	36
	Relinquishing the Master Status	37
	Configuring the Network Interfaces	39
	Selecting the Administration Interface	41
	Configuring VLAN Interfaces	42
	Configuring Alias Interfaces	42
	Configuring a Static Route	43
	Configuring Multiple Port Options	45
	Configuring SNMP Agent security	46
	Configuring SSL Certificate	47

Viewing System Settings	50
Configuring the Appliance for Recording	51
Creating a Configuration Hierarchy	52
Configuring the Route Recorder	55
Recorder Configuration Restrictions for MPLS WAN	56
Adding Protocol Instances	57
Interconnection of BGP and IGP Protocol Instances	59
Configuring a BGP Confederation	60
Configuring Multiple EIGRP Autonomous Systems	61
Configure an IGP Instance	61
Configure a BGP Instance	68
Configuring the Route Recorder for the Collector	73
Configuring SNMP v3 Profiles	80
Starting and Stopping the Route Recorder	81
Viewing and Modifying Route Recorder Settings	82
Changing the Area ID Format of an OSPF Protocol Instance	82
Deleting an Existing Domain or Protocol Instance	83
Removing an Interface from a Protocol Instance	83
Changing an OSPF Authentication Password	84
Deleting an OSPF Authentication Password	84
Configuring the Flow Collector	85
Starting and Stopping the Flow Collectors	89
Viewing Flow Collector Settings	90
Configuring Flow Analyzer Recording Status	95
Starting and Stopping the Flow Analyzer	96
Viewing Status of the Flow Analyzer	96
Deleting a Flow Analyzer	97
Additional Configuration Tasks	98
Configuring MPLS VPN-Aware LDP for Cisco Routers	98
Targeted LDP Configuration for Cisco Routers	98
Configuring MPLS-Aware NetFlow v9 on Cisco Routers	99
Configuring MPLS-Aware NetFlow v9 for Cisco Routers	100
Configuring GRE Tunnels	101
Configuring a Loopback Interface for Cisco Routers	105
Enabling Technical Support Access	106

3 Administration	109
Creating and Authenticating User Accounts	110
User Privileges	110
TACACS+ and RADIUS Parameters	111
TACACS+	111
RADIUS	112
User Administration Page	113
Selecting an Authentication Method	114
Creating New User Accounts	115
Update Login Attributes	116
Creating Traffic Groups	117
Editing Traffic Groups	120
Creating CoS Definitions	122
Configuring the VNC Server	125
Connecting to the VNC Persistent Session	127
Using On-Demand VNC Sessions	128
Managing Databases	129
Using Offline Databases	131
Deleting a Database	131
Renaming Databases	133
Using Online Databases	133
Backing Up and Restoring Data	134
Creating a Backup File	134
Saving a Backup File	139
Uploading a Backup File	139
Restoring a Backup File	140
Deleting a Backup File	141
Enabling SMB and Adding a Remote Server	141
Restoring a Backup File from a Remote Server	143
Transferring Backup Files Using FTP	145
Replacing Client and Master Appliances	145
Replacing a Client Appliance	145
Replacing a Master Appliance	147
Choosing a Data Source	150
Archiving Data	153

Configuring Automatic Archival Settings	154
Manually Archiving Data	156
Restoring Archived Data	157
Updating Software	159
Updating with Internet Access	160
Updating without Internet Access	163
Returning to a Previous Version	164
Using the Reports Scheduler	165
Configuring the Mail System	167
Setting Up and Scheduling Daily Reports	167
Understanding Daily Report Contents	168
Scheduling Top N Reports	169
Viewing Saved Daily Reports	170
Viewing Previously-Generated Top N Reports	171
Configuring the FTP Server	171
Configuring Flow Fanout	172
Viewing and Exporting Log Pages	174
Uploading Layout Backgrounds	175
Using Diagnostic Functions	176
Pinging a Network Device	176
Running a Traceroute	177
Shutting Down	178
A Router Commands for the Collector	1
Cisco IOS CLI Commands	1
JunOSe CLI Commands	2
JunOS CLI Commands (Netconf/junoscript)	2
B SNMP MIBs	1
SNMP MIBs Common to All Vendors	1
IpAddressTable	1
InterfaceTable	1
InterfaceIndex	2
IfXTable	2
SysInfo	2
IpRouteTable	2

IpForwardTable	3
IpCidrRouteTable	3
InetCidrRouteTable	3
Alcatel SNMP MIBs	4
AlcatelVrtrConfTableInfoUnit	4
AlcatelVrtrIfTableInfoUnit	5
AlcatelVrtrIpAddrTableInfoUnit	6
AlcatelVrtrStaticRouteTableInfoUnit	6
AlcatelDscpNameTableInfoUnit	6
AlcatelFCNameTableInfoUnit	7
AlcatelSapBaseInfoUnit	7
AlcatelSapIngressInfoUnit	8
AlcatelSapIngressDscpInfoUnit	8
AlcatelSapIngressIPCriteriaInfoUnit	8
AlcatelSapIngressFCInfoUnit	10
AlcatelSapIngressPrecInfoUnit	11
AlcatelSapEgressInfoUnit	11
AlcatelSapEgressFCInfoUnit	11
AlcatelSapEgressDscpInfoUnit	12
AlcatelSapEgressPrecInfoUnit	12
AlcatelSapEgrIPCritInfoUnit	12
AlcatelNetworkPolicyInfoUnit	14
AlcatelNetworkIngressDscpInfoUnit	14
AlcatelNetworkIngressLspExpInfoUnit	15
AlcatelNetworkEgressFCInfoUnit	15
AlcatelRPOperASPathInfoUnit	16
AlcatelRPOperCommunityInfoUnit	16
AlcatelRPOperPrefixListInfoUnit	16
AlcatelRPOperPolicyStmt	16
AlcatelRPOperPSPParams	17
AlcatelRPOperPSFromCriteria	17
AlcatelRPOperPSToCriteriaTableInfoUnit	18
AlcatelRPOperPSDefaultActionParamsTableInfoUnit	19
AlcatelRPOperPSAcceptActionParamsTableInfoUnit	21

C License Feature Details 23

Index 27

1 Introduction

This chapter introduces the Route Analytics Management Software route analytics tools.

Chapter contents:

- [About Route Analytics Management Software](#) on page 11
- [How Route Analytics Management Software Products Operate](#) on page 12
- [Key Components of Route Analytics Management Software](#) on page 13
- [Using Route Analytics Management Software](#) on page 17

About Route Analytics Management Software

The Route Analytics Management Software (RAMS) is an IP Route Analytics tool that listens to routing protocols and builds a real-time routing topology map. The map enables you to visualize and understand the dynamic operation of your network. RAMS Traffic also collects and aggregates traffic data, enabling you to view traffic flows on top of the routing topology.

RAMS offers the following powerful contributions to network planning and analysis:

- **Unified, real-time routing topology view**—View complex topologies hierarchically or by protocol, autonomous system (AS), Interior Gateway Protocol (IGP) area, or Border Gateway Protocol (BGP)/Multiprotocol Label Switching (MPLS) virtual private network (VPN). The History Navigator window lets you play back a history of your routing topology changes.

- **Monitoring and alerts**—Monitor vital service parameters such as network churn and prefix flaps, watch for changes in specific end-to-end service paths and prefixes, and look for degrading redundancy. RAMS Traffic can also raise alerts on all watched parameters to head off costly outages.
- **Interactive analysis**—Perform before and after comparisons and detailed event analysis using a comprehensive routing base and complete event history to rapidly establish the cause of the problem.
- **Planning support**—Display network activity patterns to help optimize performance and minimize unnecessary transit fees or bandwidth costs. You can simulate a link failure or change link metric costs, to see how your routing topology responds to specific failures or upgrades. You can also import and export these simulated changes to manage multiple routing scenarios using external editors.
- **Reports**—View trends and identify emerging issues before they become problems. You can generate graphical user interface (GUI)-based reports for any recorded time period to obtain key information about network health.

How Route Analytics Management Software Products Operate

Route Analytics Management Software appliances physically connect to the network directly to one of the routers on the network or through a switch or hub. The appliances then establish communication with several routers in the network through the routing protocol over this single physical connection. It is only necessary for the appliance to listen to link-state routing protocols, including Open Shortest Path First (OSPF) or Intermediate system to intermediate system (IS-IS) in one location, because each router knows of all adjacencies in the network. Link-state routers send periodic update messages that communicate network information to each other, and to the appliance.

Unlike links between OSPF and IS-IS routers, BGP peerings may not follow physical paths. BGP routers and their peerings are discovered indirectly by receiving routes whose next hop attribute contains the address of a BGP router. Beyond the physical connection between a BGP router and a peer, the existence of a BGP peering is inferred if it is advertising prefixes.

When you first connect the appliance to the network, it usually acquires the topology in a matter of minutes; however, the process can take up to one hour for an Enhanced Interior Gateway Routing Protocol (EIGRP) network. As noted in the *RAMS Appliance Setup Guide*, you should connect the unit to the core routers. When connected to a core router, the RAMS appliance becomes more resilient with respect to loss of edge connectivity and remains useful for recovery purposes even during a widespread outage.

The appliance then maintains a real-time topological view of the entire network. You can view and manage the network from your desktop computer through the graphical user interface.

Key Components of Route Analytics Management Software

Route Analytics Management Software deployments may include the following components:

HP RAMS Route Recorder—An appliance that records routing data and stores it in a real-time database. The recorder can concurrently monitor most major routing protocols (OSPF, IS-IS, BGP, and EIGRP) across multiple domains and ASs from a single appliance.

HP RAMS Flow Collector—An appliance that collects traffic flow information exported from the routers, as well as from NetFlow recorders, and stores this information in a database. (RAMS Traffic only)



The Flow Collector is supported only on appliance models with two disk volumes. See *HP Route Analytics Management Software Appliance Setup Guide* for more information.

HP RAMS Flow Analyzer—An appliance that correlates traffic and routing data and then uses the combined data to produce reports. (RAMS Traffic only)

HP RAMS Modeling Engine — An appliance that creates a synthesized view of data collected across the network. The Modeling Engine presents this data in a graphical user interface accessible from your desktop, providing a single, cohesive view of network activity.

The size and distribution of the network and the number of concurrent users to be supported will determine the needed number and type of appliances. In distributed networks, a single Modeling Engine can support multiple, geographically distributed Route Recorders. In RAMS Traffic deployments, separate appliances should be installed for the Modeling Engine, Flow Analyzer, Flow Collectors, and Route Recorders.

With RAMS Traffic, you can monitor and record network events in different parts of the network with multiple Route Recorder units. The distributed Route Recorders collect routing data locally, from the area where they are installed, through generic route encapsulation (GRE) tunnels, or both. A centralized Modeling Engine retrieves the recorded data from each recorder. Users can then monitor network-wide routing from the Modeling Engine. Users can also archive network-wide data from a central location, and obtain reports from every Route Recorder in the configuration when they access the Modeling Engine.

When there are multiple Route Recorders in a distributed RAMS Traffic deployment, you can configure each appliance to record data per protocol or per multiple protocols, per area or per area within a protocol, or in any combination thereof. Recorder configuration is described in [Chapter 2, “Configuration and Management”](#)

The next figures show how data flows through the network. RAMS is shown in [Figure 1](#) and RAMS Traffic is shown in [Figure 2](#).

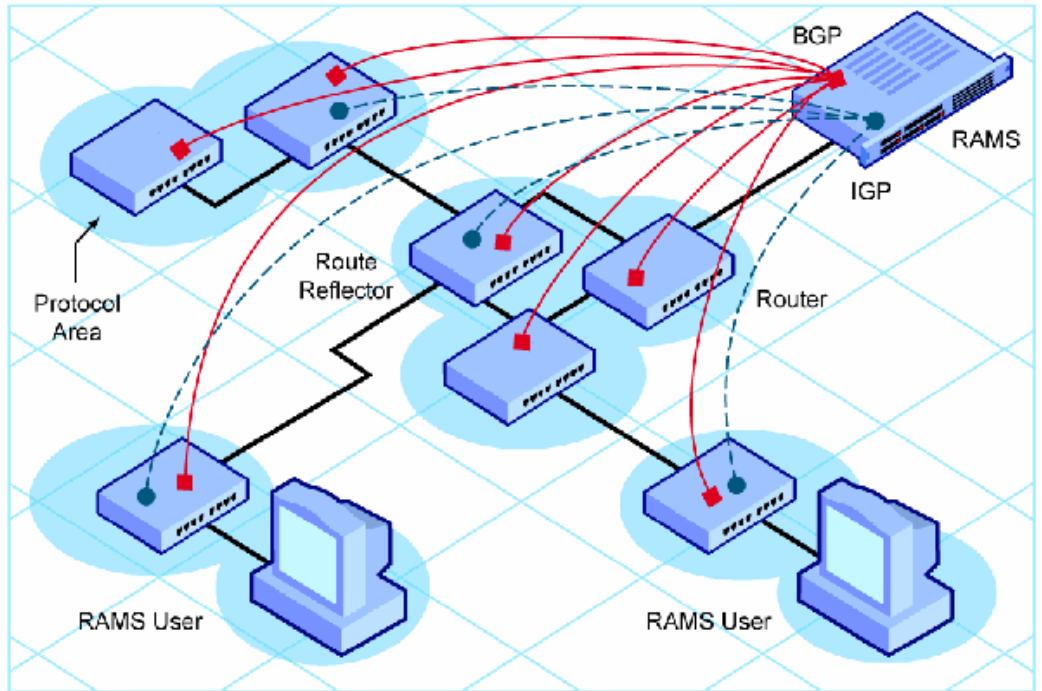


Figure 1 RAMS Data Flow

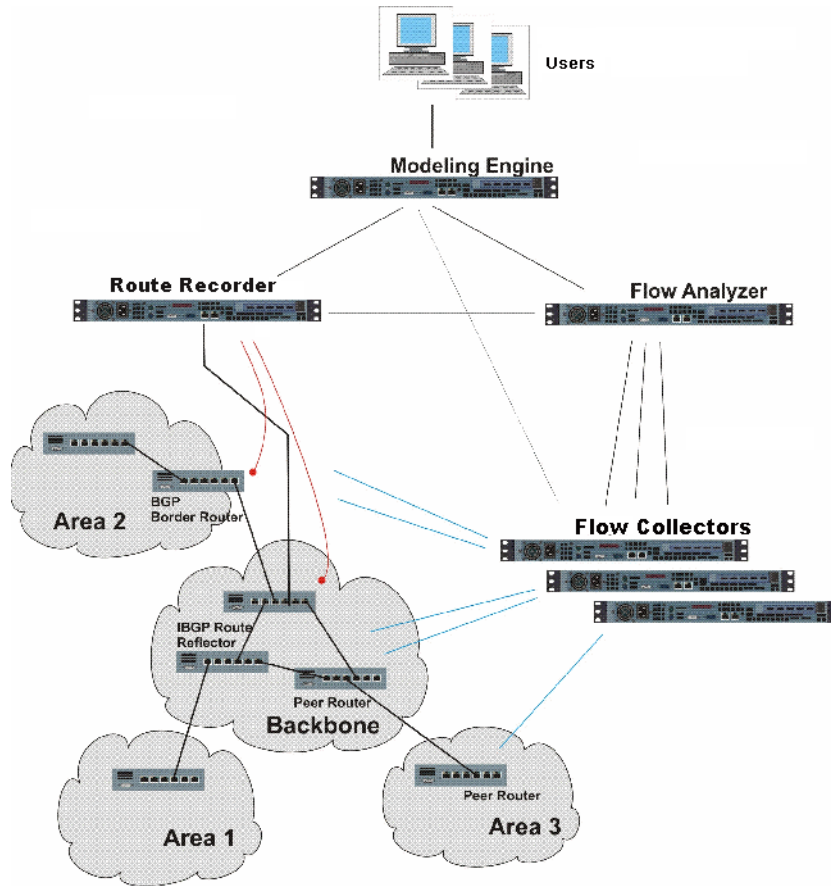


Figure 2 RAMS Traffic Data Flow

In a distributed environment where multiple appliances are installed on the network, you must designate the Modeling Engine as the master appliance during the configuration process (with the Master Capability license key). The Route Recorders in the deployment act as clients. (For RAMS Traffic, the Route Recorder, Flow Collectors, and Flow Analyzer are all client units.) From the master, you view and configure clients for recording. You also manage licenses for the entire configuration from the master.

In RAMS Traffic, Flow Collectors are located near the router where they collect traffic flow data. The recorders aggregate this data before providing it to the Flow Analyzer. The Flow Collector receives routing data from the Route

Recorder and traffic data from the NetFlow exporters to aggregate this data. The Flow Analyzer receives data from one or multiple Flow Collectors, and combines the data to create a network-wide report. The Modeling Engine queries the routing and traffic databases of each appliance to create a synthesized view of both route and flow across the network, then updates the topology map with this data whenever the routing topology changes, thereby providing an accurate, real-time view of how the network is directing traffic.

Using Route Analytics Management Software

You can connect to the appliance using either of the following methods:

- A web browser for accessing the Administration web pages. Use the web interface to perform tasks such as database management, report creation, software updates, and recorder configuration. For information on supported browsers, refer to [Connecting to the Web Interface Home Page](#) on page 22.
- A Virtual Network Computing (VNC) or X Window System client for displaying the Route Analytics Management Software application. Network engineers and operators use the VNC or X client interface to view the routing topology map and analyze network activity.

Both types of viewers accommodate remote access, so you can view and manage one or more units from any desktop computer connected to the network, providing that it has a web browser and a VNC or X Window System client installed. Refer to the “Viewers” chapter in the *HP Route Analytics Management Software User’s Guide* for instructions on setting up client access.

The Web Interface

After you log into the appliance through a web browser, the Home page opens. At the top of the Home page are the following navigational links, which provide access to each area of the web interface:

- **Administration**—Connects you to the Administration pages, where you perform administrative tasks such as user management and software updates.

- **Recorder Configuration**—Connects you to the Recorder Configuration page. In a distributed system, you configure recorders and analyzers on the Recorder Configuration page of the master unit. On client units, the Recorder Configuration page is view-only and shows just that client's branch of the configuration tree.
- **Reports Portal**—Connects you to the reports pages of the recorder, where you can run reports detailing recorder activity for IGP and BGP protocols. In a deployment with multiple Route Recorders, you can use the Reports Portal of the centralized Modeling Engine to obtain network-wide reports from a single location.
- **Support**—Connects you to a page providing links to documentation in PDF format, as well as links to the Self Service Support site and software downloads.

You will also find a link to **Logout** of the web interface. To log back in, you must re-enter your user name and password.

The Application Interface

After you launch the application in a VNC or X Window System viewer, you open a routing topology map, which is a real-time graphical representation of the network. There are three display modes for viewing and manipulating the topology map:

- **Monitoring mode**—In this mode, the topology is currently being recorded and updates to the routing database are shown on the topology map as they occur.
- **Planning mode**—In this mode, planning features are enabled for the topology map.
- **Analysis mode**—In this mode, only previously recorded information in the routing database is shown on the topology map.

See the “The Routing Topology Map” chapter in the *HP Route Analytics Management Software User’s Guide* for instructions on opening the maps. Monitoring mode is available only with databases that are configured for recording data.

In Planning mode and Analysis modes, you can focus on a snapshot of network activity that is meaningful to your network planning and analysis. For example, you can view network data for the last hour, the entire month, or create a customized time range reflecting the state of the network from 11 a.m. to 2 p.m.

Topologies normally open in Monitoring mode, with the following exception: In RAMS Traffic, if you are opening up a topology including a traffic database, the topology automatically opens in Analysis Mode with the selected time set to the latest available traffic data. Due to the inherent delay of NetFlow sampling, aggregation and buffering, traffic data is typically delayed by 20 minutes from real time. If you are only interested in routing data, you can open the topology in Monitoring Mode by deselecting the traffic databases in the Open Topology dialog box.

To change modes, click the mode icon in the lower left corner of the window and select the desired mode.

In addition to the main topology map window, the following tools are available:

- **History Navigator**—Allows you to replay and analyze historical data. This tool is useful in investigating the cause of past events and helps network engineers plan for better performance in the future.

- **Planning Reports**—Allows you to view a table listing all edits you've made to the topology map in Planning mode. This tool also provides analysis of how the edits theoretically affect network traffic.
- **Capacity Reports**—Allows you to view an estimate of what future traffic demands could be like based on past data that has been collected. This enables you to plan potential expansion of the network in order to meet future demands. (RAMS Traffic only)
- **Traffic Reports**—Allows you to view reports based on traffic collected by Flow Collectors, then correlated and analyzed by the Flow Analyzer. (RAMS Traffic only)
- **Path Reports**—Allows you to generate reports to analyze network connectivity and optimize routing performance.
- **IGP and BGP Reports**—Allows you to view IGP- and BGP-protocol routing data collected from the Route Recorders. In a distributed deployment with multiple Route Recorders, connect to the centralized Modeling Engine to view consolidated reports containing IGP- and BGP-protocol data collected across the network.

Before proceeding with this document, you should make sure that the RAMS appliance is installed and networked as described in the *RAMS Appliance Setup Guide*.

2 Configuration and Management

After you install the hardware that is required to connect one or more appliances to the network, you can configure each appliance using the administrative web interface. This chapter describes how to access the web interface and perform configuration tasks.

Chapter contents:

- [Configuration Overview](#) on page 21
- [Connecting to the Web Interface Home Page](#) on page 22
- [Logging In](#) on page 23
- [Setting the Time and Date](#) on page 26
- [Applying License Keys](#) on page 28
- [Designating the Master and Clients](#) on page 32
- [Configuring the Network Interfaces](#) on page 39
- [Configuring SNMP Agent security](#) on page 46
- [Viewing System Settings](#) on page 50
- [Configuring the Appliance for Recording](#) on page 51
- [Additional Configuration Tasks](#) on page 98
- [Enabling Technical Support Access](#) on page 106

Configuration Overview

In a distributed deployment with multiple Route Recorders, a Modeling Engine must serve as the master appliance. You designate this appliance as the master during the configuration process. The other units in the deployment become clients of the master.



Master and client designations do not apply to single-appliance configurations.

The following properties apply to the master and clients:

- **Master**—A Modeling Engine that allows centralized configuration of all client appliances in a multi-appliance deployment. You can monitor and manage the clients using the web interface on the master.
- **Clients**—One or more appliances that are configured and monitored by the master in a distributed configuration. A client can be a Route Recorder, Flow Collector, or Flow Analyzer.

Follow the procedures in this chapter to configure the Route Recorder to listen to particular protocols, the Flow Collectors to collect and aggregate traffic data, and the Flow Analyzer to create network-wide reports.



Make sure that you complete the tasks in the order in which they appear in this chapter.

Connecting to the Web Interface Home Page

A built-in web server provides primary administrative access. The following browsers are supported:

- Internet Explorer 8.0
- Firefox 3.5.2
- Safari 4

To connect to the web interface Home page, perform the following steps:

- 1 Open a standard web browser and enter the initially configured address or hostname of the appliance.

In a distributed configuration, enter the address or hostname of the designated master.

The Home page is password-protected and user input is encrypted using SSL. A confirmation security dialog box opens the first time you access the website. The secure web pages have self-signed certificates from the appliance.



(Internet Explorer 7.0) When you enter the IP address or hostname in Step 1, a window may open with the warning “There is a problem with this website’s security certificate.” It is safe to ignore this warning. Select “Continue to this website (not recommended)” to connect to the Home page.

- 2 Click **Yes** to accept the certificate and allow the secure web pages to open. The Login page opens as shown in [Figure 3](#).

Login

Username

Password:

Your web browser must accept cookies to login.

Figure 3 Log-In Page

Logging In

Before you begin configuration tasks, you must log into the Administration pages and change the default administration password.



To log into the system, your browser must accept cookies.

To log into the Administration pages, perform the following steps:

- 1 Open a standard web browser and enter the initially configured address or hostname of the appliance to open the Login page.

Login

Username

Password:

Your web browser must accept cookies to login.

Figure 4 Log-In Page

The Home page is password-protected and user input is encrypted using SSL. A confirmation security dialog box opens the first time you access the website. The secure web pages have self-signed certificates from the appliance.



(Internet Explorer 7.0) When you enter the IP address or hostname in Step 1, a window may open with the warning “There is a problem with this website’s security certificate.” It is safe to ignore this warning. Select “Continue to this website (not recommended)” to connect to the Home page.

- 2 Enter the default administrator user name (admin) and the default password (admin).
- 3 Click **Login**.

After a period of inactivity, you must repeat this step to have continued access to the Administration pages.

After a successful login, the Home page opens as shown in [Figure 5](#).

Home

The **Administration** link presents a menu of pages for configuration and maintenance of the HP Route Analytics Management System appliance. The first steps for configuration are:

1. Applying **license** keys if needed (on the unit that will be Master)
2. Setting the **time and date** (on all units, using NTP)
3. Designating the Master and Client **units** (on the Master)

The **Recorder Configuration** page is used to configure the recording of routing protocols and traffic statistics on one or more units in the HP Route Analytics Management System system after the initial configuration steps are completed. A configuration hierarchy represents the relationship among the protocol domains.

The **Reports Portal** link presents a menu of pages where reports on network activity and status may be generated and viewed. Reports for a particular protocol domain are available only through the Reports Portal of the unit recording that domain. HP Route Analytics Management System can generate and email a daily summary report if configured using the Administration - **Mail** page, and you can view saved daily reports through the Reports Portal link.

The **Support** page provides links to download the HP Route Analytics Management System **User's Guide** that provides a detailed description of the configuration procedures, as well as X Window System software or VNC Viewer software to allow connecting to HP Route Analytics Management System to view the graphical user interface and an SVG browser plug-in for viewing saved BGP event animations.

For technical support, visit:

<http://www.hp.com/go/hpssoftwaresupport>

<http://www.hp.com/go/hpssoftwaresupport>

Figure 5 Home Page



The Home page provides links to support and documentation downloads for the X Window system or VNC, either of which is required to run the software. The X Window system is recommended for users with high-speed Internet connections, while VNC is more appropriate for users with dial-up or Digital Subscriber Line (DSL) connections.



The third-party X Window system software provided with the appliance comes with a 30-day evaluation license. After this initial 30-day period, you must purchase a license from StarNet Communications Corporation to continue using the software.

For security reasons, we recommend that you change the administrator password when you first log in, and on a regular schedule after that.

To change the administration password, perform the following steps:

- 1 From the Home page, choose **Administration > Users**.
- 2 On the User Administration page, select the administrator's user name from the **Current Users** list, and then enter the new password.
- 3 Click **Update**.

For more information about user administration, see [Chapter 3, "Administration"](#)

Setting the Time and Date

You must set the time and date for every appliance in your configuration before continuing with the procedures described in this chapter. To access the Time and Date page, choose **System > Time and Date** from the Left Navigation Bar pane.



In a multi-appliance configuration, access the Time and Date page of each client appliance individually to configure time and date settings.

We strongly recommended that you synchronize the time and date for each appliance with a Network Time Protocol (NTP) server to avoid having to make manual time adjustments, potentially backwards in time. (For multi-appliance configurations, NTP is required.) Because the recorded routing topology database requires that time progresses monotonically, the NTP daemon will not adjust the time if the discrepancy is large enough to require a step adjustment rather than slowly slewing the clock. To avoid any problems, set the time manually to the correct time (within a few minutes), and then select **Get time from server**. After the time is set using the NTP server option, you can verify the results on the View Configuration page.



If you must set the clock backwards manually, you must first rename all currently recording databases and start a new database.

To set the time and date for each appliance, perform the following steps:

- 1 Choose **Administration > Time and Date**.
- 2 Select the time zone from the **Time Zone** drop-down list (Figure 6).
- 3 Choose whether to set the time and date from an NTP server or set it manually.
 - **Get time from server**—Enter the primary and secondary NTP server (if necessary) in the **Primary NTP Server** and **Secondary NTP Server** text boxes, respectively.
 - **Set time manually**—Click the **Set time now** check box and adjust the time fields as necessary.
- 4 Click **Update**.



Modifications to the Time and Date page are not permitted if recording is in progress.

Time and Date

Time Zone:

Get time from server

Primary NTP Server:

Secondary NTP Server:

NTP is intended to keep the system clock accurate. To make large time changes, manually set the time then configure the NTP servers.

Set time manually

Set time now:

/ / :

Year Month Day Hour Minute
yyyy mm dd h24 mm

Warning: Route Recorder must be stopped before altering time configuration. It is strongly recommended to use the Database Administration page to delete all previously recorded databases, then change time configuration before resuming recording.

Figure 6 Time and Date Page

Applying License Keys

A license determines the available functions and the number of supported users and routers. For Route Recorder it also determines the supported protocols.

Each license key is tied to an identification number, or Unit ID, which corresponds to an appliance with the same Unit ID. In a distributed configuration, license keys for all units in the configuration are applied to the master, which in turn assigns the appropriate license keys to its clients based on the Unit ID numbers. RAMS Traffic rejects licenses without a Unit ID.

To view the license information, start on the *Administration* page. Locate the **Maintenance** link in the left frame, then click **License** to launch the *License Update* page. This page displays the current license information for the system, and lets you activate your temporary license or install new license keys. This page displays three buttons:

- **RAMS** — Provides GUI functionality and is enabled for viewing traffic information
- **Traffic** — Provides traffic functionality
- **Modeling Engine** — Provides functions for testing configurations with replication enabled

RAMS comes with a temporary license that unlocks all protocols for up to three users and 1000 routers. The temporary license expires after 60 days. To activate a temporary license, click the corresponding button on the *License Update* page, shown in [Figure 7: RAMS, Traffic, or Modeling Engine](#). For example, to activate the RAMS license, click **RAMS**, and the temporary license is applied.

If the temporary license expires before you have installed a permanent license, data recording is disabled, protocol configuration is disabled, and a warning message is displayed on the RAMS user interface. For uninterrupted use of the RAMS, you must obtain and install your permanent license key before the temporary license expires.



If you are setting up a system of multiple units, you will need to activate the temporary license on each appliance separately by logging into the *Administration* page, navigating to the *License Update* page, and installing the appropriate temporary license key. From the master appliance, you can then proceed to add clients, configure recording, etc.

To install a new license key, perform the following steps:

- 1 Enter the license key text-string in the space provided, exactly as it was given to you, including punctuation. If you received your license key electronically, you can use the cut-and-paste feature on your computer. Otherwise, you can manually type it in. Take care to avoid typing mistakes.
- 2 Click **Update**. This installs the license key. The functionality authorized by the license key is immediately available. Each licensing component is described in [Appendix C](#), “License Feature Details.”

License Update

License Information for Master Unit ID 001279D5AE6D		
Feature	Value	Expiration Date
OSPF:	Enabled	2008-11-14
ISIS:	Enabled	2008-11-14
EIGRP:	Enabled	2008-11-14
BGP:	Enabled	2008-11-14
MPLS VPN:	Enabled	2008-11-14
GUI:	Enabled	2008-11-14
RAMS Traffic SPI:	Enabled	2008-11-14
Route Analyzer Alerts:	Enabled	2008-11-14
Route Analyzer Reports:	Enabled	2008-11-14
Database Server:	Enabled	2008-11-14
Database Client:	Enabled	2008-11-14
Master Capability:	Enabled	2008-11-14
Router Count:	Unlimited	2008-11-14
MPLS VPN Prefix Count:	Unlimited	2008-11-14
User Count:	5	2008-11-14
Software Update:	Enabled	2008-11-14

Aggregate License Information	
OSPF:	Enabled
ISIS:	Enabled
EIGRP:	Enabled
BGP:	Enabled
MPLS_VPN:	Enabled
Router Count:	Unlimited
MPLS VPN Prefix Count:	Unlimited

License Update
Copy-Paste the License Update File contents here:
<div style="border: 1px solid gray; height: 100px;"></div>
<input type="button" value="Update"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/> <input type="button" value="Re-Apply All"/>
<input type="button" value="Remove all licenses on this unit"/>

Figure 7 License Update Page

The License Update page displays the applied license key components and the corresponding expiration dates. The master later distributes license features to client units as described in [Designating the Master and Clients](#) on page 32.

In some cases, you may need to reapply licenses from the master to its clients. For example, if a client is unreachable when a new license key is applied to the master, that client will not receive the new key when it is initially distributed among the appliances in the configuration. When the client reestablishes contact with its master, click the **Re-Apply All** button to redeploy the new license key.

If incorrect licenses have been applied on an appliance, you may correct that by clicking **Remove all licenses on this unit**. This erases all licenses that have been applied and allows you to reapply the correct licenses.

Designating the Master and Clients

Distributed configuration and management allows an administrator to configure and monitor multiple Route Analytics Management Software components from a central location. If you are working with a single-appliance configuration, skip this section and proceed to [Configuring the Network Interfaces](#) on page 39.

The following component definitions apply to the units in a distributed configuration:

- **Route Recorders**—Collect routing information to store in the database.
- **HP RAMS Modeling Engine** — Create a synthesized view of all network data collected by the recorders. In a deployment with multiple Route Recorders, a Modeling Engine must serve as the master appliance. It replicates the data collected by each Route Recorder, providing a locally accessible database of network-wide information. The centralized Modeling Engine also feeds prefix information to the Flow Collectors and supplies data to the Flow Analyzer to create reports. For RAMS Traffic, Modeling Engine displays this data in a VNC or X viewer. See the “Viewers” chapter in the *HP Route Analytics Management Software User’s Guide* for more information.
- **Flow Collector**—Collects traffic flow information from NetFlow recorders and stores it in the database. The Modeling Engine queries the database to create a synthesized view of traffic flow through the network.
- **Flow Analyzer**—Receives traffic data from the Flow Collectors. The Flow Analyzer uses this information to generate aggregate traffic flow reports and alerts.

Assigning the Master Role to an Appliance

The master in a distributed configuration allows you to view and manage multiple Route Analytics Management Software appliances through its administration interface. You must designate the Modeling Engine as the master.



The appliance designated as master will associate itself with client units through an HTTP POST. To authenticate that initial POST, you must use the Master-Client Shared Secret. A default shared secret is already set. If you want to choose a different one, use the `Configure Master-Client Shared Secret` command on the master appliance and on each client appliance to set the new secret.

The Master-Client Shared Secret must be the same on all units.

To designate the master appliance, perform the following steps on the system that will be the master:

- 1 Choose **Administration > Units**.
- 2 On the Units page, the IP address of the administrative interface on the master appliance is listed in the text box. Click **Make Master**.

The master appliance is designated and the Client Configuration section appears on the Units page.

Units

Client Configuration

<div style="background-color: #e6e6fa; text-align: center; padding: 2px;">Client List</div> <div style="display: flex; align-items: flex-start;"> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;"> (192.168.1.31) (192.168.1.58) (192.168.0.127) </div> <div style="border: 1px solid #ccc; padding: 2px; margin-left: 5px;">Delete</div> </div>	<div style="background-color: #e6e6fa; text-align: center; padding: 2px;">Add New Client</div> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;">IP Address: <input style="width: 100px;" type="text"/></div> <div style="border: 1px solid #ccc; padding: 2px; margin-left: 5px;">Add</div> </div> <p style="font-size: small; margin-top: 5px;">This may take several seconds</p>																
<div style="background-color: #e6e6fa; text-align: center; padding: 2px;">Client Status</div>																	
<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 25%; text-align: left; border-bottom: 1px solid #ccc;">Unit</th> <th style="width: 25%; text-align: left; border-bottom: 1px solid #ccc;">Type</th> <th style="width: 15%; text-align: left; border-bottom: 1px solid #ccc;">Status</th> <th style="width: 35%; text-align: left; border-bottom: 1px solid #ccc;">Version</th> </tr> </thead> <tbody> <tr> <td>192.168.1.31 001279D5AE6D</td> <td>RAMS</td> <td>Up</td> <td>6.0.69-R</td> </tr> <tr> <td>192.168.1.58 001B784260F2</td> <td>RAMS</td> <td>Up</td> <td>6.0.69-R</td> </tr> <tr> <td>192.168.0.127 00118550FF79</td> <td>Flow Collector Flow Analyzer</td> <td>Up</td> <td>6.0.69-R</td> </tr> </tbody> </table>		Unit	Type	Status	Version	192.168.1.31 001279D5AE6D	RAMS	Up	6.0.69-R	192.168.1.58 001B784260F2	RAMS	Up	6.0.69-R	192.168.0.127 00118550FF79	Flow Collector Flow Analyzer	Up	6.0.69-R
Unit	Type	Status	Version														
192.168.1.31 001279D5AE6D	RAMS	Up	6.0.69-R														
192.168.1.58 001B784260F2	RAMS	Up	6.0.69-R														
192.168.0.127 00118550FF79	Flow Collector Flow Analyzer	Up	6.0.69-R														
<div style="display: flex; justify-content: center; gap: 10px;"> <div style="border: 1px solid #ccc; padding: 2px 10px;">Refresh Client Status</div> <div style="border: 1px solid #ccc; padding: 2px 10px;">Relinquish Master Role</div> </div>																	

Figure 8 Units Page

The address of the master appliance appears in the Client List box.

You must now assign each of the clients that the master appliance will manage.

Adding Clients to the Configuration

Before you assign client units to the master, be sure the systems in the configuration are running and reachable. When you add a client, the master appliance automatically applies the appropriate license keys. When a client is bound to the master, that client cannot be bound to another master until the master-client relationship is dissolved (see [Relinquishing the Master Status](#) on page 37). License details are returned when a client is added successfully. For instance, a message indicating that two license keys were applied is displayed on the master's Units page after you have added a client.



The clocks of the units must be synchronized before you add clients to the configuration.

To add clients to the configuration, perform the following steps:

- 1 On the Units page of the master, enter the IP address of a client in the Add New Client text box.
- 2 Click **Add**.

A success message is displayed. The IP address of the client is now listed in the Client List box. If the client does not appear in the Client List box, make sure the system is properly connected to the network and reachable by the master.

As you add each client, the Client Status table on the Units page is refreshed to display an updated list of clients. Each client IP address has an associated type. For example, if a system is licensed to act as a Modeling Engine, the **Type** column lists this description. The **Status** column indicates whether the client is running (Up) or not (Down).

Use the **Refresh Client Status** button at the bottom of the Units page to update the displayed version, type, and status of the clients listed on the page.

Units

The screenshot shows the 'Client Configuration' section with a 'Client List' containing three entries: (192.168.0.165), (192.168.0.148), and (192.168.0.160). Each entry has a dropdown arrow and a 'Delete' button. To the right is the 'Add New Client' section with an 'IP Address:' text box and an 'Add' button. Below this is the 'Client Status' table with columns for Unit, Type, Status, and Version.

Client Configuration			
Client List		Add New Client	
(192.168.0.165)	▲	IP Address:	<input type="text"/>
(192.168.0.148)	▬	<input type="button" value="Add"/>	This may take several seconds
(192.168.0.160)	▼		
<input type="button" value="Delete"/>			
Client Status			
Unit	Type	Status	Version
192.168.0.165 00304871DEEE	Modeling Engine	Up	Build 4.0.72-E
192.168.0.148 00E0188A5F3C	Route Recorder	Up	Build 4.0.72-E
192.168.0.160 00E0188A5880	Flow Collector	Up	Build 4.0.72-E
192.168.0.166 003048850D56	Flow Analyzer	Up	Build 4.0.71-E

At the bottom of the screenshot are two buttons: 'Relinquish Master Role' and 'Refresh Client Status'.

Figure 9 Client Status Section of Units Page

Adding a Second Modeling Engine to the Configuration

One Modeling Engine is sufficient for most networks. However, if you anticipate that more than five users will need to access the Modeling Engine simultaneously, or if you have recorders at a vast geographical distance from the Modeling Engine, you will need to add an additional Modeling Engine to your network.



Before adding the second Modeling Engine, verify that the master unit has all the necessary licenses.

To add a second Modeling Engine to your network, perform the following steps:

- 1 Choose **Administration > License**.
- 2 Paste the license for the second Modeling Engine into the License Update box, and click **Update**.
- 3 Return to the Units page, and enter the IP address for the second Modeling Engine in the IP Address text box.
- 4 Click **Add**.



If the license was successfully applied for the second Modeling Engine, **Data Source Configuration** is listed in the left navigation bar.

You now need to specify how to obtain the routing data for the Modeling Engine. There are several ways to obtain data:

- From the Route Recorder
- From the primary Modeling Engine (if it is replicating)
- From the second Modeling Engine

See [Choosing a Data Source](#) on page 150 for more information.

Relinquishing the Master Status

If necessary, you can remove the master status from an appliance and assign this function to another Modeling Engine in the configuration. Keep in mind that relinquishing the master role requires you to delete all client configurations.

To remove the master status, perform the following steps in the order listed:

- 1 Delete each of the client configurations on the master from the Recorder Configuration page. To delete client configurations on the master appliance, perform the following steps:
 - a Choose **Recorder Configuration**.
 - b Click **Stop All Recording**.
 - c Click the client to remove from the tree structure.
 - d Click **Delete**, and then click **Yes** to confirm.
 - e Repeat Steps c and d to remove additional clients from the configuration.



If a client is inaccessible for any reason, you will receive a warning message when you attempt to delete its configuration. If necessary, you can forcibly remove the configuration of the inaccessible client. If you choose to forcibly remove the client configuration of an inaccessible appliance, the client will be unusable until it is reset to factory defaults.

- 2 On the Units page of the master appliance, remove each of the clients from the Client List box. To remove clients from the client list, perform the following steps:
 - a Choose **Administration > Units**.
 - b Select the client IP address from the Client List box.
 - c Click **Delete**.

A success message appears. The IP address of the client is now removed from the Client List box and from the Client Status table on the Units page.

Deleting a system from the Client List box means the client appliance no longer has a relationship with the master and is free to become the client of another master.

- 3 On the Units page, click **Relinquish Master Role**.

The appliance no longer functions as the master of the distributed configuration. You can now designate a second appliance the configuration master and, if desired, add the first appliance as a client of the new master. For more information, see [Designating the Master and Clients](#) on page 32.

Configuring the Network Interfaces

Use the Network and Interface Configuration page (Figure 10) to set the appliance's networking configuration and add interfaces and static routes.

Network & Interface Configuration

Any operation on this page may cause the HTTP server to go away for up to 2 minutes.

Hostname:
 Domain Suffix:
 Primary DNS: Secondary DNS:

Interface	Name	Use DHCP	IP Address	Netmask	Allow Admin	Status
Slot 0/Port 1 (00:30:48:86:44:B6)	<input type="text" value="eth0_10.64.15.202"/>	<input type="checkbox"/>	<input type="text" value="10.64.15.202"/>	<input type="text" value="255.255.255.0"/>	<input checked="" type="radio"/>	Up
Slot 0/Port 2 (00:30:48:86:44:B7)	<input type="text" value="eth1_172.16.200.202"/>	<input type="checkbox"/>	<input type="text" value="172.16.200.202"/>	<input type="text" value="255.255.255.0"/>	<input type="radio"/>	Up

Interface	Auto Negotiate	Speed	Duplex
Slot 0/Port 1	<input checked="" type="checkbox"/>	<input type="radio"/> 10 Mbps <input checked="" type="radio"/> 100 Mbps <input type="radio"/> 1000 Mbps	<input type="radio"/> Half <input checked="" type="radio"/> Full
Slot 0/Port 2	<input checked="" type="checkbox"/>	<input type="radio"/> 10 Mbps <input checked="" type="radio"/> 100 Mbps <input type="radio"/> 1000 Mbps	<input checked="" type="radio"/> Half <input type="radio"/> Full

VLAN Interfaces

Interface	VLAN ID
<input type="text" value="Slot 0/Port 1"/>	<input type="text"/>

Alias Interfaces

Interface	Alias Name	IP Address
<input type="text" value="Slot 0/Port 1"/>	<input type="text" value="s0/1_alias1_172.16.10.1"/>	<input type="text" value="172.16.10.1"/>
<input type="text" value="Slot 0/Port 2"/>	<input type="text" value="s0/2_alias2_172.16.20.1"/>	<input type="text" value="172.16.20.1"/>
<input type="text" value="Slot 0/Port 1"/>	<input type="text"/>	<input type="text"/>

Static Routes

Destination	Default Router	Netmask
<input type="text" value="0.0.0.0"/>	<input type="text" value="10.64.15.5"/>	<input type="text" value="0.0.0.0"/>
<input type="text" value="172.16.0.0"/>	<input type="text" value="172.16.200.100"/>	<input type="text" value="255.255.0.0"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 10 Network and Interface Configuration Page



Before you can change the Administrative Interface IP address on a system (the one with Allow Admin selected), you must delete all recorder configurations, delete all associations between master and client, and relinquish the master role. Failure to do so may require a reset to factory defaults on all units to recover.



In a multi-appliance configuration, access the Network and Interface Configuration page of each client appliance individually to configure network and interface settings.

Before you configure the network manually or using DHCP, enter the hostname of the appliance in the Hostname text box.



It is strongly recommended that you use static IP addresses rather than DHCP when you configure a stand-alone system. In a multi-appliance deployment, static IP addresses are required.

To configure the network manually (recommended), perform the following steps:

- 1 Choose **Administration > Network and Interface**.
- 2 Configure the following information:
 - Hostname, which may be a fully qualified domain name or just the simple name. It should be the same name that users specify when accessing the appliance with a web browser in order to avoid authentication warnings. Enter the host name before you configure the network manually or using DHCP.
 - Domain suffix, which is the default value that the appliance uses when looking up host names that have been supplied without a domain name.
 - Primary DNS IP address
 - Secondary DNS IP address (optional)
 - Properties for each interface (name, IP address, and netmask). Select Allow Admin on one interface. Refer to [Selecting the Administration Interface](#) on page 41.

- 3 Click **Update**.

To configure the network using DHCP (single units only), perform the following steps:

- 1 Choose **Administration > Network and Interface**.
- 2 Select **Use DHCP**.
- 3 Enter a name to identify the interface.
- 4 Select **Auto Negotiate** to use automatic speed and duplex settings.
- 5 Click **Update**.

DHCP automatically configures the IP address, netmask, default router, and primary and secondary DNS servers.

Selecting the Administration Interface

Administrative access to the appliance is available only through one of the configured interfaces. For configurations without an option card, this interface is one of the two RJ-45 jacks labeled Port 1 and Port 2 (Port 1 by default). If you have a multiple port option card, any of the interfaces can act as the Administration Interface. On the Network and Configuration page, click **Allow Admin** for the interface that acts as the Administration Interface.



For OSPFv3, you must specify an instance ID when configuring an interface.

Use the IP address that is associated with the interface to administer the appliance. The IP address is also used in the following ways:

- As a File Transfer Protocol (FTP) address for file transfer to the appliance.
- As an address where XML queries are sent.
- As an address required by technical support when any request for assistance is made.
- As an address for the X Window System or VNC client software connections.

Configuring VLAN Interfaces

The appliance can support virtual LAN (VLAN) interfaces that are configured on top of the physical Ethernet interfaces. By configuring VLAN interfaces on the Network and Interface Configuration page, you can ensure compatibility with network installations in which the switches present multiple VLANs on a port.

A configured VLAN interface can serve the same purposes as a physical interface, including serving as the selected administrative interface. You can configure multiple VLANs, for example, to connect to each of the areas in a multiple-area OSPF network.

To configure a VLAN interface, perform the following steps:

- 1 Choose **Administration > Network and Interface**.
- 2 In the VLAN Interfaces section, select the desired interface from the Interface drop-down list.
- 3 Enter the VLAN ID.
- 4 Click **Update**.

The new interface is added to the table near the top of the page, and a new entry line is added in the VLAN Interfaces area. Add additional VLAN interfaces as needed by repeating the previous steps.

- 5 For each VLAN, enter the following information in the interface table.
 - Name (optional)
 - IP address
 - Netmask
- 6 Click **Update**.

To modify an interface, make changes, and click **Update**. To remove an interface, manually erase the details, and click **Update**.

Configuring Alias Interfaces

Use an alias interface to add an additional IP address to an interface inside the netmask that is configured for that interface.

To configure an alias interface, perform the following steps:

- 1 Choose **Administration > Network and Interface**.
- 2 In the Alias Interfaces section, select the desired interface from the Interface drop-down list.
- 3 Enter a name for the alias in the Alias Name text box.
- 4 Enter the IP address in the IP Address text box.
- 5 Click **Update**.

The new interface is added to the table near the top of the page, and a new entry line is added in the Alias Interfaces area. Add additional alias interfaces as needed by repeating the previous steps.

- 6 For each alias interface, enter the following information in the interface table.
 - Name (optional)
 - IP address
 - Netmask
- 7 Click **Update**.

To modify an interface, make changes, and click **Update**. To remove an interface, manually erase the details, and click **Update**.

Configuring a Static Route

Use a static route to route packets directly to a specific router in a particular network area. If the address of the Administration Interface is configured, as recommended, then you must also configure a default static route.

For EIGRP topologies, the default route configured on an interface must be suitable for a Telnet or SSH transmission to all routers in the autonomous systems monitored on that interface. If multiple physical interfaces or tunnels are configured, you can configure a separate default route on each interface by specifying a target router on the subnet of the interface.

If no default route is set on a particular interface, the EIGRP Route Recorder uses policy routing to direct Telnet or SSH packets through one of the EIGRP peer routers. All the EIGRP peer routers on an interface are suitable for this purpose. In this case, you must install a default route on that interface to avoid

the possible selection of an unsuitable peer. If more than one interface is connected to the same autonomous system (for improved visibility), the Route Recorder prefers a broadcast interface over a tunnel interface. [Configuring the Route Recorder for the Collector](#) on page 73 describes how to configure the Collector for non-EIGRP topologies.



The appliance does not monitor the Internet Control Message Protocol (ICMP) redirect messages that are used by some enterprises to route around failures. The appliance does not accept ICMP redirects to update its routing table.

To add a static route, perform the following steps:

- 1 Choose **Administration > Network and Interface**.
- 2 In the Static Routes section, enter the destination, default router, and netmask.
- 3 Click **Update**.

The new interface is added to the table near the top of the page, and a new entry line is added in the Static Routes area. Add additional static routes as needed by repeating the previous steps.



You can override the default gateway that is inserted by DHCP by adding two static routes: 0.0.0.0/128.0.0.0 and 128.0.0.0/128.0.0.0.

To modify a static route, make changes, and click **Update**. To remove a static route, manually erase the details, and click **Update**.



It can take up to 30 seconds before a static route becomes visible while the new information is written to the system asynchronously. If you click **Update** again in this time period, the new static route information is erased. If the page returns earlier and does not display the new routes, click **Reload** on the browser to refresh the page.

Configuring Multiple Port Options

You can monitor a different OSPF or IS-IS area or EIGRP autonomous system with each of the ports on the appliance, including those on a multiple port option card. Multiple area monitoring is also available using tunnels. See [Configuring GRE Tunnels](#) on page 101 for more information.

To set up multiple port monitoring, keep the following factors in mind:

- The default router must be on the same network as the Administration Interface.
- One of the interfaces must be the Administration Interface. RAMS defaults to slot 0 port 1.
- You can use DHCP to set the IP address on the Administration Interface.
- You must assign an IP address to each of the ports or interfaces.

To configure multiple ports from the [Network & Interfaces Configuration](#) page, perform the following steps:

- 1 Choose **Administration > Network and Interface**.
- 2 Click **Allow Admin** to switch the administrative interface to the desired port.
- 3 To use DHCP on the Administrative Interface, select **Use DHCP**.



It is strongly recommended that you use a static IP address rather than DHCP. In a distributed configuration, a static IP address is required.

- 4 For each of the other interfaces on the card, enter the following information in the appropriate text boxes:
 - Name (optional)
 - IP address
 - Netmask
- 5 Click **Update**. It may take some time for all of the interfaces to become active.

After the network is configured, check that the network settings are correct by reviewing the View Configuration page.

Configuring SNMP Agent security

You can define the security settings that apply to the Simple Network Management Protocol (SNMP) agent running on the appliance by way of the SNMP Agent Configuration page. See [Configuring the Route Recorder for the Collector](#) on page 73 for information on how SNMP is used with the Collector.

If you plan to use SNMPv3, see [Configuring SNMP v3 Profiles](#) on page 80 for instructions on defining SNMP v3 profiles before you configure SNMP agent security.

To configure SNMP agent security, perform the following steps:

- 1 Choose **Administration > SNMP Agent Configuration**.

The SNMP Agent Configuration page opens ([Figure 11](#)).

SNMP Agent Configuration

The screenshot shows the 'SNMP Agent Configuration' page. It contains three main configuration fields: 'v2 community name' with the value 'packet', 'v3 user' with the value 'user1', and 'v3 profile' with a dropdown menu showing 'authPriv'. Below these fields are two lines of explanatory text: '* read-only access' and '** select 'none' to disable v3'. At the bottom of the form is a 'Save' button.

Figure 11 SNMP Agent Configuration

- 2 If you plan to use SNMP v2, enter the SNMP v2 community name.
- 3 If you plan to use SNMP v2, select an SNMP v3 profile. See [Configuring SNMP v3 Profiles](#) on page 80 for instructions on defining SNMP v3 profiles.
- 4 Click **Save**.

Configuring SSL Certificate

The appliance web server uses a built-in self-signed certificate for SSL security on https connections. This may result in security warnings from web browsers that access the server. Use the SSL Certificate page to create a Certificate Signing Request (CSR). The CSR allows you to obtain and install a certificate that is signed by a public or corporate Certificate Authority (CA).

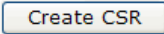
To create and submit a CSR:

- 1 Choose **Administration > SSL Certificate**.

The SSL Certificate page opens (Figure 12).

Web Server SSL Certificate Configuration

The web server is currently using a built-in self-signed certificate for SSL security on https connections. This may result in security warnings from web browsers accessing this server. You can obtain and install a certificate signed by a public (or company) Certificate Authority by creating a Certificate Signing Request here.

A rectangular button with a light gray background and a thin border, containing the text "Create CSR".

If you need to restore a private key and certificate for this web server created previously and backed up elsewhere, click here.

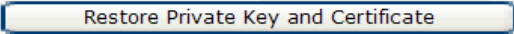
A rectangular button with a light gray background and a thin border, containing the text "Restore Private Key and Certificate".

Figure 12 SSL Certificate Page

- 2 Click **Create CSR** to display the request form.

Web Server SSL Certificate Configuration

Enter the information required to complete the Certificate Signing Request. See the guidelines from the Certificate Authority you will use regarding requirements for this information. The Common Name must be the name by which web browsers will refer to this server when making queries. This is normally the fully-qualified hostname of this unit. Some Certificate Authorities also require that the Organization Name be exactly the same as what appears at public domain name registries as the owner of the domain name that is part of the full-qualified hostname.

Number of bits in server key:	<input type="text" value="1024"/>
Country Name (2 letter code):	<input type="text"/>
State or Province Name (full name):	<input type="text"/>
Locality Name (city):	<input type="text"/>
Organization Name (domain name owner):	<input type="text"/>
Organizational Unit Name (optional):	<input type="text"/>
Common Name (web server's hostname):	<input type="text" value="rex71-215"/>

Figure 13 CSR Form

- 3 Complete all of the requested information, and click **Generate Key and CSR**. 1024 bits is the default.

The key and CSR are generated, and a page displaying the request opens.

Web Server SSL Certificate Configuration

Send the following Certificate Signing Request to the Certificate Authority.

Certificate Signing Request

[File Download](#)

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBuzCCASQCAQAwEzELMAkGA1UEBhMCVVMxExARBgNVBAGTCkNhbG1mb3JuaWEx
FDASBgNVBACTC1NhbhRhIENsYXJhMRYwFAYDVQQKEw1QYWNrZXQgRGVzaWduMRYw
FAYDVQQLEw1Eb2N1bWVudGF0aW9uMREwDwYDVQQDEwhjb2xvcmFkbzCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAyCLL/7FoZg6c0awIPiuyhXkftN1sM9J2vAH6
Nc4zzfYz21UgLuqh9F11ZNGkND7HF3If//Cg6tcz40/ZF61f7XasCYu9TzKKBTVs
D7eIAPzSvu0ii/XJfqdBnYwBo9Nbeig7LDZLnLW/PqmHhA8fdEicVdPtGjhlcSdF
Qv/1300CAwEAAaAAMAOGCSqGSIb3DQEBBQUAA4GBAMXL0YSkWXwB7GenprfQakGe
5KikA0D9gn+rHVJEhThnSGKEWOPdp8dCAH1AAJJ10Kp3unznf5B1vcPQ9/Xnnqd/
dlek2YIH9mZwLWm1B0uhZZ872K+Bb1K71yqH4RSvNgbh2zFTGiRaxvEs/qBkv5fn
9k1t/bBWbt4n08dmk+70
-----END CERTIFICATE REQUEST-----
```

The server's Private Key that corresponds to the CSR is kept on this unit, but should be backed up elsewhere. It is not encrypted, so it must be kept in protected storage.

Server Private Key

[File Download](#)

To abandon this CSR and continue using the built-in self-signed certificate, click here.

[Cancel CSR](#)

To begin using the signed Certificate returned by the Certificate Authority, paste or upload the Certificate here and click the button below.

Server Certificate

File Upload [Browse...](#)

[Clear](#)

[Use Certificate](#)

Figure 14 CSR Key and Download Options

- 4 Perform any of the following operations from this page:
 - Click **File Download** under Certificate Signing Request to download the CSR to be sent to the CA.
 - Click **File Download** under Server Private Key to download a copy of the server's private key for backup. The key is kept on the appliance, but it is strongly recommended that you back it up on another system. The key is not encrypted, so make sure that you have backed it up to a private and secure location.
 - Click **Cancel CSR** if you do not want to use the generated CSR, but instead want to continue to use the built-in self-signed certificate.
 - When the CA returns the signed certificate, copy and paste the certificate into the space provided or click **Browse** to upload the file containing the certificate. Click **Use Certificate**. Click **Clear** if you need to remove the pasted certificate.

After you click **Use Certificate**, the process is now complete. When users connect from a browser that has the CA certificate installed, no security warning is issued.

If you later return to the SSL Certificate page, the page presents the following options:

- Obtain a new certificate using the same CSR. You can use this option to add an updated certificate if the previous certificate is due to expire.
- Remove the installed Certificate and resume using the built-in, self-signed certificate. This option removes the CSR completely. If you decide to request a new certificate at a later time, you must complete a new CSR.

Viewing System Settings

System settings are listed on the View Configuration page for each appliance. To access the View Configuration page, choose **Administration > View Configuration**.

Configuring the Appliance for Recording

If you are working with a single-appliance configuration, proceed to [Configuring the Route Recorder](#) on page 55, where you'll configure the Route Recorder to listen to particular protocols.

In a multi-appliance deployment, components are configured and managed from the master appliance. All configuration tasks described in this section are performed on the Recorder Configuration page of the master appliance. You cannot configure or manage appliance components from the Recorder Configuration pages of client units. The Recorder Configuration page at the client level displays only that client's branch of the configuration hierarchy tree, where settings are view-only.

You must perform the following component management tasks in this order:

- 1 [Creating a Configuration Hierarchy](#) on page 52
- 2 [Configuring the Route Recorder](#) on page 55
- 3 [Adding Protocol Instances](#) on page 57
- 4 [Configuring the Flow Collector](#) on page 85 (RAMS Traffic only)



If the Flow Analyzer is already running when you begin recording on the Route Recorder or Flow Collectors, you must restart the Flow Analyzer as described on [Starting and Stopping the Flow Collectors](#) on page 89.

Additional configuration tasks include the following:

- [To listen to routing traffic on a network other than the local network, remotely connect that network to a secondary network interface on the appliance, or use a GRE tunnel to form the adjacency.](#) on page 101
- [Configuring a Loopback Interface for Cisco Routers](#) on page 105

Click **Recorder Configuration** on the top navigation bar to access the Recorder Configuration page.

Creating a Configuration Hierarchy

This section describes how to create a configuration hierarchy. Use a configuration hierarchy to organize components into a tree structure, with each branch representing a different part of the configuration. For example, [Figure 15](#) shows branches for RAMS Traffic for different protocols and the recorders that listen to those protocols. You can also organize the tree according to the area being monitored within each protocol.

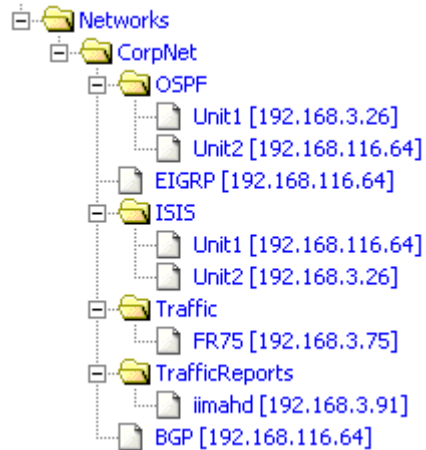


Figure 15 Configuration Hierarchy

The branches in the tree are grouped under a top-level administrative domain, represented by a folder icon on the web interface. You should first establish one top-level administrative domain so that you can easily rename the complete hierarchy of recorded databases for backup purposes. You can add multiple administrative domains beneath the top-level administrative domain as needed to organize the structure of the network, for example, to reflect geographical regions, or management divisions running separate protocol instances, or to designate traffic and reports instances. This tree structure is useful when opening a topology, because you can load the entire tree or focus only on particular branches. For more information, see the “The Routing Topology Map” chapter in the *HP Route Analytics Management Software User’s Guide*.

The organization of the tree is reflected by the Modeling Engine when you open a topology in the VNC or X viewer.

To begin creating a configuration hierarchy, perform the following steps:

- 1 On the master appliance, choose **Recorder Configuration** to open the Recorder Configuration page.
- 2 Click **Networks**.
A pop-up menu opens.
- 3 Move the cursor to **Add**, and select **Administrative Domain** (see [Figure 16](#)).



Figure 16 Administrative Domain

The Recorder Configuration page opens.

Recorder Configuration

Name of new Administrative Domain:

IP Address

Domain is a BGP AS Confederation

BGP AS Confederation Id:

Figure 17 Adding an Administrative Domain

- 4 Enter a name for the administrative domain. The name must consist solely of alphanumeric characters, with an alphabetic character first.

This is the top-level domain under which you will create the rest of your hierarchy.
- 5 (Distributed configurations only) In the IP Address field, choose **None** from the drop-down list if you are establishing a top-level domain. Otherwise, choose the IP address of the appliance to add to the hierarchy.
- 6 If the administrative domain represents a BGP confederation, perform the following steps:
 - a Select **Domain is a BGP AS Confederation**. A BGP confederation is a domain that contains multiple member autonomous systems, but appears to outside autonomous systems to have a single AS identifier. For more information, see [Configuring a BGP Confederation](#) on page 60.
 - b Enter the confederation ID number in the BGP AS Confederation Id text box.
- 7 Click **Add Domain**.
- 8 Click the + symbol to the left of Networks to open the folder that shows the domain name you just entered.
- 9 See the next section, [Configuring the Route Recorder](#) on page 55, to configure one or more Route Recorders to listen to different protocols across the network.

Configuring the Route Recorder

This section introduces the main functions of the Route Recorder and describes how to configure a Route Recorder to start recording. You must configure the Route Recorder before configuring other appliance components.



Set the time and date before configuring the recorder, per the instructions described in [Setting the Time and Date](#) on page 26. The date and time must be set before data recording begins because the system relies on accurate time stamps to generate reports. We strongly recommend that you use NTP to set the time and date.

In a deployment with multiple Route Recorders, you can configure different network segments to be recorded by different Route Recorders and configure each to listen to one protocol or multiple protocols per area or AS. Only one Route Recorder can record per area or AS.

To add a Route Recorder to the configuration hierarchy, perform the following steps:

- 1 Choose **Recorder Configuration** on the master appliance.
- 2 Click the top-level domain name you added in [Creating a Configuration Hierarchy](#) on page 52 (for example, CorpNet).
- 3 Move the cursor to **Add**.
The option to add another level of domain name hierarchy appears, as shown in [Figure 16](#).
- 4 Click **Administrative Domain**.
The **Name of new Administrative Domain** box appears as shown in [Figure 17](#).
- 5 Enter a name for the administrative domain. The name must consist solely of alphanumeric characters, with an alphabetic character first (for example, IGPRecorders).
- 6 (Distributed configurations only) From the **IP Address** drop-down list, choose the IP address of a Route Recorder, or choose **None**. When you choose **None**, you create a branch in the configuration tree that you can use to organize the tree by protocol or by area. For example, assume that you

add a IGPRecorders branch to the tree. In subsequent steps, you can add OSPF and IS-IS branches under IGPRecorders. Then, under OSPF and IS-IS, you can add one or more Route Recorders.

- 7 If the administrative domain represents a BGP confederation, perform the following steps:
 - a **Select Domain is a BGP AS Confederation.**

A BGP confederation is a domain that contains multiple member autonomous systems, but appears to outside autonomous systems to have a single AS identifier. For more information, see [Configuring a BGP Confederation](#) on page 60.
 - b Enter the confederation ID number in the BGP AS Confederation ID text box.
- 8 Select the check box for MPLS WAN if you want to set up this domain as an MPLS WAN site. See the “MPLS WAN” chapter in the *HP Route Analytics Management Software User’s Guide* for guidelines on setting up a domain as an MPLS WAN site.
- 9 **Click Add Domain.**

The domain name you just entered (for example, IGPRecorders) appears in the hierarchy.

The Route Recorder listens to routing protocol packets and records that data in a database. To set up the databases, refer to [Adding Protocol Instances](#) on page 57.

Recorder Configuration Restrictions for MPLS WAN

The following guidelines apply to recording by protocol for MPLS WAN. For more information, see the “MPLS WAN” chapter in the *HP Route Analytics Management Software User’s Guide*.

- Record IGP protocols as usual (via tunnels if needed).
- Record internal BGP (IBGP) peering with customer edge (CE) routers.
- For static recording:
 - There is usually one static instance per network.
 - Collect static routes from CE routers if they have static routes to/from provider edge (PE) routers.

- Create a static instance (even if there is no route collection), for MPLS WAN with traffic.
- Traffic (if applicable):
 - Put all traffic-related instances outside of sites
 - Record traffic at a site through all CE interfaces (simple) or through CE interfaces on CE-PE links, plus interfaces with outbound traffic to capture the effect of outbound traffic.
 - You can record traffic differently on different sites, but do not mix the different recording options within the same site.

Adding Protocol Instances

The appliance uses a hierarchical tree to represent the collection of IGP and BGP routing protocols to be recorded and the relationships among them.

Each instance of an IGP or BGP routing protocol is represented by a page icon as a leaf in the tree. A protocol instance includes the set of routers that communicate directly with each other using that routing protocol. For example, the routers within a set of interconnected OSPF areas form one protocol instance.

Note that multiple instances of the same protocol cannot be configured within a single administrative domain. If a network contains two instances of the same protocol, then you must create two administrative domains to contain them. Also, a BGP instance cannot be configured in an administrative domain whose ancestor directly contains a BGP instance.

Before starting to record routing data using the Route Recorder, you must assign a name to the database where the data will be stored. You must also specify the routing protocol (IS-IS, OSPF, EIGRP, or BGP) and the network interface used to listen to the routing protocol packets.



For each interface, the appliance supports an interface password and an area or domain password. If that interface is recording Level 1, enter the area password when configuring that interface in the recorder configuration. If the interface is recording Level 2, the domain password should be used. If the interface is recording both Level 1 and Level 2, then the area and domain passwords configured on the router must be the same.

When configuring the appliance for the first time, at least one database must be specified for storing routing data.

To add a protocol instance and start recording routing data, perform the following steps:

- 1 Choose **Recorder Configuration** on the master appliance.
- 2 Click the label that you added in [Configuring the Route Recorder](#) (for example, IGPRecorders) and choose **Add**.
- 3 Choose the desired type of protocol instance (BGP, OSPF, OSPFv3, IS-IS, or EIGRP).

One of the following options is displayed to the right of the configuration tree:

- If the label you added in [Configuring the Route Recorder](#) is bound to an IP address, the configuration section for the selected protocol appears. Proceed to [Configure an IGP Instance](#) on page 61 or [Configure a BGP Instance](#) on page 68 for detailed instructions about how to configure the protocol instance.
 - If the label you added in [Configuring the Route Recorder](#) is unbound, a drop-down list of Route Recorders appears with the **Select a unit** button. Proceed to Step 4.
- 4 Choose one of the following options, and then click **Select a unit**:
 - If you will be adding only one Route Recorder under this protocol, choose the Route Recorder's IP address from the drop-down list. The configuration section for the selected protocol appears. Proceed to [Configure an IGP Instance](#) on page 61 or [Configure a BGP Instance](#) on page 68 for detailed instructions about how to configure the protocol instance.
 - If you will be adding more than one Route Recorder under this protocol, choose **Multiple** from the drop-down list. Proceed to Step 5.
 - 5 Click the protocol label you just added and select **Add Route Recorder** from the pop-up menu. Then choose the IP address of the Route Recorder from the pop-up menu.

The configuration section for the selected protocol appears on the right side of the Recorder Configuration page. For detailed instructions about how to configure the protocol instance, see [Configure an IGP Instance](#) on page 61 or see [Configure a BGP Instance](#) on page 68.



You do not need to stop recording to configure protocol instances.

- 6 You can configure additional protocol instances by repeating the preceding steps.



You can add multiple different protocol instances under one administrative domain, but only one instance of a particular protocol is allowed.

The structure of the administrative domain hierarchy also affects how the appliance associates the protocol instances to connect them in the routing topology map and to calculate routes. The next sections explain the requirements to consider when you configure the hierarchy:

- Correct interconnection of BGP and IGP protocol instances depends on their proximity in the hierarchy.
- If the network is a BGP confederation, this must be indicated in the administrative domain configuration.
- You can configure multiple EIGRP autonomous systems in one administrative domain or in separate ones.

After you determine the administrative domain hierarchy that is appropriate for your network, see the specific instructions in [Configure an IGP Instance](#) on page 61.

The appliance supports up to 100 areas. This limitation applies to the total of OSPF areas, IS-IS areas (levels), EIGRP autonomous systems, and BGP autonomous systems.

Interconnection of BGP and IGP Protocol Instances

A single physical router can run multiple routing protocols and be a member of multiple protocol instances. The appliance will attempt to consolidate all the instances of that router as a single node on the routing topology map so that the protocol instances will be connected. Because the various protocols identify routers in different ways, the appliance employs a heuristic algorithm to match routers.

A BGP node that peers with the appliance is identified by the peering address, while a BGP node created as a next-hop from a BGP peer is identified by the address in the BGP NextHop attribute of some of the routes learned from that BGP peer. The appliance searches for the nearest IGP protocol instance in the hierarchy containing a router with matching router ID or interface address, or, failing those, a router that advertises a prefix containing the BGP address. If the hierarchy is configured with an administrative domain for each AS containing the BGP and IGP protocol instances of that AS, the intended IGP protocol instance will be nearest. However, if the hierarchy is configured inappropriately, the closest IGP with a match might not be correct.

For example, consider a network with two BGP and two IGP instances. Here, the two BGP instances represent two BGP autonomous systems that are connected with an external BGP peering across a link. In each AS, The appliance would peer with the BGP router on the end of the link in that AS, and from that peer it would learn routes of the other AS. Along with these routes, it would also learn an interface address of the BGP router on the other end of the link using the BGP NextHop attribute of the routes.

To join the two autonomous systems by a link on the map, the appliance must consolidate this interface address with an IGP router in the other AS. To do this, it first finds the BGP instance of the next-hop router using the AS number from the BGP AS path attribute, and then it searches from that point in the hierarchy for the closest IGP instance containing a matching router as described above. If each of the BGP and IGP instances were in its own administrative domain under the Separate domain rather than being paired in the East and West domains, then both IGP would be equally distant and either might have matched (because both are likely to advertise a prefix covering that interface address). As a result, the wrong IGP might be found first, causing the next-hop router to be consolidated with the router at the wrong end of the link.

Configuring a BGP Confederation

A BGP confederation is a domain that contains multiple member autonomous systems but appears to outside autonomous systems to have a single AS identifier. If your network is configured as a BGP confederation, you must create an administrative domain to represent the confederation and configure it with the confederation AS identifier. Under that administrative domain, you then configure an administrative domain for each member AS.

There are two types of BGP confederations. The member BGP autonomous systems in the confederation may all be contained within one IGP domain, or each member BGP AS may be running a separate IGP instance. The

administrative domains **Common** and **Separate** are the ones that represent the confederation in each case. Underneath these are the West and East administrative domains, each of which contains a BGP instance for the member AS. For the common IGP case, a single IGP instance is configured under the confederation domain. For the separate IGP case, an IGP instance is configured along with the BGP instance in each member AS domain. You can adapt the approaches in these examples for monitoring your BGP confederation. See [Configure a BGP Instance](#) on page 68 for guidelines on configuring BGP.

Configuring Multiple EIGRP Autonomous Systems

A network with multiple EIGRP autonomous systems can be configured in either of the following ways:

- Configure a single protocol instance with multiple network interfaces that are connected to the different EIGRP autonomous systems, provided that no two autonomous systems have the same number.

Advantages: Fewer configuration steps are required, and the autonomous system configuration need only be entered once.

- Create separate administrative domains for each AS, each with its own protocol instance. However, you can only configure a particular network interface under a single protocol instance, so you must configure all of the autonomous systems that may be heard on a single interface under the same domain and protocol instance.

Advantages: Each AS can be given a name rather than being identified only by number.

Configure an IGP Instance



After you create an OSPF, IS-IS, or EIGRP protocol instance, the configuration section for the selected protocol instance appears on the right side of the Recorder Configuration page, as shown in [Figure 18](#).

Protocol ISIS

Name : Dynamips.AudiBug12113

Capture raw protocol packets

Record protocol packet events

IPv6

Interfaces

Active	Not Active
<div style="border: 1px solid gray; padding: 2px;">Slot 0/Port 1</div>	<div style="border: 1px solid gray; padding: 2px;"> Tunnel-49.4000-R3-L1L2 TunnelR21 TunnelR31 </div>

Status

Interface	Area	Last Hello	Last Event	Neighbor ID	Adjacency Status
Slot 0/Port 1	Level 2	Mon Feb 16 13:28:21 2009	Mon Feb 16 13:27:36 2009	1760.1600.1001	full

Disk space used: 64%

Figure 18 Configuring an IGP Protocol Instance

The following buttons and check boxes may appear on-screen, depending upon the specific instance you specified:

- **Capture raw protocol packets**—Save the protocol packets (BGP updates, LSPs, or LSAs) in the format in which they are observed over the network.
- **Record protocol packet events**—Enable recording of a pseudo-event that marks packet arrivals in the detailed Events table. You can then view the pseudo events in the History Navigator. The pseudo-events are interspersed with the real events. By recording the protocol packet events, you can determine whether the routing protocol is behaving properly, for example, whether the update refresh rate is correct.
- **IPv6**—Record IPv6 prefixes (IS-IS protocol only).
- **Configure**—Choose this button to configure an interface. This button is enabled once you make a selection in the Active or Not Active columns.

- **Delete**—Choose this button to delete an interface from the Not Active column. This button is not enabled if you make a selection from the Active column.
- **New Tunnel**—Choose this button if a GRE tunnel is required to connect to a remote router. See [Configuring GRE Tunnels](#) on page 101 for instructions.
- **Start/Stop Recording**—Choose this button to start or stop recording.



Recording does not need to be stopped to configure protocol instances.

- 1 Follow the steps on [page 58](#) to open the Recorder Configuration page and specify the protocol to configure.
- 2 To receive diagnostic trace information for your network, select **Capture raw protocol packets**. The information is saved in a log file within the ftp directory.
- 3 Beneath the Interfaces section of this page, the configured network interfaces are displayed in the Not Active column, and the interfaces that are currently available for recording display in the Active column. Select the interface that is connected to a network area or autonomous system you wish to configure. You can toggle the selections between the columns using the < and > buttons.
- 4 If a GRE tunnel is required to connect to a remote router, click **New Tunnel**, and then follow the instructions in [Configuring GRE Tunnels](#) on page 101 to create the tunnel interface.

For EIGRP, there can be multiple interfaces connected to a single autonomous system in order to get complete coverage. You may need to configure a default route for each interface as described in [Configuring a Static Route](#) on page 43.



The procedures for configuring an IGP instance vary between the protocols after Step 5. If you are configuring for IS-IS protocol, continue to Step 6. If you are configuring for OSPF, continue to Step 7, and if you are configuring for EIGRP, continue to Step 9.

- 5 Enable authentication by selecting the desired interface from the Active column, and click **Configure**. The Configure Interface page opens, as shown in [Figure 19](#).

Configure Interface		
Interface	ISIS Authentication	GRE Tunnel
Tunnel_TO_120.21	Interface: <input checked="" type="checkbox"/> HMAC MD5 <input type="checkbox"/> Simple Password: <input type="password" value="..."/> Area/Domain: <input type="checkbox"/> HMAC MD5 <input type="checkbox"/> Simple Password: <input type="password"/>	Remote IP Address: <input type="text" value="192.168.120.21"/> Tunnel Destination Local IP Address: <input type="text" value="10.204.204.2"/> Netmask: <input type="text" value="/30"/> Interface: <input type="text" value="Slot 0/Port 1"/>
<input type="button" value="Update"/> <input type="button" value="Cancel"/>		
<input type="button" value="Stop All Recording"/> <input type="button" value="Start All Recording"/>		

Figure 19 Configure Interface Page for IGP (IS-IS Protocol)

- 6 (IS-IS only) Select the form of authentication you wish to use for the interface or the area/domain for the interface:
 - MD5 (Message Digest Algorithm 5) Key-ID: requires a password (up to sixteen characters) and a Key-Id (a number between 1 and 255, inclusive)
 - Simple: requires only a password (up to eight characters)

After entering the information, click **Update**.

You can now begin recording routing topology information for this IS-IS protocol instance, or you can complete the configuration of all other protocol instances in the topology, if any, before you begin recording.

- 7 (OSPF only) Select the form of authentication you wish to use for OSPF authentication:
 - MD5 Key-ID: requires a password (up to sixteen characters) and a Key-Id (a number between 1 and 255, inclusive)
 - Simple: requires only a password (up to eight characters)



To monitor two OSPF areas that are linked to a single Cisco router, you must configure a loopback interface on the router to monitor both areas with RAMS Traffic. See [Configuring a Loopback Interface for Cisco Routers](#) on page 105.

- 8 After entering the information, click **Update**.

You can now begin recording routing topology information for this OSPF protocol instance, or you can complete the configuration of all other protocol instances in the topology, if any, before you begin recording.



Steps 3 through 14 are for configuring EIGRP protocol instances only.

- 9 (For EIGRP only) For an EIGRP instance, one or more autonomous systems must also be configured. Click **New AS** to display the autonomous system configuration section, as shown in [Figure 20](#).

For a network with more than one EIGRP AS, there are two configuration choices as explained in [Configuring Multiple EIGRP Autonomous Systems](#) on page 61.

Configure Autonomous System	
AS Number (0 for any):	<input type="text"/>
Periodic Explore Interval* (hours):	<input type="text" value="8"/>
Periodic Explore Start Time (00:00 - 23:59):	<input type="text" value="4:00"/>
Full Explore Interval* (hours):	<input type="text" value="48"/>
Full Explore Start Time (00:00 - 23:59):	<input type="text" value="4:00"/>
Max. Outstanding Queries:	<input type="text" value="10"/>
Telnet Line Password:	<input type="text"/>
TACACS/SSH Username:	<input type="text"/>
TACACS/SSH Password:	<input type="text"/>
Login Method :	<input checked="" type="checkbox"/> telnet <input type="checkbox"/> ssh

Configure Blocked Interfaces	
Interface Address	Remove
<input type="text"/>	<input type="text"/>

Configure Interface Passwords			
Interface Address	Username	Password	Remove
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 20 Configuring an EIGRP Autonomous System

- 10 In the Configure Autonomous System table, specify the following:
- Enter either an explicit AS number or zero to allow the appliance to record all autonomous systems that are heard on the selected interfaces. To restrict the recording to a subset of the autonomous systems that may be heard, configure each desired AS number explicitly, one at a time.
 - Topology Exploration parameters:
 - **Periodic Explore Interval**—Determines the frequency of periodic exploration, and may be configured or left at its default value of 8 hours. Entering zero disables periodic exploration.
 - **Periodic Explore Start Time**—Determines when periodic exploration begins, and is expressed in 24-hour clock mode in the time zone set on RAMS Traffic.
 - **Full Explore Interval**—Determines the frequency of full topology exploration, and may be configured or left at its default value of 48 hours. Entering zero disables exploration.

- **Full Explore Start Time**—Determines when full exploration begins, and is expressed in 24-hour clock mode in the time zone set on RAMS Traffic.
- You can change the setting for Max Outstanding Queries, but the default value is recommended. This setting controls the maximum number of routers to which simultaneous Telnet or SSH connections will be issued to query topology information using the command line interface.
- **Telnet Line Password, Terminal Access Controller Access-Control System (TACACS)/SSH Username, and TACACS/SSH Password**— These authentication parameters are used to access the command line interface of the routers to collect information about the network topology using **show** commands. If all routers use the same line password or TACACS username and password combination, enter the router line login password or a TACACS username and password combination (or both if some routers will use one and some routers will use the other). You can supply an optional second set of these parameters if, for example, some routers are managed by one server and some by another. The TACACS fields can also be used for username and password authentication when the routers are configured to use Remote Authentication Dial In User Service (RADIUS) or a locally configured set of accounts.



Refer to Step 13 if each router in the AS has a unique simple password or TACACS user name and password combination.

- In the Login Methods area, select the method that the appliance will use to log into routers to collect EIGRP topology information by selecting **telnet**, **SSH**, or both if some routers use Telnet and some use SSH. If both are selected, SSH will be tried first.
- 11 In the Configure Blocked Interfaces table, specify any router interfaces that you do not want included in the topology map.

You can use this feature to specify routers that RAMS Traffic should not attempt to log into, or to limit the scope of the RAMS Traffic topology exploration.
 - 12 Enter an interface address, and then click **Update AS**.

- 13 Use the Configure Interface Passwords table to override the generic passwords that are specified in Step 10 for any router that has a password different from those specified in the Configure AS table. Enter an interface address and its password or TACACS user name and password combination, and then click **Update AS**.



You must configure the password for all interfaces on the router.

- 14 When you have configured all of the autonomous systems, blocked interfaces, and interface passwords, click **Save** to complete the recorder configuration process.

You can now begin recording routing topology information for this EIGRP protocol instance, or you can complete the configuration of all other protocol instances in the topology, if any, before you begin recording.

Configure a BGP Instance

After you create a BGP protocol instance as described in [Adding Protocol Instances](#) on page 57, the BGP configuration section appears on the Recorder Configuration page as shown in [Figure 21](#). This section presents guidelines for choosing the peerings to establish between the appliance and the BGP routers.

		Peers
BGP Id: 192.168.122.90		
Confed Id: 65533		
Member AS: 65510		
Name: LabRight_ConfedsTest_ConfedTestTop: BGP		
Interface:	ConfedAlias2	
<input type="checkbox"/> Log Traces		
Save		
		25.0.0.1
		25.0.0.21
		Add
		Edit
		Delete

Figure 21 Configuring a BGP Instance

For every configured BGP AS, the AS number and list of IP addresses of peers in the AS are required during configuration. Configure each as an IBGP peer with the appliance. It is important that no policies are applied to the routes

sent to the appliance. The appliance does not send any routes to its peers. Nevertheless, you should install filters on the peer routers to prevent the acceptance of any routes from the appliance.

If multiple autonomous systems are monitored, you must assign an alias must for each additional AS. Aliases are logical interfaces that are created by the operating system (OS) and assigned their own IP addresses. They behave in the same way as any other physical interface. Aliases identify the multiple personalities that are required for participation in multiple autonomous systems. These additional addresses can be the tunnel end-point addresses or they can be configured IP alias addresses. See [Configuring Alias Interfaces](#) on page 42. Any tunnels should be into the corresponding autonomous systems.

If you use IP alias addresses, all the addresses should be from the AS to which the main/physical routing interface connects. The router at the other end of this interface connection should ensure that each of these addresses is routable. The easiest way to ensure this is to assign all of the alias addresses from the same address block as the interface (from the subnet of the interface). In this case, no additional configuration is required in the AS routers. However, when the additional IP addresses are not from the same subnet block, the static routes to the AS routers must be configured and injected into the IGP/BGP so that the system is reachable from each BGP peer.

Use the following approaches (in order of preference) to configure a BGP instance in relation to the IBGP full mesh:

- 1 Ensure that the system participates as part of the IBGP full mesh with a neighbor relationship (peer relationship) with all of the IBGP routers. This allows the appliance to have access to all of the IBGP updates sent by all of the routers in the mesh. The appliance constructs the topology from the same perspective as the other IBGP routers.
- 2 If your network has route reflectors, you can set up a peer (neighbor) relationship between the appliance and all of the Route Reflectors in the network. Note that you are configuring the Route Reflectors to treat the appliance as a peer, not as a client. In this scenario, the appliance receives all of the updates from Route Reflector clusters. This provides information

about all routes being advertised, but the information is more limited than if the appliance were part of the full IBGP mesh. In particular, if some of the Route Reflector clusters have multiple exit points for the same route, the appliance might be able to see only a few (if there are multiple route reflectors present in the cluster), or only one of the exit points.

- 3 The least preferred method is to configure the appliance as a Route Reflector client. This option provides only one view of the network, that of the Route Reflector. This limits the ability of the appliance to do some types of analysis, but route tracing should work correctly.

To increase the available amount of routing information, you can configure the appliance to be a client of several key Route Reflectors. For best coverage, you should select Route Reflectors in geographically distant major PoPs.



When you set up peer relationships with Route Reflectors as a client, the total number of received routes is the product of the number of Route Reflectors multiplied by the number of prefixes. Because the total number of advertised routes can be very high, it is recommended that the appliance support no more than 10 Route Reflectors when it is configured as a client.

You can choose the third option even if you do not currently have any Route Reflectors in your network. You can configure any router to be a Route Reflector to peer with the appliance. This does not affect the other BGP neighbors of the router, because Route Reflector is a per-neighbor setting. Consider the third option if the first two options would entail too much configuration effort. If you choose the third option and later decide to change to the first or second option, you can simply reconfigure the Route Reflectors to treat the appliance as a peer instead of a client.

Configuring the appliance as an external BGP peer is not recommended because there are several drawbacks associated with EBGP peer relationships:

- EBGP routing information does not include certain BGP attributes such as the NextHop, Local-Pref, and MED attributes. These attributes are essential to determine the best BGP routes inside an AS. Without them, the appliance is unable to determine the correct exit routers or find correct paths for BGP prefixes.

- From each of the EBGP peers the appliance will learn one route for each prefix known in the autonomous system, rather than only those routes for which the peer is responsible. This applies unless a policy filter is used to limit this information. If the appliance peers with many BGP routers in the AS, the total number of routes may exceed its capacity.
- Although the appliance will be maintaining many more routes than with IBGP peering, the fidelity of the routing information is less due to missing attributes. Without the attributes, the routes passed to the appliance by different routers is almost identical.

After you have configured a BGP instance for IBGP peering with the routers in your own AS, you may want to determine which routes are advertised to other autonomous systems. For this purpose, you can configure the appliance with a separate BGP instance to EBGP peer with one or a few of the border routers in your AS.

In a BGP confederation, configure the appliance to peer with each member AS using one of the three approaches described earlier in this section for a non-confederated BGP AS. For each member AS, configure the appliance as an IBGP peer to participate in the full mesh of IBGP routers in the member AS, or as a Route Reflector peer or client. You must assign a different alias to the appliance for each member AS.

If your appliance has a license for BGP and VPN protocols and you want to monitor VPN routing, you can collect complete routing information by configuring peering to all of the PE routers or to all of the Route Reflectors that serve the VPN routes in the AS. When configuring each peering, enable BGP extensions for MPLS VPNs, as indicated in the next procedure. See the “VPN Routing” chapter in the *HP Route Analytics Management Software User’s Guide* for more information about configuring customer/Route Target (RT) associations for routing reports.



When configuring BGP peers in the recorder configuration, you can configure a prefix (such as 192.168.0.0/24), rather than multiple individual peer addresses that fall within that prefix. However, it is not possible to use MD5 authentication if a prefix is used for the peer configuration.

To configure a BGP instance, perform the following steps:

- 1 Follow the steps on [page 58](#) to open the Recorder Configuration page and specify the protocol to configure.

- 2 Enter the BGP IP address in the **BGP Id** box.
- 3 Enter the autonomous system number in the **AS** box. If the BGP protocol instance is within a confederation, enter the AS number of the member in the **Member AS** box. This is not the confederation ID, which is shown separately.
- 4 From the **Interface** drop-down list, select the physical interface slot and port or select the logical interface alias.
- 5 To receive diagnostic trace information for your network, select **Capture raw protocol packets**. The information is saved in a log file within the ftp directory.
- 6 In the **Peers** column, click **Add** to add peers.
The peer configuration table opens at the left side of the screen as shown in [Figure 22](#).

Peer Information	Options
IP Address(es) or Prefix(es): <input type="text"/> AS: <input type="text"/> MD5 Password: <input type="text"/>	<input checked="" type="radio"/> Internal <input type="radio"/> External <input type="checkbox"/> BGP ext for MPLS VPNs <input type="checkbox"/> BGP ext for IPv6
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	
<input type="button" value="Stop All Recording"/> <input type="button" value="Start All Recording"/>	

Figure 22 BGP Peer Configuration

- 7 In the **Peer Information** column, enter the IP address or addresses of the peers, and the MD5 password of the peer, if applicable.
You can add multiple peers at once by typing each IP address on a separate line in the IP Address text box.
- 8 In the **Options** column, specify whether the peers are internal or external.
If you enter multiple peers at once, all of the peer addresses must share the same internal or external setting.
- 9 If this BGP topology is a BGP MPLS VPN, select **BGP ext for MPLS VPNs**. Otherwise, leave this check box empty.

- 10 If this BGP topology is a BGP IPV6, select **BGP ext for IPV6**. Otherwise, leave this check box empty.
- 11 When you have entered all information for the peers, click **Update Peer** to return to the BGP instance configuration.
- 12 Click **Save**.

You can now begin recording routing topology information for this protocol instance, or you can complete the configuration of all other protocol instances in the topology, if any, before you begin recording.

To Edit a BGP Peer, perform the following steps:

- 1 In the **Peer** column shown in [Figure 21](#), click on the peer you wish to edit.
- 2 Click **Edit**.
The BGP Peer Configuration table displays.
- 3 Modify the fields you wish to edit, and click **Save**.



You can delete multiple BGP peers by selecting the peers you want to delete, and then clicking the **Delete** button.

Configuring the Route Recorder for the Collector

This section describes how to configure the Route Recorder for the Collector, which collects router interface information, static and connected routes, and VRF-related information.



The available Collector capabilities depend upon the installed licenses.

The Collector process uses SNMP, Telnet, and/or SSH to gather information on all topologies except EIGRP. (For EIGRP, the same interface parameters and static route information is collected using Telnet or SSH as part of acquiring the EIGRP topology.) The Collector records two kinds of routes: connected and static. A router maintains a connected route for each of its network interfaces based on the prefix specified the interface. The Collector derives these connected routes from the interface information it retrieves using SNMP or SSH/telnet.

Static routes are manually configured on the router by specifying a destination prefix and the next hop to which a packet should be sent towards that destination. When the collection method is SSH/telnet, static routes are always collected, because doing so imposes very little additional load on the router and the network. When the collection method is SNMP, static routes are only collected if that option is selected. Collecting static route information using SNMP can consume substantial resources on the routers because it requires retrieving the full routing table.

You can configure SNMP collection of static routes from the subset of routers for which static routes are present and the routing table is not too large. Groups of routers are selected by specifying a prefix that covers one or more interface addresses on the routers. Multiple prefixes can be specified to apply different sets of collection parameters to different groups of routers. For any router address, the longest matching prefix determines the applicable parameters. To avoid undue resource load for routers with large routing tables, you can first configure collection of information without static routes on the full set of routers of interest (perhaps using the default 0.0.0.0/0 table entry that includes all routers known from the IGP and BGP protocols). Then separately configure one or more table entries with more-specific prefixes that have static route collection enabled to cover the subset of routers for which static routes are present and the routing table is not too large.

You can configure the Collector on any appliance that performs route recording. The scope of the Collector is determined by the location in the hierarchy that you choose when configuring the recorder and applies to the selected subtree (Figure 23). You can configure multiple Collector instances, provided that their scope is not overlapping. This may be desired for geographically distributed recorders. If you attempt to configure overlapping instances, an error message is displayed.

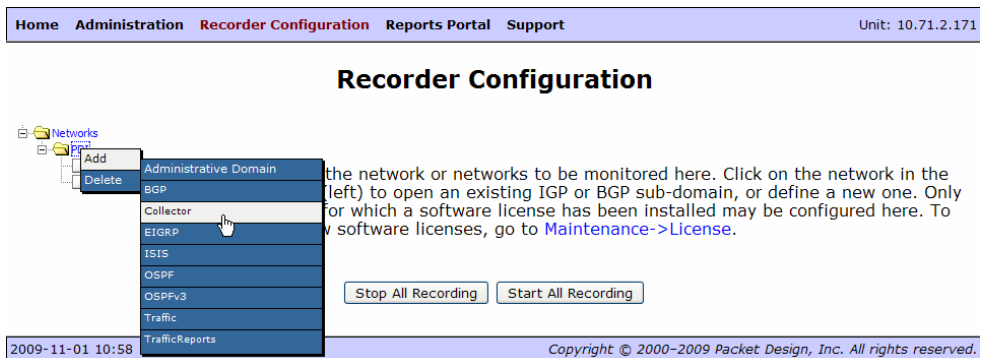


Figure 23 Choosing Scope for Collector

The appliance collects VRF-related information for VPN traffic reports and for VPN routing reports. To use these features, SNMP v2 or v3 is required on all platforms, and Juniper and Cisco routers also require Telnet/SSH. For a list of Juniper and Cisco router commands, refer to [Router Commands for the Collector](#) on page 1.

Before you configure the Collector, you must enable the XML RPC query server on the Route Recorder or Modeling Engine. On a distributed system, it is normally best to use the Modeling Engine, because it has the complete network topology and can provide the complete list of routers. If there is only one Route Recorder unit in the system, then selecting the Route Recorder itself is the right choice because that recorder will have the full network topology and that is the same appliance where the Collector will be running. If there are multiple Route Recorder units, however, you should select the Modeling Engine. For more information on the query server, see the *HP Route Analytics Management Software Developer's Guide*.

To enable the query server, perform the following steps:

- 1 Choose **Administration > Queries**.
- 2 Select the **XML-RPC Query Server** and **Enable remote access** check boxes.
- 3 Enter and confirm the password for query access.
- 4 Click **Update**.

To configure the Collector, perform the following steps:

- 1 Verify that the routers to be included in the Collector are configured for SNMP v2 or v3 and Telnet or SSH (for Juniper and Cisco routers).
- 2 Choose **Recorder Configuration**.
- 3 Click the desired level in the recorder hierarchy in the left navigation bar and choose **Add > Collector**.
- 4 If you have a distributed system, choose the Route Recorder appliance from the drop-down list, and click **Select** to open the Recorder Configuration window. (Figure 24). If you have a single appliance, it is not necessary to select the appliance to open the Recorder Configuration window.
- 5 Make changes as needed to the following Global Router Access Configuration settings:

- **Router list query server**—Indicates the Route Recorder or **Modeling Engine** where the query server is configured. The field is read-only if this is a single unit (not part of a distributed system). Otherwise, select the IP address of the query server that you enabled in the previous procedure.
- **Router list query server password**—Enter the same password that you configured for the query server in the previous procedure.
- **Router list refresh time**—Specifies the interval for polling the Query Server for the current list of known routers. A shorter interval allows detection of new routers more quickly so information will be collected from them; a longer interval reduces interference with user access to the Query Server.
- **Polling schedule**—Specifies the schedule used to query all routers that match the Collector configuration to collect any changes in the recorded information.
- **Discovery at next start recording**—If selected, indicates that the appliance begins performing discovery immediately when recording is started rather than waiting for the scheduled start time.

Recorder Configuration

Global Router Access Configuration

Domain: PECE_CORE
 Router list query server: 10.64.15.145
 Router list query server password: *****
 Router list refresh time (hours): 1
 Polling schedule: Hourly Day Thursday Hour 18 Minute 0
 Discovery at next Start Recording:

Global SSH/Telnet Parameters

Login User 1: Username packet Password *****
 Login User 2: Username admin Password *****
 Number of routers to query in parallel: 50

Global SNMP Parameters

SNMP v2 community: public
 SNMP v3 profile: arvind
 Number of routers to query in parallel: 50
 Interval between queries to a router (seconds) within the polling cycle: 1
 Collect Static Routes: Warning: Collecting static routes for SNMP is not advised for routers with large routing tables

Specific Router Access Configuration

Routers (Prefix)	SNMP	SSH	Telnet	SNMP v2 Community	SNMP v3 Profile	SNMP collect static routes*	SSH/Telnet Username	SSH/Telnet Password	Delete
10.120.1.5/32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		none	<input type="checkbox"/>			<input type="checkbox"/>
10.120.1.8/32	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	public	arvind	<input type="checkbox"/>			<input type="checkbox"/>
10.120.1.17/32	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	public	arvind	<input type="checkbox"/>	admin	*****	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		none	<input type="checkbox"/>			<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		none	<input type="checkbox"/>			<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		none	<input type="checkbox"/>			<input type="checkbox"/>

*Warning: Collecting static routes for SNMP is not advised for routers with large routing tables
 Warning: A router gets black listed if no login method (SNMP/SSH/Telnet) is selected

SNMP Status

Status	Last Status Update
Up	Fri Sep 11 12:51:17 2009

Show password

Figure 24 Recorder Configuration Window for the Collector

- 6 If you are using SSH and/or Telnet, you can configure the following global SSH/Telnet parameters to be referenced by entries in the Specific Router Access Configuration section:

- **Login User 1/Login User 2**—Enter up to two user names and passwords for SSH and Telnet access.
 - **Number of routers to query in parallel**—Indicates the number of routers that will be queried for new information at the same time using SSH/Telnet. Default is 50.
- 7 If you are using SNMP, you can configure the following global parameters to be referenced by entries in the Specific Router Access Configuration section:
- **SNMP v2 Community**—Enter the SNMP community for the router, if SNMP v2 is used.
 - **SNMP v3 Profile**—Choose the SNMP v3 profile, if SNMP v3 is used. See [Configuring SNMP v3 Profiles on page 80](#) for instructions on creating SNMP v3 profiles.
 - **Number of routers to query in parallel**—Indicates the number of routers that will be queried for new information at the same time using SNMP (default 50).
 - **Interval between queries to a router (seconds) within the polling cycle**—Enter the number of seconds between queries to individual routers within a particular polling cycle (default 1).
 - **Collect Static Routes**—Select the check box to collect static route information from the specified routers. Because static route collection can consume substantial router resources, we recommend that you collect static routes only from routers with small routing tables.
- 8 You must create one or more entries in the Specific Router Access Configuration section to specify prefixes that cover the addresses of all the routers from which information should be collected. The default 0.0.0.0/0 prefix entry will include all routers known from the IGP and BGP protocols that are recorded. For each of these entries, you can use the global settings or optionally configure settings that differ from the global settings. You can specify the following settings:
- **Routers (Prefix)**—Specify a prefix that contains the router ID or interface addresses of a set of routers to be queried. Only routers that are known through IGP or BGP recording will be queried, except that a /32 prefix will always be queried.

- **SNMP/SSH/Telnet**—Select check boxes if you want to configure SNMP, SSH, or Telnet settings for the specific routers. When you select one of these check boxes, the settings for that item are activated. The router is blacklisted if none of these is specified.
- **SNMP v2 Community**—Enter the SNMP community for the router, if SNMP v2 is used.
- **SNMP v3 Profile**—Choose the SNMP v3 profile, if SNMP v3 is used. See [Configuring SNMP v3 Profiles](#) on page 80 for instructions on creating SNMP v3 profiles.
- **SNMP Collect Static Routes**—Select the check box to collect static route information from the specified routers. Because static route collection can consume substantial router resources, we recommend that you collect static routes only from routers with small routing tables.
- **SSH/Telnet User Name**—Enter the user name for SSH and Telnet access.
- **SSH/Telnet Password**—Enter the password for SSH and Telnet access.

9 Click **Save**.

The Collector is now configured and ready to start collection when you start recording.

To view the Collector configuration, perform the following steps:

- 1 Open the client application as described in the “Viewers” chapter in the in the *HP Route Analytics Management Software User’s Guide*.
- 2 Choose **Tools > Find Router**.
- 3 Enter the router address of interest and click **OK**. The router is highlighted on the map and flashes briefly in yellow.
- 4 Right-click the router to open its information panel.
- 5 Open the Collector tab. You may need to click the right-facing arrow near the top of the panel to find the Collector tab.

The information includes prefixes, events, and interfaces. Only the up interfaces are listed.

Configuring SNMP v3 Profiles

Use the SNMP v3 Profiles page to define SNMP v3 profiles for the Collector. When you define a profile, it becomes available for selection on the Recorder Configuration page. See [Configuring the Route Recorder for the Collector](#) on page 73.

To configure an SNMPv3 profile, perform the following steps:

- 1 Choose **Administration > SNMP v3 Profiles**.
- 2 Choose one of the following options:
 - To create a new profile, click **New**.
 - To edit an existing profile, select the profile and click **Edit**.

The SNMP v3 Profiles page opens ([Figure 25](#)).

SNMP v3 Profiles

Profile Name	<input type="text"/>
User Name	<input type="text"/>
Select maximum security level	<input type="radio"/> No authentication or privacy (noAuthNoPriv) <input type="radio"/> Authentication with no privacy (authNoPriv) <input checked="" type="radio"/> Authentication with privacy (authPriv) (recommended)
Authentication protocol	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication passphrase	<input type="text"/>
Privacy protocol	<input checked="" type="radio"/> DES <input type="radio"/> AES
Privacy passphrase	<input type="text"/>

Figure 25 SNMP v3 Profile Configuration

- 3 Enter or confirm the profile name. The name is used when you select a profile for the Collector.
- 4 Enter the name of the SNMP user.
- 5 Choose one of the following security options for the SNMP messages, and configure additional information as indicated:
 - **No authentication or privacy (noAuthNoPriv)**—Permits all SNMP v3 messages with no authentication or privacy protection.

- **Authentication with no privacy (authNoPriv)**—Requires authentication for SNMP v3 messages. If you select this option, choose the default MD5 or Secure Hash Algorithm (SHA) authentication protocol and enter an authentication passphrase.
- **Authentication with privacy (authPriv)**—Requires authentication for SNMP v3 messages and adds message encryption. If you select this option, configure the authentication options described in the previous bullet. Choose the default Data Encryption Standard (DES) or Advanced Encryption Standard (AES) privacy protocol and enter a privacy passphrase. This option is recommended for full protection.

6 Click **Save**.

Starting and Stopping the Route Recorder

To start recording routing topology data for any of the protocols you added in [Configuring the Route Recorder](#) on page 55, perform the following steps on the Recorder Configuration page of the master appliance:



(RAMS Traffic only) If a Flow Analyzer is running in the configuration, you must stop the Flow Analyzer before you can start recording. See [Deleting a Flow Analyzer](#) on page 97.

- 1 Choose **Recorder Configuration**.
- 2 In the configuration hierarchy tree, click the protocol instance where you'll start recording routing data, and select **View**.

If the protocol instance is not already recording, the **Start Recording** button is displayed on the Recorder Configuration page.

- 3 Click **Start Recording**.

When recording has begun, the **Stop Recording** button appears.

- 4 Restart the Flow Analyzer, if it is stopped. (RAMS Traffic only)

The Route Recorder will write routing data for the selected protocol to the database until you click **Stop Recording**.

Use the **Start All Recording** and **Stop All Recording** buttons to start and stop recording for the entire configuration tree.

Viewing and Modifying Route Recorder Settings

After the Route Recorder is started, as described in [Starting and Stopping the Route Recorder](#) on page 81, RAMS Traffic is ready to receive routing announcements from the peer routers.

You can check the status of the recorder using the Status table on the Recorder Configuration page.

To access the Status table, perform the following steps:

- 1 Choose **Recorder Configuration**.
- 2 In the configuration hierarchy tree, click the protocol instance, and select **View**.

Depending on the protocol instance, the following information is displayed:

- For non-BGP protocols, the table shows the status of the protocol adjacency, the time the last “hello” packet was received as part of the routing protocol, the time the last event was written to the database by the Route Recorder. The table also identifies the interface, AS, and neighbor AS.
- For BGP protocols, the table shows the peer status for the AS, including IP address of the peer, the BGP Id, the state of the peering, and how long that state has existed (“Since”).

From the Status table for each protocol instance, you can also change recorder settings, as described in the following sections.

Changing the Area ID Format of an OSPF Protocol Instance

For an OSPF instance, viewing the configuration also displays the Area ID Format selection. An OSPF Area ID can be displayed either as a single decimal number or in dotted decimal format. The format selection controls both the administration pages and the RAMS Traffic client, but you must restart the client for a change in the format to take effect. If you use VNC, you must also stop the VNC server and restart it to see the change.

To change the Area ID format, perform the following steps:

- 1 Choose **Recorder Configuration**.
- 2 In the configuration hierarchy tree, click the protocol instance, and select **View**.

- 3 From the Area ID Format drop-down list, choose **Decimal** or **Dotted Decimal**.
- 4 Click **Submit**.
- 5 Choose **Administration > VNC Configuration**.
- 6 On the VNC Configuration page, click **Stop**. This stops the VNC server and closes any active VNC sessions.
- 7 Click **Start** to restart the VNC server.
- 8 Restart any VNC client sessions.

Deleting an Existing Domain or Protocol Instance

To delete an existing administrative domain or any instance, perform the following steps:

- 1 Choose **Recorder Configuration**.
- 2 In the configuration hierarchy tree, click the protocol instance, and select **View**.
- 3 Click **Stop Recording**.
- 4 Click an existing instance from the tree structure on the left side of the screen.
A pop-up menu appears.
- 5 On the pop-up menu, click **Delete**.
- 6 Click **Yes** on the confirmation screen that opens.
This deletes the instance, but the database remains in RAMS Traffic as a historical record.

Removing an Interface from a Protocol Instance

To remove an interface from a protocol instance, perform the following steps:

- 1 Choose **Recorder Configuration**.
- 2 In the configuration hierarchy tree, click the protocol instance, and select **View**.
- 3 Click **Stop Recording**.

- 4 Choose an existing interface name. If the chosen interface is in the **Active** column, move it to the **Not Active** column.
- 5 If the interface is a tunnel that you want to delete, highlight the interface name and click **Configure**.
The Configure Interface section opens on the Recorder Configuration page.
- 6 Click **Delete**. A confirmation message page opens.
- 7 Click **Yes**. The tunnel is deleted and the Recorder Configuration status page returns.

Changing an OSPF Authentication Password

To change an OSPF authentication password, perform the following steps:

- 1 Choose **Recorder Configuration**.
- 2 In the configuration hierarchy tree, click the protocol instance, and select **View**.
- 3 Click **Stop Recording**.
- 4 Choose an existing interface name. If the chosen interface is in the **Active** column, move it to the **Not Active** column.
- 5 Select the interface name, and then click **Configure**.
- 6 Highlight the password and enter another password.
- 7 Click **Update**. This changes the password.

Deleting an OSPF Authentication Password

To delete an OSPF authentication password, perform the following steps:

- 1 Choose **Recorder Configuration**.
- 2 In the configuration hierarchy tree, click the protocol instance, and select **View**.
- 3 Click **Stop Recording**.
- 4 Choose the existing interface name with the affected password. If the interface is Active, it is first necessary to move it to the **Not Active** column.
- 5 Select the interface name and then click **Configure**.

- 6 Deselect **Enable**.
- 7 Delete the password.
- 8 Click **Update**. This deletes the OSPF authentication password.

Configuring the Flow Collector



This section applies to RAMS Traffic only. The Flow Collector is supported only on appliance models with two disk volumes (3510 FR and 4000 FR).

A Flow Collector receives and stores NetFlow traffic data from various routers on the network to the database, and creates reports. The Flow Analyzer aggregates the reports and is responsible for issuing alerts. See [Configuring MPLS-Aware NetFlow v9 on Cisco Routers](#) on page 99 for information on configuring NetFlow for Cisco routers.

In releases prior to 8.0, it was possible to double-count traffic flows that passed through more than one exporting router; therefore, it was important for users to select the set of exporting routers such that traffic flows would not pass through more than one exporting router. Now a deduplication process stops the projection of a traffic flow when it reaches a second exporter so it won't be counted more than once. This allows greater flexibility when setting up the appliance.

- Enterprises can increase coverage by measuring traffic flows at all data centers and peering points where significant traffic originates.
- VPN service providers can enable traffic collection from combination P/PE routers in addition to the downstream P routers. In doing so, the service provider must restrict the set of exporting interfaces on the P/PE router to those that are connected to upstream PE routers (the interfaces used in the router's P role). This restriction applies because at the ingress to a PE router, the traffic is not yet encapsulated in the VPN, and information is not yet available to specify the VPN. Therefore, such traffic cannot be shown as VPN traffic within the provider's network.

In MPLS VPN deployments, you must establish Label Distribution Protocol (LDP) peering sessions to exporting routers to learn of the MPLS labels assigned to ingress traffic for the routers, except in the cases where this information is already carried in the NetFlow records. See [Configuring MPLS VPN-Aware LDP for Cisco Routers](#) on page 98.

LDP peering is established in two phases. First, a hello adjacency (UDP) is established, and then a session is established to work over TCP.



You must configure the Route Recorder as described in [Configuring the Route Recorder](#) on page 55 before you begin configuration of the Flow Collectors.

To configure a Flow Collector, perform the following steps:

- 1 Choose **Recorder Configuration** on the master appliance.
- 2 Click the top-level domain name you added in [Creating a Configuration Hierarchy](#) on page 52 (for example, CorpNet) and select **Add**.

A list of options appears on the pop-up menu.

- 3 Click **Traffic** near the bottom of the list.

A status message indicates that a traffic label was added to the configuration hierarchy. The traffic label is used to organize one or more Flow Collectors, which you will add in Steps 4-18.

- 4 Click the **Traffic** label in the configuration hierarchy and move the cursor to **Add** Flow Collector.

A choice of IP addresses appears. Each IP address corresponds to a RAMS Traffic client licensed to function as a Flow Collector.

- 5 Click an IP address.

The Recorder Configuration page appears as shown in [Figure 26](#). The domain is pre-populated with the name of the administrative domain.

Recorder Configuration

Flow Collector Configuration

Domain: HPOspfTest
 Flow Collector Id: FR
 UDP Port:
 Sampling:
 Prefix Source*:

Routers sending NetFlow data

Exporter IP Address	Router IP Address**	Sampling Rate***	Physical Interface	Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Slot 0/Port 1"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Slot 0/Port 1"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Slot 0/Port 1"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Slot 0/Port 1"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Slot 0/Port 1"/>	<input type="checkbox"/>

** Route Recorder or Report Server
 *** Corresponding router IP address if different from exporter
 **** Sampling rate of individual exporter if different from global setting
 *****Check to show/hide

Flow Collector Status

Status	Last Status Update	Last NetFlow Record
Down	Mon Mar 17 14:48:21 2008	

Recorder event times are not available

Replication Status

IP Address	Databases	Status

Figure 26 Configuring a Flow Collector

- 6 In the Flow Collector Id text box, enter a label for the Flow Collector.

The appliance uses this label to identify the Flow Collector in the configuration hierarchy tree, and as the name of the Flow Collector database file. This text box is editable until a valid ID is entered. After the ID is validated, the text box is no longer editable, and you cannot change the Flow Collector ID.

- 7 In the UDP Port text box, verify the UDP port number. The number in this text box must match the port number to which the routers will send NetFlow data. The text box is pre-populated with the port from which flow exports are received.
- 8 In the Sampling Rate text box, enter the NetFlow sampling rate configured on the routers, if any. All routers must use the same sampling rate. If no sampling is done on the routers, enter 1.
- 9 The Prefix Source field specifies the appliance that will provide the list of prefixes learned from all routing protocols that are being recorded.

The prefix source is the Route Recorder or explorer in systems with only one appliance recording routes, or the Modeling Engine with Report Server enabled when there are multiple units recording routes.
- 10 In the Exporter IP text box, enter the IP address of the router from which the Flow Collector will accept NetFlow data exports. The number of routers specified in this section is not limited.
- 11 In the Router IP text box, enter the IP address of the corresponding router if the exporter is not known to the Route Recorder.
- 12 In the Sampling Rate text box, enter the sampling rate that is configured on the routers, if the sampling rate from the exporter is different from the sampling rate shown in Step 8.
- 13 Click the LDP Enabled text box.



LDP should not be enabled for IPv4 deployments.

- 14 Enter a password for the LDP MD5 Password for additional security for the exporting router.
- 15 Select the physical interface from the drop-down menu.
- 16 Click **Delete** box remove the configuration information for the row.
- 17 Repeat steps 10 through 15 to choose additional routers.



If more than five routers need to be configured you must enter the first five rows of addresses first, and click the **Save** button. After clicking **Save**, five more rows will appear in the table.

- 18 Review the information in the Flow Collector Configuration portion of the window, and click **Start Recording**. This button also saves the configuration.

The Flow Collector appears in the domain hierarchy.

In the Flow Collector Status portion of the Flow Collector Configuration window, you can view recording status for the Flow Collectors. The columns in this section of this window are as follows:

- **Status**—Displays whether recording is under way.
- **Last Status Update**—Displays the most recently requested update for the recorder. Click **Show Last Event Times** to view the last report times for the routing and traffic databases from the point of view of the FR, or click **Hide Last Event Times** to hide that information.
- **Last NetFlow Record**—Displays detailed statistics for the NetFlow records received.

The bottom of the Flow Collector Configuration page displays the status of LDP peering with each neighboring exporters that the recorder is configured to communicate with. Detailed status is also available to show the number of NetFlow packets received by the Flow Collector, the number of NetFlow packets lost, if any, and the number of traffic flows known to the Flow Collector.

Starting and Stopping the Flow Collectors



This section applies to RAMS Traffic only.

After configuring the Flow Collectors as described in the previous section, you can start or stop recording NetFlow data using the Recorder Configuration page of the master appliance.

To start recording traffic flow data, perform the following steps:

- 1 If a Flow Analyzer is running in the configuration, you must stop the Flow Analyzer before you can start recording. To do so, choose **Recorder Configuration**, select the Flow Analyzer, and click **View**. Click **Stop** on the Recorder Configuration page.
- 2 In the configuration hierarchy tree, click the Flow Collector instance where you will start recording traffic data.

A pop-up menu appears.

3 Click **View**.

If the Flow Collector is not already recording, the **Start Recording** button is displayed on the Recorder Configuration page.

4 Click **Start Recording**.

When recording has begun, the **Stop Recording** button appears.

5 Restart the Flow Analyzer, if you stopped it in Step 1.

The Flow Collector will write traffic data to the database until you click **Stop Recording**. Changes to Flow Collector configuration are not allowed after recording has started.

Viewing Flow Collector Settings



This section applies to RAMS Traffic only.

You can view settings for a configured Flow Collector using the Recorder Configuration page on the master appliance.

To view Flow Collector settings, perform the following steps:

1 On the Recorder Configuration page, click the Flow Collector to view in the tree structure on the left side of the page.

A pop-up menu appears.

2 Click **View**.

A Status table appears at the bottom of the Recorder Configuration page. If this table is not empty, then a database is being created for RAMS Traffic. If the table is empty, verify that the connection to the router or the tunnel is properly configured.

The Flow Collector Status table displays each Flow Collector ID and gives its status (Recording, Not Recording, or Down). The table also shows the time the status was last updated, and when the last NetFlow record was received.

You can view more detailed status messages about the traffic database by clicking **Show Detailed Status** (Table 1). The Detailed Status table displays information such as the number of NetFlow packets received by the Flow Collector, the number of NetFlow packets lost, if any, and the number of traffic flows known to the Flow Collector.

Table 1 Detailed Status Table

Time elapsed since last start in seconds	Amount of time in seconds since the last Flow Collector start.
NetFlow packets	Number of NetFlow packets (all export formats) received from all exporting routers. This count is cumulative since the most recent time the recorder was started (or restarted). Note: This count should be equal to the sum of NetFlow v1/v5/v8 packets and NetFlow v9 packets.
NetFlow v1/v5/v8 packets	Number of NetFlow v1/v5/v8 packets received from all exporting routers. This count is cumulative since the most recent time the recorder was started (or restarted).
NetFlow v9 packets	Number of NetFlow v9 packets received from all exporting routers. This count is cumulative since the most recent time the recorder was started (or restarted).
Netflow packets from invalid exporters	Number of packets that arrived at the recorder but were dropped because they came from an invalid exporter. If this number is non-zero, it could indicate misconfiguration of the Flow Collector (or the router), or a malicious outsider attempting to flood the Flow Collector.
NetFlow packets with invalid timestamps	Number of NetFlow packets received with invalid timestamps Flow Collectors reject NetFlow packets with timestamps more than sixty seconds in the past or more than sixty seconds in the future.
NetFlow records	Number of NetFlow records received (all protocols) from all exporting routers. This count is cumulative since the most recent time the recorder was started (or restarted).

Table 1 Detailed Status Table (cont'd)

NetFlow IPv4 records	Number of NetFlow records received describing native IPv4 flows from all exporting routers. This count is cumulative since the most recent time the recorder was started (or restarted).
NetFlow VPN records	Number of NetFlow records received describing VPN flows from all exporting routers. This count is cumulative since the most recent time the recorder was started (or restarted).
NetFlow records lost	Number of NetFlow records estimated to be lost since the recorder started (or was restarted). This is estimated by examining the sequence numbers in the NetFlow packets. When recording a new traffic database, a burst of loss at the start of recording is normal (a number less than .01% of the total NetFlow records). Low traffic deployments may see zero lost packets.
NetFlow records with invalid timestamps	Number of NetFlow records received with invalid timestamps. Flow Collectors reject NetFlow records with timestamps more than one hour in the past or more than sixty seconds in the future.
Current/Mean/Maximum five-minute count of NetFlow Records	Current/Mean/Maximum number of NetFlow records received from all exporting routers in the past five minutes since the last Flow Collector start.
NetFlow records sampled	Number of records sampled since the recorder started. For low traffic level deployments, this number should be the same as the number of NetFlow records received. Number of records processed through algorithms since the recorder started. For low traffic level deployments, this number should be the same as the number of NetFlow records. For high traffic environments, sampling is done at the level of NetFlow records and this number counts only the records that were selected by the sampling algorithm. (Currently, a cap of 500,000 records per five minutes).

Table 1 Detailed Status Table (cont'd)

NetFlow records successfully processed	Number of Netflow records processes since the last Flow Collector start to generate traffic statistics. In the absence of errors in NetFlow records, this number should be the same as the number of NetFlow records received.
NetFlow records dropped outside aggregation window	Number of Netflow records dropped due to late export (greater than 20 minutes) by the exporting router.
NetFlow records dropped due to source/destination not in prefix table	Number of Netflow records dropped due to source or destination address of the reported flow not in the set of routing prefixes heard by the Route Recorders.
NetFlow records dropped due to IPv4 source/destination not in prefix table	Number of NetFlow records describing native IPv4 flows dropped due to source destination address of the reported flow not in the set of routing prefixes heard by the Route Recorders.
NetFlow records dropped due to VPN source/destination not in prefix table	Number of NetFlow records describing VPN flows dropped due to source destination address of the reported flow not in the set of routing prefixes heard by the Route Recorders.
NetFlow records dropped with multicast information	Number of Netflow records with multicast information that are received by the Recorder. Multicast Netflow records are currently not processed by the Flow Collector.

Table 1 Detailed Status Table (cont'd)

Known flows	Instantaneous measure of the number of flows (each flow represents a source or destination prefix/exporter combination) that the Flow Collector is tracking. This influences the amount of memory used by the system.
Prefixes	Instantaneous measure of the number of prefixes known to the Flow Collector. It uses these prefixes for aggregation purposes. The appliance uses these prefixes when aggregating data. This number should be the count of prefixes known to all of the IGP and BGP areas.
Exporters	Instantaneous measure of the number of exporters on a router (An exporter refers to an interface on a router). For example, in a deployment with two routers each exporting from ten interfaces, this value would be 20.

To delete a Flow Collector from the configuration hierarchy, perform the following steps:

- 1 Stop the Flow Collector, as described in [Starting and Stopping the Flow Collectors](#) on page 89.
- 2 On the Recorder Configuration page of the master appliance, click the Flow Collector to delete in the tree.
- 3 In the pop-up menu that opens, click **Delete**. Click **Yes** to confirm.

This deletes the instance, but the database remains in the appliance as a historical record.

Configuring Flow Analyzer Recording Status



This section applies to RAMS Traffic only.

A Flow Analyzer processes traffic data received from the Flow Collectors to generate aggregate traffic reports and alerts.

To configure the recording status of the Flow Analyzer, perform the following steps:

- 1 On the Recorder Configuration page of the master appliance, click the top-level domain name you added in [Creating a Configuration Hierarchy](#) on page 52 (for example, CorpNet).

- 2 Move the cursor to **Add**.

A list of options appears on the pop-up menu.

- 3 Click **Traffic Reports**.

A status message appears in the browser window indicating that a traffic label was added to the configuration hierarchy. The traffic label is used to organize one or more Flow Analyzers, which you will add in the following steps.

- 4 Click the **Traffic Reports** label in the configuration hierarchy and move the cursor to **Add Flow Analyzer**.

The Flow Analyzer's IP address appears.

- 5 Click an IP address.

The Flow Analyzer Status window opens.

The following buttons are found at the top of this window:

- **Stop**—Stops all report daemons for the Flow Analyzer.
- **Refresh Status**—Refreshes the information found on-screen.
- **Restart Replication**—Restarts the Flow Collector to collect traffic data, write reports to correlate routing and traffic information to the Flow Analyzer.

Starting and Stopping the Flow Analyzer



This section applies to RAMS Traffic only.

To start and stop the Flow Analyzer, perform the following steps:

- 1 On the Recorder Configuration page of the master appliance, click the Flow Analyzer instance.
A pop-up menu appears.
- 2 Click **View**.
If the Flow Analyzer has not already been started, the **Start** button is displayed on the Recorder Configuration page.
- 3 Click **Start**.
When the Flow Analyzer is running, the **Stop** button appears.
- 4 Click **Stop** to stop the Flow Analyzer.

Viewing Status of the Flow Analyzer



This section applies to RAMS Traffic only.

You can view the recording status of the Flow Analyzer on the Recorder Configuration page. You can also stop recording and restart replication.



Configuring the Flow Analyzer occurs automatically when you configure the Flow Collector.

In the Flow Analyzer Status portion of the window, a row is displayed for each of the following time intervals:

- 5-Min Report
- Hourly Report
- Daily Report

- Weekly Report
- Monthly Report

The following columns of information are displayed for each interval:

- **Report Type**—Displays the following schedule of reports:
- **Last Report Time**—Displays the date and time the report was last written.
- **Status**—Displays whether the Flow Analyzer is Up or Down.

In the **Database** portion of the window, the names of the Flow Collector database displays in the left portion of the table. The **Status** column displays whether the database is running on or offline.

The bottom of the Flow Analyzer Status window displays the Replication Status table. The following columns are displayed:

- **IP Address**—Displays the IP address of the Flow Collector.
- **Databases**—Displays the Flow Collector database name.
- **Status**—Displays whether the recorder is running or not. If it isn't, click **Restart Replication** to restart replication.

Deleting a Flow Analyzer



This section applies to RAMS Traffic only.

To delete a Flow Analyzer from the configuration, perform the following steps:

- 1 Stop the Flow Analyzer as described in [Starting and Stopping the Flow Analyzer](#) on page 96
- 2 On the Recorder Configuration page of the master appliance, click the Flow Analyzer to delete in the tree.
- 3 In the pop-up menu that opens, click **Delete**. Click **Yes** to confirm.

This deletes the instance, but the database remains in RAMS Traffic as a historical record.

Additional Configuration Tasks

Configuring MPLS VPN-Aware LDP for Cisco Routers

LDP is a protocol in which two Label Switch Routers (LSRs) exchange label mapping information. LDP is used to build and maintain LSR databases that are then used to forward traffic through MPLS environments. LDP relies on the underlying routing information provided by an IGP in order to forward label packets. LDP is used only for signalling best-effort LSPs.



The configuration procedures that follow are intended for P routers. You also must have MPLS VPN configured on your network before working through the sections that follow.

Targeted LDP Configuration for Cisco Routers

To learn what labels your router is using, you must set up a targeted LDP session. This session forces the router to send you all the labels that it is using throughout the MPLS VPN.



Refer to the Cisco router documentation for detailed router configuration instructions.

To configure targeted LDP on a Cisco router, perform the following steps:

- 1 Open a session with the router.
- 2 Enter the following command in global configuration mode:

```
mpls ldp neighbor <flow-collector-ip-address> targeted
```

The `mpls ldp neighbor <flow-collector-ip-address> targeted` command sets up a targeted LDP neighbor peering with the Flow Collector, which then receives the NetFlow v9 flow records.

To set the Router ID, perform the following steps:

- 1 Open a session with the router.
- 2 Enter the following command in global configuration mode:

```
mpls ldp router-id interface [ ]force
```

The `mpls ldp router-id interface []force` command specifies a preferred interface for determining the LDP router's ID.



This command may be necessary to ensure that there is a matching router-id for the router in the IGP and/or BGP routing space that is being recorded by the Route Recorders.

Configuring MPLS-Aware NetFlow v9 on Cisco Routers

NetFlow v9 provides network administrators access to information about IP flows within their data networks. This data can be used for network management and planning, enterprise accounting, and data warehousing. By analyzing flow data, a picture of traffic flow and volume can be built.



MPLS-aware NetFlow v9 is available only in certain IOS versions. Verify that the version of IOS you are running supports MPLS-aware Netflow. Refer to the Cisco router documentation for detailed router configuration instructions.

Configuring MPLS-Aware NetFlow v9 for Cisco Routers

To configure MPLS-aware Netflow v9 on Cisco routers, enter the following commands (in EXEC mode):

- 1 Open a session with the router.
- 2 Enter the following commands in EXEC mode:

```
ip flow-export version 9
```

The `ip flow-export version 9` command enables v9 data export for the main cache.

```
ip flow-cache mpls label-positions 1 2
```

The `ip flow-cache mpls label-positions 1 2` command enables MPLS-aware NetFlow.

To enable NetFlow v9 on each Cisco interface, perform the following steps:

- 1 Open a session with the router.
- 2 Enter the following command in EXEC mode:

```
interface / interface-type interface number
```

The `interface / interface-type interface number` command configures an interface (or subinterface) type, and enters Interface Configuration mode.

- 3 Enter the following command in Interface or Subinterface configuration mode:

```
ip flow ingress
```

The `ip flow ingress` command configures NetFlow on an interface or subinterface.



`ip flow ingress` was introduced in IOS release 12.3. If you are using an earlier IOS version, use the command `ip route cache flow` instead.

To view the status of NetFlow exports, perform the following steps:

- 1 Open a session with the router.
- 2 Enter the following commands in EXEC mode:

```
show ip flow export
```

The `show ip flow export` command displays information about the software-switched flows for the data export, including the main cache and all other enabled caches.

```
show ip cache flow
```

The `show ip cache flow` command displays a summary of the NetFlow cache flow entries.

```
show ip cache verbose
```

The `show ip cache verbose` command displays additional information for the NetFlow cache entries.

Configuring GRE Tunnels

This section introduces GRE tunnels and describes how they are configured. GRE is used to listen to routing traffic on a network other than the local network. This section also describes how to configure a loopback interface for Cisco routers. Use a loopback interface to monitor two areas that are linked to a single router.

To listen to routing traffic on a network other than the local network, remotely connect that network to a secondary network interface on the appliance, or use a GRE tunnel to form the adjacency.

The GRE tunnel follows standard routing across the network to the destination. Only the source router and appliance need to be configured to bring up the tunnel.

In general, a small address block is assigned to the tunnel (usually a /30 address block with four addresses in it). Of these four addresses, the first and last address are the network and broadcast addresses, respectively. The second address is assigned to the router end of the tunnel, and the third to the

appliance end of the tunnel. For example, assume that the address block 10.0.1.0/30 is assigned to the GRE tunnel. The four addresses are allocated as follows:

- 10.0.1.0/30 is the network address.
- 10.0.1.1/30 is the router end of the tunnel.
- 10.0.1.2/30 is the appliance end of the tunnel.
- 10.0.1.3/30 is the broadcast address.

The tunnel extends from the router to the appliance, and you must configure the tunnel on the router and on the appliance.

When you configure the router, keep the following points in mind:

- From the router perspective, the tunnel source is the IP address of either a loopback or physical address on that router.
- The tunnel destination is the IP address of the physical interface on the appliance.
- The IP address of the tunnel has to be assigned to the monitored protocol on the router. For example, there must be a network statement in OSPF for the network IP address of the tunnel.

When you configure the appliance, keep the following points in mind:

- The tunnel source is the IP address for the physical interface on the appliance.
- The tunnel destination is the IP address of the physical interface of the remote router.



The default Maximum Transmission Unit (MTU) size is 1476 for OSPF and EIGRP and 1514 for IS-IS.

To create a GRE tunnel on Cisco destination router, the information in [Table 2](#) must be configured for the router. (This description applies to Cisco routers and may vary for others. Refer to the router documentation for detailed router configuration instructions.)

For a GRE tunnel that will carry an EIGRP peering, the default 7 kb/s bandwidth setting of the tunnel must be increased to a value that reflects the bandwidth available on the physical path. This change is required because

EIGRP protocol packets are paced to consume no more than half of the available bandwidth, and 3.5 kb/s may not be sufficient to deliver Update packets for the full EIGRP routing table in less time than the 180-second stuck-in-active (SIA) timeout. As a consequence, the peering can flap indefinitely if any routes are active at the time the peering is initiated. A bandwidth setting of 1000 kb/s, as shown in [Table 2](#) , is generally sufficient, but this may be increased if the bandwidth of the physical path is higher. Setting the bandwidth for protocols other than EIGRP is fine, too, although not required.

Table 2 Required Tunnel Information on Remote Router

Item	Example of Command
Tunnel Interface	<code>int tunnel <n></code>
Tunnel IP	<code>ip address 10.0.1.1 netmask 255.255.255.252</code>
Tunnel Source	<code>tunnel source loopback 0</code>
Tunnel Destination	<code>tunnel dest <RAMS Traffic IP address></code>
Bandwidth	<code>bandwidth 1000</code>
Network Statement	The routing protocol configuration must include a network statement with the assigned IP address of the tunnel and the inverse of the network mask. For example: <code>router ospf <n> network 10.0.1.0 0.0.0.3 area <area to be monitored></code>

To configure a GRE tunnel, perform the following steps:

- 1 On the Recorder Configuration page, select a protocol instance name on the tree.
- 2 From the pop-up menu, click **View** to see the protocol configuration.
- 3 Click **New Tunnel** on the Recorder Configuration page.

The Configure Interface section opens, as shown in [Figure 27](#).

Configure Interface		
Interface	OSPF Authentication	GRE Tunnel
	<input type="checkbox"/> Enable Password: <input type="text"/> MD5 Key-Id: <input type="text"/>	Remote IP Address: (Tunnel Destination) <input type="text" value="192.123.4.5"/> Local IP Address: <input type="text" value="10.0.1.2"/> Netmask: <input type="text" value="/"/> Interface: <input type="text" value="Slot 0/Port 1"/>
Tunnel2OSPF		

Figure 27 Configuring a GRE Tunnel Interface

- 4 In the Interface text box, enter a descriptive name for the tunnel.
- 5 If you are configuring a tunnel for an OSPF instance, and OSPF authentication is configured for the area to be monitored, then you must configure authentication by selecting the **Enable** check box.
 - For simple authentication, enter a password in the Password text box that matches the password in the remote area.
 - For MD5 authentication, enter a password and MD5 Key-ID that match the password and key used in the remote area.

If an MD5 key is entered, it is assumed that there is MD5 authentication for this OSPF area. If no MD5 key is entered, then simple authentication is presumed.

- 6 In the Remote IP Address text box, enter the IP Address of the physical interface or loopback on the remote router.

This IP address should be the same as the **Tunnel Source** address you configured on the router.
- 7 In the Local IP address text box, enter the IP Address assigned to the tunnel on RAMS Traffic.

Using the example addresses listed above, this would be 10.0.1.2
- 8 In the Netmask text box, enter the network mask of the **Tunnel IP** address that you configured on the router.

The format for the Netmask field can be one of the following:

- CIDR notation (/x)
- Netmask notation (x.x.x.x)

Here is an example based on the addresses used in [Figure 27](#):

- **Remote IP Address:** 192.123.4.5 (IP address of the physical interface or loopback on the router that is the tunnel destination.)
- **Local IP Address:** 10.0.1.2 (IP address assigned to the tunnel on RAMS Traffic.)
- **Netmask:** /30 (mask length for the Tunnel IP address of the tunnel.)

9 Click **Update**.

The protocol instance configuration box returns on the Recorder Configuration page with the new tunnel name appearing in the Not Active interface list.

10 To begin recording data for the tunnel, move the tunnel name into the **Active** column.

11 Click **Update**.

Configuring a Loopback Interface for Cisco Routers

To monitor two areas that are linked to a single router, you must configure a loopback interface on the Cisco router. If you do not do this, only one adjacency will be formed with the remote router. Both areas will come up initially with full adjacency, but the first one to come up will fail soon after. Use the command line interface to the router to configure the loopback interface.

To configure a loopback, perform the following steps:

- 1 Open a session with the router.
- 2 Enter the following commands:

```
int loopback <n>
ip address <ip address> <netmask>
int tunnel <n>
ip address <tunnel ip address> <netmask>
tunnel source <loopback ip address>
tunnel destination <RAMS Traffic ip address>
router ospf <process number>
network <loopback ip address> <inverse netmask> area <a>
network <tunnel ip address> <inverse netmask> area <a>
```

Enabling Technical Support Access

To enable or disable technical support options, choose **Administration > Support Access**. The Technical Support Configuration page displays as shown in [Figure 29](#).



In a multi-appliance configuration, access the Technical Support Configuration page of each system individually to enable tech support access.

Technical Support Configuration

Technical support access is enabled.

Technical support callback is disabled.

Enabling technical support callback enables technical support access.
Disabling technical support access disables technical support callback.

Figure 28 Technical Support Configuration Page

The Technical Support Configuration page has two buttons that control access by technical support personnel. The first, **Technical support access**, is enabled by default. It allows HP technical support personnel to connect using an SSH connection and a specially encrypted key. Access is restricted to HP technical support personnel and is initiated only after obtaining your permission as part of your requested assistance. To disable technical support access, click **Disable Access**.



Disabling technical support access makes it impossible for HP to reset the password or perform diagnostic services. In this case, you must return the appliance to receive support.

If the appliance is connected to a network where direct remote access is not possible due to firewall restrictions, enable the Technical support callback feature by clicking **Enable Callback**. This initiates an SSH connection from the appliance to a dedicated and tightly secured server at HP. Firewall rules

usually allow such outbound SSH connections. The connection is configured in such a way that new login sessions can be tunneled from the server at HP through the SSH connection back to the appliance. As in the case of direct remote access, these login sessions use SSH and require a specially encrypted key.



When you enable technical support access, technical support callback is also enabled. When you disable technical support access, technical support callback is disabled as well.

Technical Support Configuration

Technical support access is enabled.

Technical support callback is disabled.

Enabling technical support callback enables technical support access.
Disabling technical support access disables technical support callback.

Figure 29 Technical Support Configuration Page

3 Administration

Administration includes ongoing maintenance tasks such as managing users, updating software, and maintaining databases. You perform these tasks per client, rather than using the Administration pages of the master appliance. To access the Administration pages, click **Administration** at the top of the appliance Home page.

Before performing the administrative tasks described in this chapter, see [Chapter 2, “Configuration and Management”](#) for information about how to access the Administration pages, log in, and configure components.

Chapter contents:

- [Creating and Authenticating User Accounts](#) on page 110
- [Creating Traffic Groups](#) on page 117
- [Creating CoS Definitions](#) on page 122
- [Configuring the VNC Server](#) on page 125
- [Managing Databases](#) on page 129
- [Backing Up and Restoring Data](#) on page 134
- [Replacing Client and Master Appliances](#) on page 145
- [Choosing a Data Source](#) on page 150
- [Archiving Data](#) on page 153
- [Updating Software](#) on page 159
- [Using the Reports Scheduler](#) on page 165
- [Scheduling Top N Reports](#) on page 169
- [Configuring the FTP Server](#) on page 171
- [Configuring Flow Fanout](#) on page 172
- [Viewing and Exporting Log Pages](#) on page 174

- [Uploading Layout Backgrounds](#) on page 175
- [Using Diagnostic Functions](#) on page 176
- [Shutting Down](#) on page 178



The links and buttons on the Administration pages might differ from those shown in the examples in this guide, depending on the functions for which your system is licensed. If your system is not licensed for a particular function, the links or buttons related to that function do not appear on the Administration pages.

Creating and Authenticating User Accounts

You can configure authentication to be performed locally or through a remote TACACS+ or RADIUS server. In multi-unit deployments, you have the option of using the master unit as the authentication server for the client units (using TACACS+).

Local authentication is always used as a fallback in the event that authentication through a remote server (Master or external server) fails. For this reason, it is important to always have at least one administrator account configured on each appliance. It is also important to change the passwords on the factory installed accounts to more secure values because these local accounts will be used for authentication if access to the remote server fails.

User Privileges

Every user is assigned one of the following privileges:

- Administrators have full access privileges and can perform the following functions:
 - Configure other user accounts.
 - Load, modify, or delete any layout, as described in “The Routing Topology Map” chapter of the *HP Route Analytics Management Software User’s Guide*.

- Modify or delete groups of network elements (routers, links, prefixes) that are owned by others, as described in “The Routing Topology Map” chapter in the *HP Route Analytics Management Software User’s Guide*.
- Configure alerts, as described in the “Alerts” chapter of the *HP Route Analytics Management Software User’s Guide*.
- Operators can access the Application and the Report pages, but do not have any administration privileges. Operators can load any layout, but if they save a layout that they do not own, a new copy of the layout is created with the same name, but with the new owner. Operators can also save a layout under a new layout name.
- Guests are view-only users. They have the same access as operators, but cannot save or delete routing topology map layouts.

When administrators, operators, and guests use SSH for access, the X Window System or VNC client displays the graphical interface.

- CLI Access users use SSH to connect to the TTY user interface rather than the graphical user interface. Once connected, the CLI access user can run diagnostic commands, reboot the appliance, or shut it down. For more information about using diagnostic and other command-line functions, see the *RAMS Appliance Setup Guide*. [Boot Sequence](#) on page 10.

TACACS+ and RADIUS Parameters

You can use existing TACACS+ or RADIUS server that is configured for user accounts; however, changes to the account parameters are required to authorize the users for access to the appliance at an appropriate privilege level.

TACACS+

To configure a TACACS+ server for use with the appliance, you must define a set of authorized users, which are expressed as service/protocol pairs. There are four classes of users:

- Administrator (rex-admin)
- Operator (rex-op)
- Guest (rex-guest)
- CLI (rex-cli).

Each user should be authorized for service “ppp,” with the protocol as one of the above strings (for example, rex-admin). For example, a guest user would have service=ppp protocol=rex-guest. The “ppp” is a convention used by the appliance to identify users.

A user should not be in more than one of the four user classes. If the account needs FTP or secure File Transfer Protocol (SFTP) access, it should be assigned separately (for example, service=ppp protocol=rex-ftp).

The following example shows a tac_plus.conf configuration file. The example creates an administrative user “admin” with password “mypassword.” It also creates an Operator “op,” with FTP access; and a CLI account called “cliuser.” The latter two accounts store their passwords encrypted.

```
key = SomethingSecret
user = admin {
    pap = cleartext mypassword
    service = ppp protocol = rex-admin {}
}
user = op {
    pap = des sOzm4t1mClWDg
    service = ppp protocol = rex-op {}
    service = ppp protocol = rex-ftp {}
}
user = cliuser {
    pap = des 6bjKZUV4xsNRQ
    service = ppp protocol = rex-cli {}
}
```

RADIUS

For RADIUS, configure each of the four user classes as a NAS Identifier and then list the user names associated with each identifier. In FreeRADIUS, the configuration is done by populating a “huntgroups” file, as in the following example:

```
rex-op          Nas-Identifier == rex-op
                User-Name == op

rex-admin       Nas-Identifier == rex-admin
                User-Name == admin
```



```

rex-ftp      Nas-Identifier == rex-ftp
             User-Name == admin,
             User-Name == op,
             User-Name == cliuser

rex-guest    Nas-Identifier == rex-guest

rex-cli      Nas-Identifier == rex-cli
             User-Name == cliuser

```

It is important to specify all of the groups, even if they are empty. Otherwise the system will grant those group privileges to any user. User names in FreeRADIUS are defined in a “users” file, as in the following example:

```

admin      Cleartext-Password := "mypassword"
op         Cleartext-Password := "operator"
cliuser    Cleartext-Password := "cliuser"

```

User Administration Page

Open the User Administration page to select an authentication server, create and update user accounts for local authentication and log-in attributes for the users you support.

To open the page, choose **Administration > Users**. The top portion of the User Administration page displays the following authentication information:

- **TACACS Server**—TACACS+ is a security system that can provide centralized validation of users.
- **RADIUS Server**—RADIUS is a method that was originally designed for authenticating modem and ISDN connections and for tracking connection time, but subsequently extended for general authentication service.
- **Local Authentication**—This is the default choice for user authentication. The system contains a TACACS+ server that references the database of users configured through the User Administration page. Always configure local authentication on the master appliance in a multi-appliance deployment.
- **Authenticate via Master**—The client will use the master as its TACACS+ authentication server.

Selecting an Authentication Method

To select the authentication method for all users to access the system, perform the following steps:

- 1 Choose **Administration > Users** to open the User Administration page (in Figure 30).

The screenshot shows the 'User Administration' page with a section titled 'Authentication Type'. It contains several radio button options and text input fields. The 'Local Authentication' option is selected. There is also a checkbox for 'Show Shared Secret' and an 'Update' button.

User Administration

Authentication Type

TACACS+ Server
TACACS Shared Secret:

RADIUS Server
RADIUS Shared Secret:

Local Authentication
Local Shared Secret:

Authenticate via Master
Master's Shared Secret:

Show Shared Secret

Figure 30 Authentication Method Section of User Administration Page

- 2 Select **TACACS+ Server**, **RADIUS Server**, or **Local Authentication** as the authentication method, and enter the shared secret in the Shared Secret text box for the option you selected.

If you have a master/client configuration and the master appliance is set for local authentication, then when you bring up a client, **Authenticate via Master** is selected and the shared secret is added automatically. If you reconfiguring a client to work with a master, you will need to enter the shared secret for the master.

- 3 Select the **Show Shared Secret** check box if you want the shared secret to be displayed.
- 4 Click **Update** to save the information.



After changing the authentication method, immediately test access using the new method using another browser window. If that test fails, you can switch back the authentication method using the original browser window that is still logged in.

Creating New User Accounts

User accounts that are configured on the User Administration page are always authenticated using local authentication. Always maintain at least one administrator user account, even if TACACS+ or RADIUS is selected as the general authentication method. Doing so assures that you can access the system even if the TACACS+ or RADIUS server is unavailable. It is also important to change the passwords on the factory installed “admin” and “op” accounts, or to delete them, since the default passwords may be easily guessed.

To create a new user account, perform the following steps:

- 1 Choose **Administration > Users**.
- 2 Enter the user name in the New User field ([Figure 31](#)).

Create Users

New User:

Privilege:

Password:

Confirm Password:

Enable FTP

Figure 31 Create Users Section of User Administration Window

- 3 Select the privilege level of the user from the **Privilege** drop-down list:
- 4 Enter and confirm the user password.
- 5 Click **Enable FTP** to allow the new account to access the FTP server on the appliance. See [Configuring the FTP Server](#) on page 171 for more information.
- 6 Click **Create** to save the information. Select **Cancel** to dismiss the window.

To update an existing user account, perform the following steps:

- 1 Choose **Administration > Users**.
- 2 Select a user from the **Current Users** box.

Update Accounts

Current Users:
op
sandra

Privilege:

Password:

Confirm Password:

Enable FTP

Figure 32 Update Accounts Section of User Administration Window

- 3 Make the desired changes for the user, and click **Update** to commit these changes.

Update Login Attributes

You can protect a users login by selecting a login expiration time and a timeout in case of inactivity.

To update user login attributes, perform the following steps:

- 1 Choose **Administration > Users**.
- 2 Enter the number of seconds desired before a users login is discarded in the Login Expire Time (in seconds) text box as shown in [Figure 33](#). The minimum value is 60 seconds; if you enter Never, there is no expiration.

Update Login Attributes

Login Expire Time (in seconds): (May be 'Never'. Minimum value 60.)

Login Idle-Timeout (in seconds): (May be 'Forever'. Minimum value 60.)

Figure 33 Update Login Attributes Section of User Authentication Window

- 3 Enter the amount of time (seconds) that the user must wait to log in again after the login expire time. The minimum value is 60 seconds; if you enter Forever, the user can never log in again after expiration.
- 4 Click **Update Login Timeouts** to save the information.

Creating Traffic Groups



This section applies to RAMS Traffic only.

RAMS Traffic increases visibility into the traffic flowing through the network core by classifying traffic into user-defined groups. Group rules can include a combination of source/destination prefixes, TCP/UDP ports, an IP protocol, and traffic classes. The traffic group then matches a subset of network traffic between specific locations per applications and/or classes of service.

If a traffic class is specified, it matches a subset of traffic associated with a particular Class of Service (CoS) defined by Type of Service (ToS) or Differentiated Services Code Point (DSCP) bits in the IP header. A traffic deployment can have either ToS or DSCP at one time, but not both.

After the appropriate groups are defined, network administrators can track traffic:

- Determine traffic to or from specific application servers (based on prefixes). For specific services such as “Voice Premium” or “Voice Gold” (based on ToS and DSCP: AF or EF classes).
- Determine the application or CoS.
- Send alerts when percentage utilization or rate exceeds or falls below a specified threshold per traffic group.

To access traffic groups, perform the following steps:

- 1 Choose **Administration > Traffic Groups**.

The View Group window opens, as shown in [Figure 34](#).

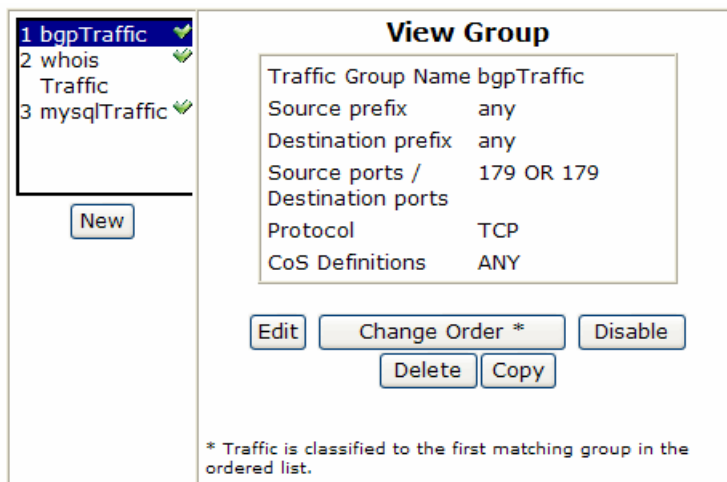


Figure 34 View Group window

- 2 To perform a task on this page, choose from the following list of buttons:
 - **New**—Create a new traffic group (see the next procedure).
 - **Edit**—Modify a previously created traffic group.
 - **Change Order***—Set the priority of the traffic group the Flow Collector will track traffic for.
 - **Enable/Disable**—Enable or disable a group.
 - **Delete**—Remove a group.
 - **Copy**—Create a new group using information for the selected group.



RAMS Traffic assigns the lowest priority to the most recently created traffic group.

To Create Traffic Groups, perform the following steps:

- 1 Choose **Administration > Traffic Groups**.
- 2 In the View Traffic Groups window, click **New**.

The New Group window opens as shown in [Figure 35](#).

New Group

Traffic Group Name

Source prefix

Destination prefix
192.168.0.0/16, 10.0.0.1/32

Source ports

and or

Destination ports
1-100,200,300

Protocol

CoS Groups

All Selected

ARVIND_DSCP_EXP_ALL
kruti-tes1
kruti-test2
kruti-test3

CoS1

Figure 35 Create New Traffic Group Page

3 Configure information in the following fields to create the traffic group:

- **Traffic Group Name**— Field where you name the traffic group.



When naming traffic groups, use upper and lower case alpha-numeric, ampersand (“&”) and underscore (“_”) to name the values.

- **Source Prefix**—Enter one or more source IP prefixes.

- **Destination Prefix**—Enter one or more destination prefixes, separated by commas.
 - **Source Ports**—Enter the source port range (e.g., 1-200, 300)
 - Choose either the **and** or the **or** radio button
 - **Destination Ports**—Enter the destination port range.
 - **Protocol**—Select **Any** or a protocol from the drop-down list.
- 4 In the **CoS Groups** section of this page, select the Class of Service you want associated with traffic group you are creating and then click the arrow button to move the class to the Selected column.
 - 5 In the Classes section, select the traffic classes you want to be part of the traffic group you are creating. You can do this by clicking once on the class, and then clicking the arrow button to the Selected category.
 - 6 Click **Submit** to save the information. The screen refreshes and displays the information entered for the new traffic group

Editing Traffic Groups



This section applies to RAMS Traffic only.

To Edit Traffic Groups, perform the following steps:

- 1 Choose **Administration > Traffic Groups**.
- 2 Select the traffic group and click **Edit**.

The Edit Group window opens as shown in [Figure 36](#).

Edit Group

Traffic Group Name: TGroup1

Source prefix: 192.168.0.0/16

Destination prefix: 10.1.1.1/32
192.168.0.0/16, 10.0.0.1/32

Source ports: 100

and or

Destination ports: 200
1-100,200,300

Protocol: EIGRP 88

CoS Groups

All: ARVIND_DSCP_EXP_ALL, kruti-tes1, kruti-test2, kruti-test3

Selected: CoS1

Buttons: Submit, Reset, Cancel

Figure 36 Edit Group Page



The history for the edited traffic group may not match the new definition.

- 3 Edit the fields you need to revise.
- 4 Click **Submit** to save the information.

Creating CoS Definitions



This section applies to RAMS Traffic only.

CoS specifies a priority value in the packet header that can be used to differentiate the service received by the packet. With this feature, you can associate a user-defined name with a particular CoS, making identifying specific traffic flows easier to locate in the various reports found in the appliance. CoS groups provide you the ability to combine multiple CoS values in a single group.



You must create CoS definitions on the master or standalone appliance.

For IPv4 networks, CoS is specified by a TOS byte or DSCP settings in the IP header. For MPLS-IPv4 and MPLS-VPN networks, CoS is specified by the experimental bits in the MPLS header. In both cases, a router examines and then applies a quality of service to the packet.

To access CoS definitions, locate Traffic on the left navigation pane, and choose **CoS Definitions**.

To create a CoS definition, perform the following steps:

- 1 Choose **Administration > CoS Definitions**.
- 2 Click **New** to define a CoS. The New CoS Definitions window opens as shown in [Figure 37](#).

CoS Definitions

New

Name:

Unselected Selected

DSCP - 1
DSCP - 2
DSCP - 3
DSCP - 4
DSCP - 5
DSCP - 6
DSCP - 7
DSCP - 9
DSCP - 11
DSCP - 13

None

Save Cancel

DSCP

ToS

Mode is common for all CoS definitions.

Note: ToS is only used without MPLS transport.

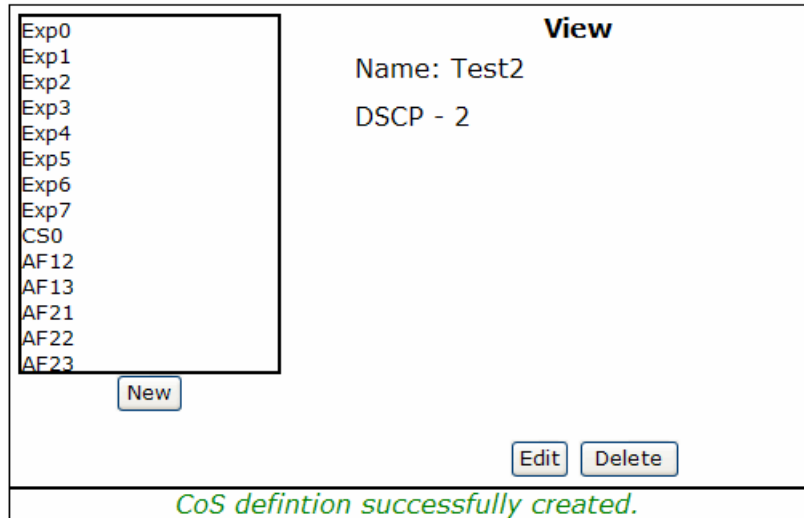
Figure 37 New CoS Definition Window



Changing modes will cause CoS definitions with the mode you want to change from will be lost.

- 3 Enter the name to define the CoS in the **Name** field.
- 4 Select a traffic value from the Unselected column and click the > arrow to move the value to the Selected column.
- 5 Click **Save** to define the CoS value. A confirmation message is displayed along with the new CoS definition and its value as shown in [Figure 38](#).

CoS Definitions



View

Name: Test2
DSCP - 2

Exp0
Exp1
Exp2
Exp3
Exp4
Exp5
Exp6
Exp7
CS0
AF12
AF13
AF21
AF22
AF23

New

Edit Delete

CoS defintion successfully created.

Figure 38 Confirming window for CoS Definitions

To edit a Cos definition, perform the following steps:

- 1 Choose **Administration > CoS Definitions**.
- 2 Select the CoS definition to edit and click **Edit**.

The screen refreshes, showing the CoS definition in the Name field, and the DSCP or ToS values in the Unselected column.

- 3 Edit the name or change the CoS values, as described in the previous section and click **Save**.

Configuring the VNC Server

If you plan to use a VNC viewer to access the system, you must configure the VNC server on a desktop machine. If users will use the X Window System rather than VNC, we recommend that you stop the VNC server. For more information about the VNC viewer, see the “Viewers” chapter in the *HP Route Analytics Management Software User’s Guide*.



VNC server configuration applies only to appliances operating with a GUI license.

You can log into a persistent VNC session that multiple operators can share, or you can log into a session that is created on-demand if both session types are enabled. The persistent, sharable session has an implicit account name, “Nobody,” and a simple password that is set as part of the VNC server configuration. This account is limited to a privilege level of Operator, so it is not possible to perform administrative tasks, such as configuring alerts, in the persistent, sharable session. Authentication for on-demand VNC sessions uses the accounts and privilege levels created on the Users page, or on a remote authentication server.



The VNC server consumes system resources, even when no sessions are active and VNC is not configured for sharing. Start the VNC server only when necessary.

To configure VNC settings, perform the following steps:

- 1 Choose **Administration > VNC Configuration** to open the VNS Configuration page (Figure 39).

VNC Configuration

VNC Display 1

Window Size	Colors	Share Session
1016x700 Width: <input type="text"/> Height: <input type="text"/>	True Color (24 bit)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

VNC Authentication

Password: <input type="text"/>	Confirm password: <input type="text"/>
--------------------------------	--

VNC Displays 2 and Higher

	Width	Height
2	<input type="text" value="1016"/>	<input type="text" value="700"/>
3	<input type="text" value="1024"/>	<input type="text" value="768"/>
4	<input type="text" value="1152"/>	<input type="text" value="768"/>
5	<input type="text" value="1152"/>	<input type="text" value="864"/>
6	<input type="text" value="1152"/>	<input type="text" value="900"/>
7	<input type="text" value="1280"/>	<input type="text" value="864"/>
8	<input type="text" value="1280"/>	<input type="text" value="1024"/>
9	<input type="text" value="1400"/>	<input type="text" value="1050"/>
10	<input type="text" value="1600"/>	<input type="text" value="1200"/>

Configure authentication for displays 2 and higher on User Administration page.

Figure 39 VNC Server Configuration Page

- 2 Configure the following settings. All users who access the system using VNC share the settings configured on this page.
 - Choose the window size, which is the size of the virtual screen of the VNC viewer. You can configure window sizes individually for display 1 and displays 2-10. For display 1, select a window size from the drop-down list, or select **Custom** and enter the width and height (in pixels). For displays 2-10, enter the width and height (in pixels).

- Choose the number of colors to use in the display.
- Choose whether to enable or disable session sharing.
- Enter and confirm the VNC authentication password.

3 Click **Update**.

4 To start the VNC server, click **Start**. When you do so, the button toggles to **Stop**. If VNC server changes are required in the future, stop the VNC server before making changes.



If you change the VNC authentication password after the VNC server is started, you must stop and restart the VNC server for the new setting to take effect.

Connecting to the VNC Persistent Session

After you start the VNC viewer, enter **hostname:1**, where hostname is the name or IP address of the appliance, and then log in using the password you entered in the VNC Configuration page. The VNC session opens using the window size, colors, and sharing properties specified in the VNC Configuration page for VNC display 1.

If you enable sharing of the persistent session, anyone with the VNC password can access the currently active session and issue commands from their desktop. Multiple users can connect at the same time and take turns controlling the user interface to jointly work on a problem. If you disable sharing, only one person at a time can connect to VNC display 1 and all other users are locked out.

When you disconnect from the persistent VNC session, the user interface continues to run. If you connect to the session again later, it resumes as you left it unless someone else has connected and made changes in the meantime.



If the network connection drops while someone is connected with sharing disabled, the VNC server might refuse to allow new connections. To restore VNC access, use the **Stop/Start** button on the VNC Configuration page to stop and restart the VNC Server.

Using On-Demand VNC Sessions

Multiple operators can log into their own sessions.

After you start the VNC viewer, specify the VNC display window size by typing the hostname, a colon, and the VNC display number. For example, enter **hostname:8** to connect to display 8. The VNC viewer will display a login window where you should log in using a user name and password you configured on the User Administration page.

If you and another user connect to the same display number, such as hostname:8, separate VNC sessions are created that both users can operate independently. Multiple users can connect to on-demand VNC sessions up to the user count limit displayed on the License page.



When you disconnect from an on-demand VNC session, the session is terminated immediately.

Managing Databases

Use the Database Administration page to delete or rename an existing database.

To open this page, choose **Administration > Databases**. See [Figure 40](#).

Database Administration

Offline Databases

	Administrative Domain	Protocol	Area ID	Size
<input type="checkbox"/>	A2CorpNet	EIGRP	1	3.6M
<input type="checkbox"/>	A2CorpNet	OSPF	0.0.0.1	50M
<input type="checkbox"/>	A2CorpNet	ISIS	490001	4.3M
<input type="checkbox"/>	A2CorpNet	ISIS	Backbone	4.3M
<input type="checkbox"/>	ConfedsTest	BGP	AS6003	236K
<input type="checkbox"/>	ConfedsTest.ConfedTestBottom	BGP	AS6003	1.9M
<input type="checkbox"/>	ConfedsTest.ConfedTestTop	BGP	AS6001	2.0M
*	CorpNet	EIGRP	1	23M
*	CorpNet	ISIS	4700230001000000000020001	2.7M
<input type="checkbox"/>	CorpNet	BGP	AS65522	112M
<input type="checkbox"/>	CorpNet	BGP	AS65522/VPN	535M
<input type="checkbox"/>	ISPtraf1	ISIS	498888096018253000	35M
<input type="checkbox"/>	ISPtraf1	ISIS	Backbone	952M
<input type="checkbox"/>	ISPtraf1	BGP	AS8888	1.5G
<input type="checkbox"/>	ISPtraf1	Traffic	fr1	4.6G
<input type="checkbox"/>	ISPtraf1	TRS	fa1	476M
<input type="checkbox"/>	UCBJul03a	OSPF	169.229.128.128	3.9M
<input type="checkbox"/>	UCBJul03a	OSPF	169.229.128.168	3.8M
<input type="checkbox"/>	UCBJul03a	OSPF	169.229.128.176	3.9M
<input type="checkbox"/>	UCBJul03a	OSPF	Backbone	5.0M
<input type="checkbox"/>	UCBJul03a	BGP	AS25	379M

New Top-Level Administrative Domain:

12148MB of **106528**MB used on disk (**11%**)

Rename Selected Databases

Delete Selected Databases

Archive Selected Databases

(*) In use databases – cannot be archived, deleted or renamed. Possible solutions - quit all instances of gui client, including stopping the VNC server

Figure 40 Database Administration Page

Databases may occasionally be renamed automatically when a software update requires a change to the database schema. Manual renaming may be required if a database becomes damaged due to a power failure. The renamed databases are considered offline since they are separate from the online databases that are being actively recorded.

The online databases are automatically trimmed to prevent the disk from becoming full. However, if there are too many offline databases on the disk, then the automatic trimming of the online databases may unreasonably limit the history available for analysis. Deleting unneeded offline databases can help you regain disk space. Because each database is stored and managed per-appliance, you must access each appliance individually to perform these administrative tasks on the database.

The length of time that traffic reports are kept in the database depends upon the granularity of the data. Reports with coarser granularity (daily, weekly, or monthly reports) are kept for much longer than reports with finer granularity (5 minute or hourly reports). The amount of time that flow data is kept depends upon load and is generally in the range of 1-2 years. In each case, the oldest data is deleted if there is not enough space left for new data to be stored.

We recommend that you run an FTP application to connect to the appliance FTP file storage area, and then use the delete command to delete any unneeded files. (See [Configuring the FTP Server](#) on page 171 for information about the FTP file storage area.)

The Database Administration page consists of two sections:

- The **Offline Databases** section lists administrative domains that are not currently being recorded.
- The **Online Databases** section lists administrative domains that are currently being recorded ([Figure 41](#)).

Online Databases

	Administrative Domain	Protocol	Area ID	Size
*	CorpNet	OSPF	0.0.0.1	38M
*	CorpNet	ISIS	Backbone	6.5M
*	LabRight.ConfedsTest	OSPF	Backbone	6.5M
*	LabRight.ConfedsTest.ConfedTestBottom	BGP	AS65520	12M
*	LabRight.ConfedsTest.ConfedTestBottom	BGP	AS65520/VPN	9.3M
*	LabRight.ConfedsTest.ConfedTestTop	BGP	AS65510	12M
*	LabRight.ConfedsTest.ConfedTestTop	BGP	AS65510/VPN	9.3M
9 weeks recorded; more than one year of recording capacity at current rate;		Number of weeks to trim:	<input type="text" value="1"/>	Trim Online Databases
Trimming databases may take some time, depending on the amount of data to be removed.				

(*) Online database – cannot be archived, deleted or renamed.

Figure 41 Online Databases Page



Before performing any database operations, quit all running instances of the client and stop the VNC server.

Using Offline Databases

Offline databases contain data from administrative domains that are not currently being recorded. You can delete these databases to save disk space, or rename them if the administrative domain name changes.

Deleting a Database

To permanently delete a database, perform the following steps:

- 1 Stop all instances of the appliance client.
- 2 Choose **Recorder Configuration** to display the Recorder Configuration page.



In a distributed configuration, use the Recorder Configuration page of the master appliance, which displays a tree representing all units in the configuration.

- 3 If the database you want to delete is currently recording, stop recording on that database. Click the node on the tree that corresponds to the database to be deleted and choose **Delete** from the pop-up menu.
- 4 If you are not working with a distributed configuration, proceed directly to Step 6. Otherwise, click **Units** on the left navigation bar to access the Units page of the master appliance and a list of clients in the configuration.
- 5 In the Client Status section of the Units page, select the client where the database was recorded to access the Home page of that client.
- 6 Navigate to the Home page of the client and choose **Administration > Databases**.
- 7 Select the check boxes to the left of the databases to be deleted.
- 8 Click **Delete Selected Databases**.
A confirmation page opens displaying the names of the selected databases.
- 9 Click **Yes** if you want to delete the selected databases.
The selected databases are deleted.

To delete an existing database and start recording to a new database, perform the following steps:

- 1 Stop all instances of the appliance client.
- 2 Navigate to the Home page of the client and choose **Recorder Configuration**.
- 3 If the database you want to delete is currently recording, stop recording on that database.
- 4 Click **Databases** on the left navigation bar.
- 5 Select the check boxes to the left of the databases to be deleted.
- 6 Click **Delete Selected Databases**.
A confirmation page opens displaying the names of the selected databases.
- 7 Click **Yes** if you want to delete the selected databases.
The selected databases are deleted.
- 8 Navigate back to the Recorder Configuration page and start recording on the configuration whose database you deleted.
A new database is created for that configuration and recording begins.

Renaming Databases

To rename one or more databases, perform the following steps:

- 1 Stop all instances of the appliance client.
- 2 Navigate to the Home page of the client and choose **Recorder Configuration**.
- 3 If the databases you want to rename are currently recording, stop recording on these databases.
- 4 Click **Databases** on the left navigation bar.
- 5 Select the check boxes to the left of the databases to be renamed to a single, new name (typically, only databases that have a common first-level administrative domain name already).
- 6 Enter the new name in the New Top-Level Administrative Domain text box. Only the first-level administrative domain name can be changed, meaning, no period is allowed in the new name. Names must begin with an alphabetic character and can contain only alphanumeric characters.
- 7 Click **Rename Selected Databases**.
A confirmation page opens displaying the names of the selected databases.
- 8 Click **Yes** to confirm that you want to rename the selected databases. The top-level name of the selected databases is renamed to the new top-level administrative domain.

Using Online Databases

The Online Databases section of the Database Administration page lists all of the Administrative Domains that are currently being recorded. Below the list is a field that indicates how many days of recording capacity remain based on the current growth rate of the most active of the databases, and a field that indicates the number of days remaining until trimming is needed. The default value of the Number of Weeks to Trim field is 7. You can specify a different interval.

When you trim the online databases, the system deletes data from the earliest point in the databases until the aggregate database size allows for a number of days' growth specified in the Number of Weeks to Trim text box. All databases are trimmed so that the data begins at approximately the same date.

Backing Up and Restoring Data

The system stores recorded route topologies and system configuration files in databases. The Backup and Restore page allows you to selectively save any or all data files, including databases and system configuration files, to one of two storage systems:

- The appliance hard disk.
- A remote storage system, such as your desktop computer. If you back up to a remote storage system, you must configure Server Message Block (SMB) information for that system. See [Enabling SMB and Adding a Remote Server](#) on page 141.

You can save the backup file through the administration interface or by using FTP. Because most web browsers do not allow file transfers larger than 2-4 GB, we recommend that you use FTP to manage large backup files. See [Transferring Backup Files Using FTP](#) on page 145.

The system saves the data files into a single backup file named `backup.dat`. The system saves the backup file with the date and time in your local time zone.



If you back up only to the appliance, there is only one backup file. After you create a new backup file, this new file automatically overwrites the old backup file.

Creating a Backup File

During the backup file creation process, a backup file is created containing the selected databases and/or system configurations. A metadata header is then attached to the backup file. The metadata header contains database and/or system configuration information. It also contains general information about the backup file, including the following items:

- The OS version number.
- The Unit ID of the appliance.
- The schema version number.
- The backup creation date and time.

The system configuration information contains the following items:

- The recorder configuration information.
- System licenses.
- All system logs.
- User account information.

To open the Backup and Restore page, choose **Administration > Backup and Restore** (shown in [Figure 42](#)).

Backup and Restore

Create Backup on This Unit's Disk

Filter by: Administrative Domain Protocol Area ID None

Select All

	Administrative Domain	Protocol	Identifier	Size
<input checked="" type="checkbox"/>	Layouts and other properties			
<input type="checkbox"/>	System Configuration			
Data				
<input type="checkbox"/>	PD64bit.PDcore	BGP	AS65464	15M
<input type="checkbox"/>	PD64bit.PDcore	BGP	AS65464/IPv6	11M
<input type="checkbox"/>	PD64bit.PDcore	BGP	AS65464/VPN	17M
<input type="checkbox"/>	PD64bit.PDcore	ISIS	270001	3.6M
<input type="checkbox"/>	PD64bit.PDcore	ISIS	Backbone	11M
<input type="checkbox"/>	PD64bit.PDospf	OSPF	0.0.0.2	33M
<input type="checkbox"/>	PD64bit.PDospf	OSPF	0.0.0.3	48M
<input type="checkbox"/>	PD64bit.PDospf	OSPF	0.0.4.76	39M
<input type="checkbox"/>	PD64bit.PDospf	OSPF	Backbone	23M

Figure 42 Backup and Restore Page

This page contains the following sections:

- **Filter By**—Allows you to filter the list of items by administrative domain, protocol, or area ID. If you make a selection and click **Filter**, the list is redisplayed with the filtering option applied.

- **Create Backup on this Unit's Disk**—Contains a list of all system configurations and databases in the system and includes the following check boxes:
 - **Layout and other properties**—This check box is always selected, because every backup includes layout and related properties. If you do not select any other check boxes, you back up only the layout and related properties.
 - **System Configuration**—Select this check box to back up the system configuration.
- **Data table**—Lists all the data files available for backup and includes the following information:
 - **Administrative Domain**—The system configuration and/or database administrative domain name.
 - **Protocol**—The protocol the file uses.
 - **Area ID**—The file area ID.
 - **Size**—The size of the file.
- **Restore from Backup on this Unit's Disk**—This section contains the backup file information and the databases and system configuration contained in that file.

Restore from Backup on This Unit's Disk

Backup Info	
Backup Date:	Tue Sep 30 14:51:59 PDT 2008
Software Version	6.5.27-E
OS Version	6.5.27
Unit ID:	003048746CE8
Unit Type:	Master
Size (in bytes)	6533120

	Administrative Domain	Protocol	Area ID	Size
<input checked="" type="checkbox"/>	Layouts and other properties			
<input type="checkbox"/>	Lab240.domain1	Static	snmp	1.2M
<input type="checkbox"/>	Lab240.domian2	BGP	AS12	556K
<input type="checkbox"/>	System Configuration			
<input type="checkbox"/> Overwrite layouts and other properties				
Warning: Restoring the System Configuration will force the system to reboot.				
<input type="button" value="Restore Selection"/>				

Figure 43 Restore from Backup Section

To create a backup file, perform the following steps:

- 1 Choose **Administration > Backup and Restore**.
- 2 Select check boxes to the left of the database and/or system configuration domains that you want to back up.



You cannot back up or restore an actively recording database. An actively recording database opens in the list in green text and an asterisk in place of the check box. Stop database recording in the Recorder Configuration page. See [Updating Software](#) on page 159.

- 3 Click **Create Backup**.

The backup process begins. Depending on the size of the database or configuration, the backup process can take several minutes. The Backup and Restore page opens and periodically updates with the file size as it progresses.

- 4 When the backup file is created, the **Finished** button is displayed on the Backup and Restore page. Click **Finished** to continue.

The Backup and Restore page displays the new backup files in the Restore from Backup on This appliance's Disk table at the bottom of the page, as shown in [Figure 43](#).



Depending on the size of the database and on the Login Idle-Timeout settings, the Administration login may time out before the backup completes. If the **Finished** button does not appear after approximately 15 minutes, log in again.

The Backup Info table appears above the backup file table. This table contains the following backup file information:

- **Backup Date**—The backup date and time.
 - **Software Version**—The software version used to create the backup file.
 - **OS Version**—The OS version used to create the backup file.
 - **Unit ID**—The ID of the appliance.
 - **Size (in bytes)**—The size of the backup file in bytes.
- 5 If you stopped recording before you backed up, start recording data again in the Recorder Configuration page.

Saving a Backup File

After creating a backup file, you can save the file to another location.



Some browsers do not allow file transfers larger than 2-4 GB. It is recommended that you use FTP to manage large backup files. See [Transferring Backup Files Using FTP](#) on page 145.

To save a backup file, perform the following steps:

- 1 Create a backup file as describe on page [page 137](#).
- 2 On the Backup and Restore page, click the **Download Backup File** button.
A File Download dialog box opens.
- 3 Click **Save**.
- 4 Enter a filename for the backup or accept the default filename (backup.dat), and then select a destination for the backup file.
- 5 Click **OK**. The system saves the backup file to the destination you specified in Step 3.

Uploading a Backup File

If you downloaded a backup file that you want to restore, you must upload the file before you restore it.



Some browsers do not allow file transfers larger than 2-4 GB. It is recommended that you use FTP to manage large backup files. See [Transferring Backup Files Using FTP](#) on page 145.

To upload a backup file, perform the following steps:

- 1 Choose **Administration > Backup and Restore**.
- 2 Click **Upload Backup File** at the bottom of the page.
The Restore Backup from File window appears.

- 3 Enter the location of the backup file in the Backup Filename text box, or browse for the file by clicking **Browse**.
- 4 Click **Upload File**.

The upload process begins. Depending on the size of the database or configuration, the upload process can take several minutes.

The databases and/or system configuration in the uploaded backup file appear in the Restore from Backup on This appliance's Disk table.

Restoring a Backup File

You can restore a backup file that has been uploaded.

To restore a backup file, perform the following steps:

- 1 Upload the backup file, if necessary, as described in [Uploading a Backup File](#) on page 139.
- 2 Choose **Administration > Backup and Restore**.
- 3 Select checkboxes to the left of the database and/or system configuration domains that you want to restore.



You cannot back up or restore an actively recording database. Stop database recording in the Recorder Configuration page. See [Updating Software](#) on page 159.

- 4 The **Layouts and other properties** check box is selected by default. Unselect this check box if you do not want to restore the layouts and related properties.
- 5 If the **Layouts and other properties** check box is selected, you can optionally select **Overwrite layouts and other properties** to override the layouts and other properties on the system. If the **Layouts and other properties** check box is not selected, this check box is grayed out.
- 6 Click **Restore Selection**.

The restore process begins. Depending on the size of the database or configuration, the restore process can take several minutes. The Backup and Restore page appears and periodically updates with the file size as it progresses.



If you are restoring the system configuration, a warning appears saying the system will reboot after the restore is complete. The configuration is restored and a message appears indicating that the system is rebooting. If the system does not respond to the browser, wait approximately three minutes for the boot process to complete, and log in again.

The Backup and Restore page displays the restored backup file in the Restore from Backup on This appliance's Disk table at the bottom of the page. If you have more than one backup table in this section, the restored backup file appears in the top table.

- 7 If you want to append new data to the restored database, start recording again in the Recorder Configuration page.

Deleting a Backup File

You can delete the backup file from the hard disk to free up space.

To delete the backup file, perform the following steps:

- 1 Choose **Administration > Backup and Restore**.
- 2 Click **Delete Backup File**, which appears below the Create Backup on This appliance's Disk table.
- 3 In the dialog box that appears, click **YES**.

The backup file information no longer appears in the Restore from Backup on This appliance's Disk section.

Enabling SMB and Adding a Remote Server

The system uses the Common Internet File System (CIFS) implementation of the SMB to create and restore backup files using a remote storage server. You can enable SMB to create more than one backup database and/or system configuration file on a remote storage server.



Remote server reachability is checked every time you open the Backup and Restore page. If the system cannot open the remote server, then the Backup and Restore page displays the backup and restore information.

To enable SMB and add a remote server, perform the following steps:

- 1 Choose **Administration > Archival Configuration** to open the Remote Storage page (Figure 50).

The screenshot shows the 'Archival and Remote Storage Configuration' page. The navigation bar includes 'Home', 'Administration', 'Recorder Configuration', 'Reports Portal', and 'Support'. The 'Administration' menu is expanded, showing options like Alerts, Application, Diagnostics, Maintenance, System, and Archival Configuration. The main content area is titled 'Archival and Remote Storage Configuration' and contains the following fields and options:

- Enable SMB Client
- * Remote username:
- Remote password:
- Remote server:
- Share name:
- Enable Archival
-

Figure 44 Archival and Remote Storage Configuration Page

- 2 Select **Enable SMB** to create or restore backup files from a remote storage server.
- 3 Enter the remote server login user name in the Remote user name text box.



If the login is for a guest only, then leave the user name blank.

- 4 Enter the remote server password.
- 5 Enter the remote server IP address.
- 6 Enter the remote server share name.
- 7 Click **Update**.

The remote storage server information appears in the Restore from Backup on This appliance's Disk section of the Backup and Restore page.

Restoring a Backup File from a Remote Server

Data files are saved in a single backup file named

`backupYYMMDDHHSS_UnitID.dat`

where `YYMMDDHHSS` is the date and time the file was saved and `UnitID` is the server Unit ID.

For example, `0506251345_00304870B6B0.dat` specifies the file was saved on June 25, 2005 at 1:45 p.m. with the Unit ID of 00304870B6B0.



If you back up to a remote storage server, you only have access to the backup files on the remote server, not on the appliance.

If you enabled SMB to save multiple backup files, all backup files appear in the Backup to SMB Storage section of the file backup table. The Restore from SMB Storage section appears underneath the file backup table.

This section displays the information of each backup file in a separate table. The file information of the table that was backed up most recently appears at the bottom of the section. The table contains the following information about the file:

- **Backup Date**—The date and time the file was backed up.
- **Software Version**—The software version used to create the backup file.
- **OS Version**—The OS version used to create the backup file.
- **Unit ID**—The ID of the appliance.
- **Size (in bytes)**—The size of the backup file in bytes.
- **Contents**—Displays the database names and/or indicates that the backup file includes the system configuration.

To restore a backup file from a remote server, perform the following steps:

- 1 Choose **Administration > Backup and Restore**.
- 2 Select the option button in the left column of the backup file.

3 Click **Select Backup File**.

The backup file databases and/or system configuration appears in the file backup table at the bottom of the Restore from SMB Storage section.

4 Select one or more check boxes to the left of the database and/or system configuration domain name that you want to back up.



You cannot back up or restore an actively recording database. Stop database recording in the Recorder Configuration page. See [Updating Software](#) on page 159.

5 Select **Overwrite layouts and other properties** if you want to restore a backup set of layouts and properties.

6 Click **Restore Selection**.

The restore process begins. Depending on the size of the database or configuration, the restore process can take several minutes. The Backup and Restore page appears and periodically updates with the file size as it progresses.



If you are restoring the system configuration, a warning appears saying the system will reboot after the restore is complete. The configuration is restored and a message appears indicating that the system is rebooting. If there is no response, wait approximately three minutes for the boot process to complete, and log in again.

The Backup and Restore page displays the restored backup file in the Restore from Backup on This appliance's Disk table at the bottom of the page. If you have more than one backup table in this section, the restored backup file appears in the top table.

7 If you want to append new data to the restored database, start recording again in the Recorder Configuration page.

Transferring Backup Files Using FTP

Most web browsers cannot manage transfers of files that are 4 GB and larger. Therefore, you have the option of saving the backup.dat file to the hard disk using FTP. You must enable the FTP server to transfer backup files using FTP. See [Configuring the FTP Server](#) on page 171.

Replacing Client and Master Appliances

Follow the procedures in this section to replace client and master appliances in a multi-unit deployment.

Replacing a Client Appliance

Follow the steps in this section to replace a client appliance within a master-client configuration. It is assumed that you have an available backup file (backup.dat).



Make sure that you take regular backups of at least the system configuration according to the instructions in [Creating a Backup File](#) on page 134 and [Saving a Backup File](#) on page 139. Be aware that backing up databases requires that you first stop recording. As an alternative, you can enable archiving according to the instructions in [Configuring Automatic Archival Settings](#) on page 154.

To replace a client appliance, perform the following steps:

- 1 Choose **Recorder Configuration**.
- 2 Click **Stop All Recording**.

Recording is stopped and the Recorder Configuration page refreshes.

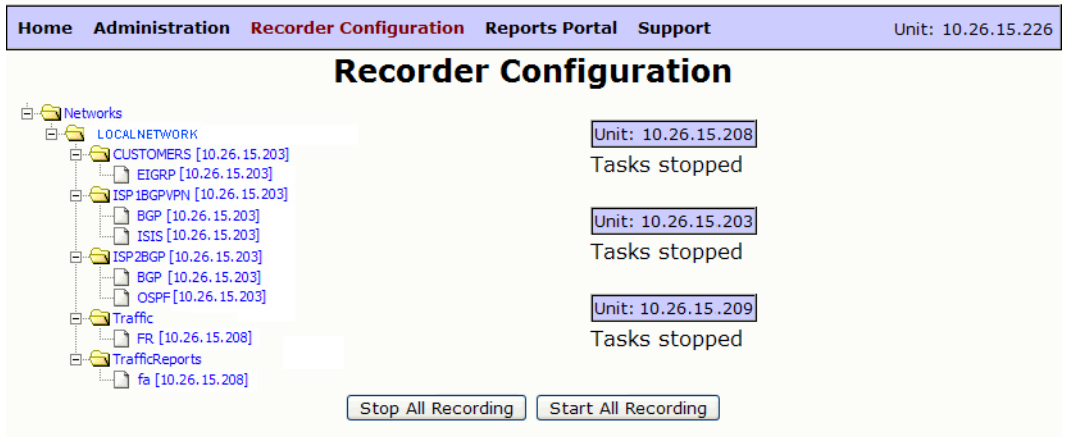


Figure 45 Stopping Recording

- 3 On the Recorder Configuration page, click the highest node in the recorder configuration hierarchy that is bound to the unit in question, and choose **Delete**. You may need to do multiple deletes if the protocols bound to the unit are configured in a disjoint manner.

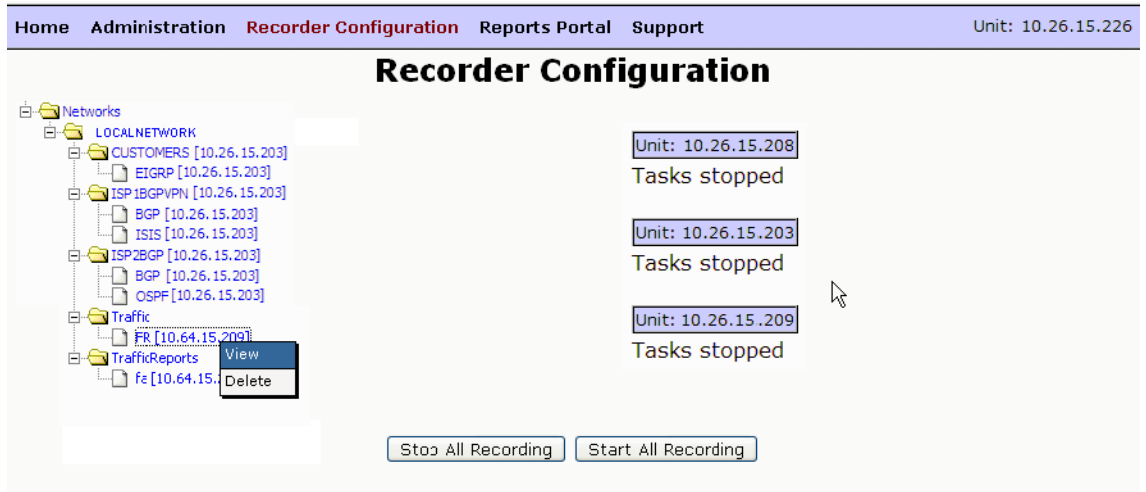


Figure 46 Deleting Units

- 4 Install the new unit. For the initial configuration, enter the IP address of the unit that you are replacing.

- 5 Perform this step if the backup was performed using remote storage on an SMB server. On the new client unit, open the web interface and choose **Administration > Archival Configuration**. Choose **Enable SMB Client** and configure the remote server parameters.
- 6 On the new client unit, open the web interface and choose **Administration > Backup and Restore**.
- 7 Click **Upload Backup File** and browse to choose and upload the backup.data file that you created earlier. If the backup was made to an SMB server, follow the instructions in Restoring a Backup File from a Remote Server on page 4-31.

The items available for backup are now listed on the Backup and Restore page.

- 8 Choose **System Configuration** plus any databases that you want to restore. You do not need to select **Overwrite layouts and other properties** if the layout, alert, or group information stored on the master appliance is already current. Click **Restore Selection**.
- 9 On the master unit, choose **Administration > License** and update the license for the new unit.
- 10 On the master unit, choose **Administration > Units**. Click **Add**, enter the IP address of the new unit, and click **Add**.

The client unit is added and the client status information is updated on the Units page.

- 11 On the master unit, choose **Recorder Configuration** and click **Start All Recording**.

Replacing a Master Appliance

Follow the steps in this section to replace a master appliance within a master-client configuration. It is assumed that you have an available backup file (backup.dat) from the master appliance containing at least one database. No system configuration backup is used.

To replace a master appliance, perform the following steps:

- 1 Use one of the following methods to stop recording:

- If you are replacing a working master, then open the web interface, choose **Recorder Configuration**, and click **Stop All Recording**. Recording is stopped and the Recorder Configuration page refreshes to show the affected units.
 - If you were unable to stop all recording from the master because the unit was not reachable, then open the web interface for each client unit. Choose **Recorder Configuration** and click **Stop All Recording**.
- 2 Disconnect the master appliance from the network.
 - 3 Install the new unit, as described in [Chapter 2, “Hardware Installation”](#). For the initial configuration, enter the IP address of the unit that you are replacing.
 - 4 On the master unit, open the web interface and choose **Administration > License**. Install the license for the new unit if it is not already installed.
 - 5 Choose **Administration > Units** and click **Make Master**.

Units

To run RAMS in a distributed fashion, elect one machine to be the master. You must also select one of the administrative interface IP addresses on this machine to be the master IP address. All other machines will be clients.



Figure 47 Making a Master Unit

- 6 On the master appliance, the system configuration must not be restored from backup because the information will be inconsistent between the old appliance and its replacement. Instead, you must manually configure the following administration items as needed:
 - Login Message
 - Queries
 - VNC Configuration
 - Archival Configuration
 - FTP Server
 - Mail

- Network and Interface (host name and DNS server)
 - Time and Date (configuring an NTP server is required)
- 7 To add the client units, choose **Administration > Units**. For each client unit, enter the IP address, and click **Add**. The recorder configuration will be pulled up from the client appliance to the master.
 - 8 On the master unit, choose **Recorder Configuration** and click **Start All Recording**. Verify that all of the recorders start and begin writing to their databases.
 - 9 Choose **Administration > Data Source Configuration**, and configure the same options that were configured on the old master. Click **Update**.
 - 10 Choose **Administration > Backup and Restore**. Click **Upload Backup File** and browse to choose and upload the backup.data file that you created earlier. If the backup was made to an SMB server, follow the instructions in Restoring a Backup File from a Remote Server on page 4-31.

The items available for backup are now listed on the Backup and Restore page.

- 11 The **Layouts and other properties** check box is selected by default. Unselect this check box if you do not want to restore the layouts and related properties.
- 12 If the **Layouts and other properties** check box is selected, you can optionally select **Overwrite layouts and other properties** to override the layouts and other properties on the system. If the **Layouts and other properties** check box is not selected, this check box is grayed out.

Backup and Restore

Restore from Backup on SMB Storage

Backup Info	
Backup Date:	Wed May 14 11:35:32 PDT 2008
Software Version	6.1.4-E
OS Version	6.1.4
Unit ID:	0030482F90C4
Size (in bytes)	13649920

	Administrative Domain	Protocol	Area ID
<input checked="" type="checkbox"/>	REP1210568707repTest.RR2	ospf	0.0.0.241
<input type="checkbox"/>	System Configuration		

Overwrite layouts and other properties

Warning: Restoring the System Configuration will force the system to reboot.

Figure 48 Restoring a Master Unit

- 13 Choose **Recorder Configuration** and click **Start All Recording**.

Choosing a Data Source

You can have multiple recorders geographically and topologically distributed in remote parts of the network. This provides you with a global view of the entire network topology from a local copy of the database, which will minimize delay. Data replication is enabled by default on the Modeling Engine.

Using the Data Source Configuration page, you can have the appliance that is licensed to act as a Modeling Engine replicate data from the Route Recorders in your distributed configuration. This centralized Modeling Engine

consolidates the data that has been collected across the network to a centralized location. You can retrieve network-wide information from a local source.

The Data Source Configuration page allows you to specify where routing data is obtained. You can obtain reports from individual Route Recorders; however, using a centralized Modeling Engine to generate reports provides a global view of the network and reduces the amount of time required to obtain that view. In addition, querying the Modeling Engine reduces the amount of work required by the Route Recorders, whose primary function is to record data.

If you do obtain routing data by querying each Route Recorder individually, you can configure GRE tunnels to connect Route Recorders deployed to remote areas of the network. Each Route Recorder provides reports specific to the local areas and protocols where it is listening.



You need at least 1 Mbps bandwidth between the Route Recorders and the replicating Modeling Engine.

Choose a data source using the Data Source Configuration page.

To set up the data source configuration on the Modeling Engine, perform the following steps:

- 1 Choose **Administration > Data Source Configuration** to open the page (Figure 49).

Data Source Configuration

Data Source Configuration

Get data from Route Recorders

Connect to a Replicating Modeling Engine

RME not found

Enable Replication

Bring back data for the past

Two Months

Central Reports/Alerts daemon*

*Required for network-wide alerts and reports, and when the Flow Recorder Prefix Source uses the Reports Server.

IP Address	Replication Status Databases	Status
10.64.15.230	PDlabSP3_bgp_AS65464 PDlabSP3_static_snmp PDlabSP3_bgp_vpn_AS65464 PDlabSP3_bgp_ip6_AS65464 PDlabSP3_isis_270001 PDlabSP3_isis_Backbone PDlabSP3_test12969_bgp_AS12 PDlabSP3_test12969_bgp_vpn_AS12 PDlabSP3_test12969_bgp_ip6_AS12	Running

Figure 49 Data Source Configuration Page

- 2 Click **Get data from Route Recorders** to disable replication of data on the Modeling Engine. To obtain network information, you must query individual Route Recorders.
- 3 Click **Connect to a Replicating Modeling Engine** in deployments where multiple Modeling Engines are co-located. You can choose one appliance to act as the centralized Modeling Engine, then point additional Modeling Engines to this central appliance to obtain network-wide data. When you select this option, you must provide the IP address of a Modeling Engine who has replication enabled as described in the following paragraph.
- 4 Click **Enable Replication** to allow replication from the Route Recorders in the deployment.

- 5 Choose a time interval from the drop-down list to obtain data for the specified interval. When you enable replication, you choose the amount of data to be copied from the network's Route Recorders to the centralized Modeling Engine.
- 6 Click **Update** to update the list of replication databases.
- 7 Click **Start Replication** to begin the replication process.

While data is being replicated, the Replication Status table lists the IP addresses of each Route Recorder in the deployment, which databases are being copied, and the status of the replication. Only databases that are currently recording are replicated.



When a Route Recorder is added to the network, the centralized Modeling Engine automatically begins replicating data from that appliance. If you opt to bring back 2 weeks of data, for example, the Modeling Engine copies data recorded up to 14 days before the Route Recorder was added to the configuration.

If replication is enabled on the Modeling Engine, you can select the **Central Reports/Alerts daemon** check box to produce network-wide reports from the local Modeling Engine.

After a database is replicated on the Modeling Engine, the Route Recorder retains ownership of that data. Any operation, such as delete or rename, that is performed on the Route Recorder will be replicated on the Modeling Engine.

Archiving Data

The automatic archival of data differs from creating backup files, which is described in [Backing Up and Restoring Data](#) on page 134:

- You can archive data without stopping the recording process or requiring users to log off.
- Segments of data are archived on an incremental basis, rather than stored at once. Segments of data are created each week, on Sunday, when the database is divided into manageable files, labelled by date and time. These files are archived at regular intervals (every 7 days, on Monday at 0:00).

Only previously unarchived data is stored during this process. Archived data remains accessible for analysis through the History Navigator. For more information, see “The History Navigator” chapter in the *HP Route Analytics Management Software User’s Guide*.



The procedures for archiving data on the Modeling Engine are the same for a distributed configuration as they are for stand-alone configurations. The only difference is the archived data for the distributed configuration will be replicated.

Unlike Backup and Restore, automatic archiving data does not allow up-to-the-minute data storage and retrieval. For example, if data is automatically segmented on Sunday, June 25 at 10:55 PM, those segments are archived Monday, June 26, at 0:00. Any data written to the database beginning on Sunday, June 25 at 10:56 PM is not archived until the following Monday, July 3 at 0:00. To capture data between intervals use the Archive Now feature. This manual option requires you to stop recording on the database before archiving, and is described in [Manually Archiving Data](#) on page 156.



If more than one recorder is recording and archiving the same network area, or if archiving is configured on both the recorder and Modeling Engine that is replicating the data, and if both are pointing to the same storage appliance, then the recorder or Modeling Engine that was invoked first will actually store the data.

Configuring Automatic Archival Settings

Manage the archival tool using the Archival Configuration and Remote Storage page ([Figure 50](#)).

Home	Administration	Recorder Configuration	Reports Portal	Support	Unit: 19
------	-----------------------	------------------------	----------------	---------	----------

Alerts
Destinations
SNMP Test
IGP
BGP

Application
VNC Configuration
Layout Backgrounds
Queries

Diagnostics
System Diagnostics
View Log
View Configuration

Maintenance
Backup and Restore
Databases
License
Software Update
Restore Archives
Shutdown

System
Support Access
Network and Interface
Time and Date
Mail

Archival Configuration

Users

Archival and Remote Storage Configuration

Configure Archival and SMB share information for creating/restoring archives/backups to and from a remote storage

Enable SMB Client

* Remote username:

Remote password:

Remote server:

Share name:

Enable Archival

Figure 50 Archival and Remote Storage Configuration Page

Data is archived every seven days. Archiving of data occurs per-appliance; you must configure archival settings on each appliance in a distributed system.

To configure the archiving tool, perform the following steps:

- 1 Enable remote storage as described in [Enabling SMB and Adding a Remote Server](#) on page 141.
- 2 Choose **Administration > Archival Configuration** to open the Archival Configuration and Remote Storage page
- 3 Select **Enable Archival**.
- 4 Click **Update**.

Any unarchived databases that exist before you enable archival functionality will be archived at the next scheduled archiving interval.

Manually Archiving Data

To archive data between regularly scheduled intervals, which occur weekly on Monday at 0:00 in the time zone set on the appliance, use the **Archive Selected Databases** button on the Database Administration page. Only offline databases can be archived. Before manually archiving data, you must stop recording on the selected database if necessary. The system then archives the most recent unarchived data. When recording is restarted, the system creates and begins writing to a fresh segment of the database.



Databases created with software 3.7x and earlier cannot be archived.

To manually archive data, perform the following steps:

- 1 Choose **Administration > Databases**.

The Database Administration page is displayed as shown in [Figure 40](#).

- 2 In the Offline Databases section, select one or more check boxes corresponding to the databases to archive.

If the database to archive is currently online (recording), it appears in green. You must stop recording to the database before you can archive data. See [Chapter 2, “Configuration and Management”](#) for more information about starting and stopping the recorders.

- 3 Click **Archive Selected Databases**.

Segments of the selected databases are archived. Filenames of the archived segments use the following format:

```
DatabaseName_<segment time in epoch>
```

For example:

```
CorpNet_Common_West_bgp_AS65520_1149663600
```

When you restart recording, the system creates and begins writing to a fresh segment of the database.

The web-based configuration page includes a **Re-archive** button as well. Using **Re-archive** forces the system to archive all available data, whether or not the data was previously archived.

Restoring Archived Data

Retrieve archived data using the Restore from Archive page (Figure 51).

Restore from Archive

Start Time:

End Time:

Databases to Restore: *

Figure 51 Archival and Remote Storage Configuration Page

This page contains the following settings:

- **Start Time:** The start time of the data to restore, in the following format:

YYYY-MM-DD HH:MM:SS

followed by the time zone (for example, PDT).

- **End Time:** The end time of the data to restore, using the format shown above.

- **Databases to Restore:** Contains the names of all databases that have segments available for restoration. The Databases to Restore box lists database names in the following format:

CorpNet.Common/ospf/Backbone

This format corresponds to the literal database name:

corpnet_common_ospf_backbone

Labels are created based on the name of the database. For example, note that if you have renamed a database as described in [Renaming Databases](#) on page 133, the original database name is used in the Databases to Restore list box.

For example, three labels are listed in the Labels to Restore box. The first label, SegmentA, contains data that began recording on June 4 at 10:31:55 PDT. The third label, SegmentC, contains data that stopped recording on June 24 at 10:31:55 PDT. The data contained in all three listed segments was recorded between the start and end times indicated.

Restoration of data occurs on a per-appliance basis; you must access each appliance in a multi-appliance deployment individually to enable and configure archival settings.

To restore archived data, perform the following steps:

- 1 Choose **Administration > Restore Archives**.
- 2 Specify a start and end time corresponding to the data to restore.

For example, to restore data that was recorded between Wednesday, June 7, 2006 and Wednesday, June 14, 2006, enter the following:

2006-06-07 0:00:00 in the Start Time text box

2006-06-14 0:00:00 in the End Time text box.

Since each segment of data begins on Sunday and ends on Sunday, the restored archives will include more than the requested

Wednesday-to-Wednesday time range. In other words, restored data will include Sunday, June 4 through Sunday, June 18.

- 3 Click to select one or more databases in the Databases to Restore list box that corresponds to the database to restore.
- 4 Click **Restore Now**.

When restoring the archived data, the system retrieves archived database segments for the time range you specified. A new database is then created to store the retrieved segments. The new database is named:

DatabaseName<Time1>to<Time2>, where DatabaseName is the name of the database whose segments have been restored, <Time1> is the start time of the first restored segment, and <Time2> is the end time of the last restored segment.

Following the example used in Step 2, the restored database name would be:

```
CorpNet_Common_West20060607to20060614_bgp_AS65520  
[or in epoch: 1149663600to1150268400]
```

Updating Software

HP provides software updates for <major number>.<minor number> versions of the software (for example, version 7.0) using the Software Update feature.

If the system has a Software Update license, you can download software updates directly from the HP FTP site. Contact HP customer service for a license key if necessary.

To download a new software update, choose **Administration** > **Software Update** to open the Software Update page ([Figure 52](#)).



In a distributed configuration, where more than one appliance is installed, you must update the software of the master appliance before updating the software on each client appliance.

Software Update

Version Information

Installed Software and OS: 8.5.37-E Installed: 2009-12-05 18:37:16
Alternate Software and OS: 8.5.36-E

Note: Installing an alternate Software and OS will cause the system to be rebooted.

Operators currently connected: 2

Download Software Update

URL:
Key:

Proxy Settings

Use Proxy

Host: Port:
Username: Password:

Figure 52 Software Update Page

The appliance has its own operating system software and application software. How you update the software depends on how it is connected to the Internet:

- The download process is easiest when the appliance is connected to the Internet, either directly or through a proxy server. See [Updating with Internet Access](#) on page 160.
- If the appliance cannot get access to the Internet, you can download an update, move it to a locally accessible FTP server and then perform the update. See [Updating without Internet Access](#) on page 163.

Updating with Internet Access

If the system can access the Internet directly or through a proxy server, follow the steps in this section. Otherwise, proceed to [Updating without Internet Access](#) on page 163.



Before updating software, stop recording on Route Recorders and the Flow Collectors. Restart recording after the update is complete. This ensures that databases are renamed correctly.

To download updates when connected to the Internet through a proxy server, first you must set up the proxy configuration. You can then proceed to the second set of steps to download the update.

To set up the proxy configuration, perform the following steps:

- 1 Choose **Administration > Software Update** on the appliance where you are updating software.
- 2 Select **Use Proxy**.
- 3 Enter the host and port details for the proxy server.
- 4 If the proxy server is password protected, enter the user name and password.
- 5 Click **Save Proxy Settings** to preserve these settings for future downloads.

In a distributed configuration, where more than one appliance is installed, you can update software on multiple machines at once after the software on the master appliance has been updated. You must leave each the Software Update page open in a browser window until the software download for the machine is complete.

To download updates when connected directly to the Internet, perform the following steps:

- 1 Choose **Administration > Software Update** on the appliance where you are updating software.

An Update Available message tells you if an update is available. If so, the URL of the update appears automatically in the URL text box. Otherwise, a message tells you no update is available.



The Check for Updates button checks only for updates within the same major.minor version number. To update to the next major or minor release, you must enter the URL manually.

- 2 In the Key text box, enter the update key provided by HP customer support. Click **Update** to begin download and installation of the update.

Alternatively, on a Modeling Engine that serves as a master appliance for a system of multiple appliances, you can click **Update All Units** to automatically update the Modeling Engine and then all of the client appliances in sequence. The **Update All Units** procedure will not be performed if any of the client appliances is not reachable. When you click **Update All Units**, the software update image is fetched to the Modeling Engine and then distributed from there to all of the client appliances. At that point, recording is automatically stopped and the Modeling Engine is rebooted. After the Modeling Engine comes back up, all of the client appliances are rebooted. The client appliances resume recording when they come back up.

You can monitor the progress of the update in the log window that is displayed on the Software Update page. If you exit your browser, the updating and rebooting process will still continue. If you later return to the Software Update page, a **Finish** button and log are displayed. Click **Finish** to complete the process.

- 3 If the download includes an operating system update, a message appears stating that you must reboot to complete the download. Click **Reboot Now** and wait for the system to reboot. This should take approximately two or three minutes.

In a multi-appliance deployment, when updating software update on a client machine, you will be automatically directed to the master appliance's Home page 5 seconds after you click **Reboot Now**.

- 4 Log in again.



If at any time during the update process a 404 page error appears, click **Back** on the browser and then click **Refresh**.

Updating without Internet Access

If the system cannot access the Internet directly or through a proxy server, you can download an update to a local FTP or HTTP server, and then install the update from the local server.

Use the full URL to download the update because the file may be hidden in an unreadable directory.

In a distributed configuration, where more than one appliance is installed, you can update software on multiple machines at once after the software on the master appliance has been updated. You must leave the Software Update page for each appliance open in a browser window until the software download is complete on that machine.

To download updates when the appliance is behind a firewall, perform the following steps:

For FTP:

- 1 Go to the HP Route Analytics Management Software product web site (<http://www.hp.com/go/hpsoftwaresupport>) and click the **Use self-solve knowledge search** link. Do not use the Software Patches link at the bottom of the page.
- 2 Search for the keywords **RAMS update**. Determine if the non-empty results of your search provides an appropriate update version of RAMS.

If an update is available, download it and save it to a convenient location. Make a note of the associated update key, which you will need to complete the update.



Instructions that accompany an upgrade may differ in some details from the steps given in this section. If so, use the instructions from the web site, as they are more recent.

- 3 Move the update package to a local server configured for anonymous FTP. The RAMS appliance itself is an acceptable server, providing you set it up as described in [Configuring the FTP Server](#) on page 171.
- 4 In the **URL** field, enter the URL for the local server you are using. For example, `ftp://anonftp.company.com/<dir>/<patch>`

If you use the RAMS appliance as your FTP server, the URL could easily be:

file:///<dir>/<patch>

5 Enter the update key that you saved in Step 2.

6 Click **Update**.

Downloading begins. If the download includes an operating system update, a message appears stating that you must reboot to complete the download.

7 Click **Reboot Now** and wait for the system to reboot. This should take approximately two or three minutes.

8 Click the **Home** link and log in again.

Returning to a Previous Version

The previously installed version of the software is saved on the appliance. If you experience difficulty running a new version of software, you can return to the previous software version. The Software Update page displays the previously installed version number.



Reverting to the previous version may require a reset to factory defaults, as described in [Shutting Down](#) on page 178, because updates may not be completely reversible. Resetting to factory defaults will erase all data and configuration settings except the installed license. After reverting to the previous version and resetting to factory defaults, you can restore the data and configuration settings if you have a backup file created with the previous version.

To reinstall a previous version of the operating system, perform the following steps:

1 Choose **Administration > Software Update** .

2 Click **Install Alternate Software and OS**.

To install only alternate software, click **Install Alternate Software**.

3 Click **Yes** to install the previously installed version.

An informational window opens stating that an alternate version is installing and the system is rebooting.

4 (Optional) If re-set is required, refer to page [page 179](#) for re-set instructions.

Using the Reports Scheduler

You can schedule a time for the appliance to send daily reports that summarize the health of a unit and its recording processes along with BGP and IGP activity using the Reports Scheduler page. The reports arrive via email. To access the Reports Scheduler, choose **Administration > Reports Scheduler**. The page appears as shown in [Figure 53](#).



Routing Reports are configured and generated only on appliances that record routing data, or on the master unit of a distributed configuration. You can configure and generate health reports on all Route Analytics Management Software appliances.

Reports Scheduler

Mail System Configuration

Configure the Mail Server (optional) and the Sender information for emailing of Daily Reports and Top N Reports.

Mail Server:

Sender:

Test Message Recipient(s):

Daily Reports Setup

Configure the daily generation and emailing of Health and Routing Reports. On-demand generation of Health and Routing Reports is available at the Reports Portal.

Report generation begins at:

Daily Reports Recipient(s):

Health Report

Summarizes the health of each unit in the network, including the status of the various recording processes and their databases, database replication (if applicable), SQL, and RAID (if applicable). Also displays a hierarchical view of the networks monitored by each unit and the license information present on each unit.

- Generate Daily Health Report
- Email Daily Health Report

Routing Report

Presents a variety of IGP reports (topology counters, flapping links, flapping prefixes, active routers, and withdrawn watch list prefixes) for each actively recording IGP domain and a variety of BGP reports (topology counters, BGP route flaps, prefix redundancy divergence, and AS reachability divergence) for each actively recording BGP topology. Only present on Master or Route Recorder units (including Standalone units).

- Generate Daily Routing Report
- Email Daily Routing Report
- Domain Level Reports

Top N Reports Setup

Configure generation and emailing of Top N Reports. Top N Reports are generated when the traffic data is being recorded on the Flow Analyzer unit.

Top N Reports Recipient(s):

Report Configuration Parameters

Report Name	Report Type	Number of Elements
Traffic Groups	<input type="text" value="none"/>	<input type="text" value="100"/>
BGP Destination AS	<input type="text" value="none"/>	<input type="text" value="100"/>
BGP Egress Router	<input type="text" value="none"/>	<input type="text" value="100"/>
BGP Neighbor AS	<input type="text" value="none"/>	<input type="text" value="100"/>
Summary Exporters	<input type="text" value="none"/>	<input type="text" value="100"/>
Summary Link	<input type="text" value="none"/>	<input type="text" value="100"/>
VPN CoS	<input type="text" value="none"/>	<input type="text" value="100"/>
VPN Customer	<input type="text" value="none"/>	<input type="text" value="100"/>
VPN Egress PE	<input type="text" value="none"/>	<input type="text" value="100"/>
VPN Ingress P	<input type="text" value="none"/>	<input type="text" value="100"/>
VPN Ingress PE	<input type="text" value="none"/>	<input type="text" value="100"/>

Email Top N Report

Figure 53 Report Scheduler Page

Configuring the Mail System

Before you can schedule daily reports on a Route Recorder, you must specify the mail system information used to deliver the reports.

You can also enable health reports and routing reports. Health reports provide status of processes of each machine running on a network (for example, this report will show recording processes and status of databases that are active). Routing reports will show IGP and BGP reports for databases that are recording. The BGP routing report also displays the date and time the report was generated.

To configure the mail system, perform the following steps:

- 1 Choose **Administration > Reports Scheduler**.
- 2 Enter the outbound mail server or relay in the Mail Server box using a DNS name or an IP address. If you do not specify a mail server, the system attempts to send directly to the mail servers of the recipients.
- 3 In the Sender text box, enter the full e-mail address to be shown as the sender of mail. Bounced e-mail messages may be sent to this address, so this address should be valid. If the hostname and domain name are omitted, or just the domain name is omitted, the corresponding names configured on the Network & Interface Configuration page will be appended.
- 4 Enter the recipient e-mail address or addresses in the **Recipients** box. If you have more than one recipient, separate each recipient address with a comma.
- 5 Click **Update Mail Configuration**.



To send a test message, enter an email address in the Test Message Recipient(s) field and click **Send Test Message** to send a test message to the recipient.

Setting Up and Scheduling Daily Reports

To schedule daily reports, perform the following steps:

- 1 Choose **Administration > Reports Scheduler**.

- 2 Select the time to generate and send reports from the **Report generation begins at** drop-down list.
- 3 Enter a list of recipients to receive the daily reports. If you have more than one recipient, separate each recipient address with a comma.
- 4 To generate health reports, select **Generate Daily Health Report**, and to include the reports in the daily email, click **Email Daily Health Report**.
- 5 To generate routing reports, select **Generate Daily Routing Report**, and to include the reports in the daily email, click **Email Daily Routing Report**.
- 6 By default, the system generates a single report that covers all protocol domains. To generate a separate routing report for each domain, select **Domain Level Reports**.
- 7 Click **Update Daily Reports Configuration**.

Understanding Daily Report Contents

The Health Report summarizes appliance health status and includes the following information:

- **Unit Status**—Lists all configured recording processes (BGP Recorder, EIGRP Recorder, ISIS Recorder, OSPF Recorder, Flow Collector, Traffic Report Server, and Flow Analyzers) with the status of the processes and the databases they are recording. Also lists the status of database replication, SQL, RAID, and NTP, where applicable.
- **Networks Monitored**—Lists all databases on the appliance and their current status: online, offline, or offline in the last 24 hours.
- **License Information**—Lists the status of all licenses on the appliance.

The Routing Report summarizes network activity, and includes the following information:

- **IGP Summary**—If IGP is recorded, this section lists the following results in all online networks:
 - Counts of the number of routers, adjacencies, and prefixes
 - Top 5 flapping links
 - Top 5 flapping prefixes
 - Top 5 active routers

- **BGP Summary**—If BGP data is recorded, this section lists the following results in all online databases:
 - Top 5 BGP route flaps
 - Top 5 prefix redundancy divergence
 - Top 5 AS reachability divergence

In master units, the Health Reports and Routing Report are a combination of the reports generated by the client units.

For Health Reports, the master unit report replicates the individual reports for itself and all of its clients as generated on the client appliances. Significant problems are summarized at the top of the report.

For Routing Reports, if the centralized report server is not enabled, the master unit report will replicate the individual reports for all client units that record routing data. If the centralized report server is enabled, the master unit report will contain one report that consolidates all of the online routing data from all of the client appliances.

Scheduling Top N Reports

Use Reports Scheduler page to run Top N reports automatically and deliver the reports at pre-configured time periods. You can select from a set of pre-defined reports, specify time ranges and frequency, and arrange for email delivery.

The following guidelines apply when configuring Top N Reports:

- We recommend that you configure Top N Reports on the Modeling Engine; however, you can configure Top N Reports on the Flow Analyzer.
- You must configure the sender address (and optionally the mail server) on the Mail page in addition to configuring the Top N Reports page. See “Using the Reports Scheduler” on page 165.
- If no recipient list is configured on the Top N Reports page, the recipient list from the Mail page is used.
- Top N Reports emails are sent from the Flow Analyzer, so communication from that appliance to the mail server or directly to the recipients must not be blocked. If it is necessary for that appliance to use a different mail server than the Modeling Engine, you can configure the mail server on the Mail page of the Flow Analyzer appliance.

To configure Top N Reports, perform the following steps:

- 1 Choose **Administration > Reports Scheduler**.
Scroll down to the Top N Reports area, as shown in [Figure 53](#).
- 2 Enter the email addresses of those needing these reports in the Top N Recipient(s) text box.



If you have more than one email to enter, separate the email addresses with a comma.

Report names will display beneath the Report Name column in the Report Configuration Parameters section of the window.

- 3 In the Report Type column, select the frequency of reports. The options you can choose from are none, daily, weekly, and monthly.
- 4 In the Number of Elements field, select a maximum of rows you want returned in the report. In the figure shown above, BGP Destination AS report will display 100 AS's that are established.
- 5 To email the selected reports, select the **Email Top N Report** checkbox.
- 6 After entering the report name, type, and number of elements, click **Update Top N Reports Configuration** to activate Top N Report generation.

Viewing Saved Daily Reports

The last 30 days of reports are saved on each appliance that records routing data, so that you can compare changes to an earlier report.

To view saved daily reports, perform the following steps:

- 1 Choose **Reports Portal**.
- 2 Click on a report file name to download or view that report.
- 3 If you click **Daily Reports** on a system that does not have the Route Analyzer Reports license, a message is displayed advising you to access a system that records routing data.

Viewing Previously-Generated Top N Reports

Top N reports are automatically saved for 30 days.

To view previously-saved Top N Reports, perform the following steps:

- 1 Choose **Reports Portal**.
- 2 Click **Saved Top N Reports** on the left navigation menu to list all of the saved reports.
- 3 Click a report link to view the report, or right-click the report link to save the report.

Configuring the FTP Server

A portion of the hard disk on the appliance is available for the storage of users' files in the FTP server directory. Upload time series files and Multi Router Traffic Grapher (MRTG) files onto the appliance using FTP for correlation with routing events (see "The History Navigator" chapter in the *HP Route Analytics Management Software User's Guide* for information about correlating time series data). Backed-up database files are also stored on the appliance.



SFTP may be used as an alternative to FTP. Use of SFTP does not require enabling the FTP server because it is carried inside the SSH protocol that is always enabled for GUI access.

The account name used in this procedure must be configured to enable FTP access. This can be done in one of the following ways:

- If the appliance is configured for local authentication, be sure to enable the FTP check box while setting up user accounts (see [Creating New User Accounts](#) on page 115).
- If the appliance is configured for remote authentication, use the `rex-ftp` parameter for remote TACACS+ or RADIUS authentication (see [TACACS+ and RADIUS Parameters](#) on page 111).

To access the FTP Server Configuration page, choose **Administration > FTP Server**.

The FTP Server Configuration window opens, as shown in [Figure 54](#).

FTP Server Configuration

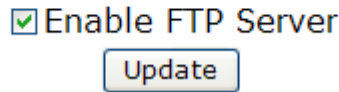


Figure 54 FTP Server Configuration Page

To enable FTP file uploads, perform the following steps:

- 1 On the FTP Server Configuration page, check the **Enable FTP Server** check box.
- 2 Click **Update** to complete configuration.

After the FTP is enabled, you can log in for FTP file transfer.

Configuring Flow Fanout

Flow fanout redistributes NetFlow packets that are received on a selected physical interface and port to specified destinations identified by IP address and port.

To enable flow fanout, perform the following steps:

- 1 Choose **Administration > Flow Fanout**.

The Flow Fanout Configuration window opens, as shown in [Figure 55](#).

Flow Fanout Configuration

Flow Fanout will redistribute NetFlow packets received on the selected physical interface to the destinations configured by IP address and port below.

IP address	Port number
<input type="text"/>	<input type="text" value="9991"/>
<input type="text"/>	<input type="text" value="9991"/>
<input type="text"/>	<input type="text" value="9991"/>
<input type="text"/>	<input type="text" value="9991"/>
<input type="text"/>	<input type="text" value="9991"/>

Physical interface

Net flow port

Figure 55 Flow Fanout Configuration Page

- 2 Select the physical interface from the Physical Interface drop-down list.
- 3 Enter the port to receive the NetFlow data.
- 4 Enter the IP addresses and port numbers of all the destinations to receive the NetFlow packets that are received on the specified interface.
- 5 Click **Save Configuration** to store the changes.
- 6 To begin redistributing the NetFlow packets, click **Start Flow Fanout**.

Viewing and Exporting Log Pages

You can view and export log files to help diagnose problems on a particular appliance. Choose **Administration > View Log** to open the View Log page (Figure 56).

To view a log page, perform the following steps:

- 1 In the Remote Syslog Collector field, enter the name or IP address of the system you want to view messages for.
- 2 Press the **Set Collector** button to display messages stored on the system.
- 3 Specify which component logs to view or choose **All** from the **Component** drop-down list.

The number of pages in the log displays automatically.

- 4 From the **Lines** drop-down list, select the number of lines to display per page.
- 5 (Optional) Enter the page number to view in the **Page** text box. If you leave the text box empty, page 1 displays by default.

View Log

Remote Syslog Collector:

Filter

Component: Lines: Page: of 362

Show most recent first

Log

Figure 56 View Log Page

- 6 Select the **Show Most Recent First** check box to see the last recorded log entries.
- 7 Click **Apply Filter**.

You can print a copy of this page using the print command on the web browser.



If no relevant records are found, the message “No Recent Applicable Messages” will display.

To export the log as plain text, perform the following steps:

- 1 Choose which section of the log to export by following the previous set of steps in this section.
- 2 Click **Export Log as Plain Text**.
The log page is redisplayed in plain text form in the browser window.
- 3 Use the **File** menu on your browser or right-click in the window to open the pop-up menu.
- 4 Choose **Save As**.
- 5 Enter the directory where the log file will be stored, and then click **Save**.
- 6 Click the **Back** button on your browser to return to the View Log page.

Uploading Layout Backgrounds

Layout backgrounds are images that you can apply to the routing topology map to provide additional visual cues to the layout. For example, you can upload a map depicting the geographic location of network routers, which would enable you to arrange nodes based on physical or logical groupings, such as per building or per lab.

Create or convert a desired background image using JPEG, PNG, BMP, SVG, or XPM (X PixMap, an ASCII image format used by the X Window System). Adobe Illustrator, Corel Draw, OpenOffice Draw, and a number of other

graphics tools support SVG images. Import the image using the Layout Backgrounds page. The image files are stored in a database and are accessible from any appliance on the network.

To import an image, perform the following steps:

- 1 Choose **Application > Layout Backgrounds**.
- 2 Click **Browse** to locate the image file to upload. Be sure the appropriate file extension is included in the file name.
- 3 Click **Upload**.



Binary images should not exceed 12 MB in size, and other images should not exceed 16 MB.

The uploaded file, as well as any other layout background files that have been uploaded, appears in the **Image Name** column, along with the type of image file. You can preview the image by clicking **View**.

- 4 To delete any of the uploaded background image files, check the corresponding check box, and then click **Delete**.

If a background image is in use, a green star appears in the **Delete** column; the image cannot be deleted until it is removed from all routing topology map layouts.

- 5 To apply or remove a background image to or from the routing topology map layout, see “The Routing Topology Map” chapter in the *HP Route Analytics Management Software User’s Guide*.

Using Diagnostic Functions

The system supports the diagnostic functions ping and traceroute. Use these functions to investigate network failures or outages.

Pinging a Network Device

Use ping to determine if a destination host is reachable on the network.

To ping another network device, perform the following steps:

- 1 Choose **Administration > System Diagnostics**.
- 2 Enter the IP address or DNS name of the destination device.
- 3 Click **Ping**.

The System Diagnostics page displays the results of the ping function.

Running a Traceroute

Use traceroute to trace the path a packet takes through the network from the appliance to the destination you specify.

To run the traceroute function, perform the following steps:

- 1 Choose **Administration > System Diagnostics**.
- 2 Enter the IP address or DNS name of the destination device.
- 3 Click **Traceroute**.

The System Diagnostics page displays the results of the traceroute function.

Shutting Down

The system can be shut down at any time. The system shutdown options are displayed on the Shutdown page (Figure 57).

To access the Shutdown page, choose **Administration > Shutdown**.

The following options are available on the Shutdown page:

- **Reboot this system**—Click this button, and then click **Yes** to reboot the system. The VNC server and data recording are stopped, and the operating system and recording software are reloaded from the disk. The VNC server and recorders are automatically restarted using the previous system settings. The message “Please wait for the system to reboot then click on Home” should appear. If this message does not appear, wait three minutes, and then click **Home**. Log in to the Administration pages and verify that the VNC server and recorders are operating correctly.

Shutdown

Shutdown options

Reboot this system

Shutdown and power off

Reset to factory defaults and reboot

Reset to factory defaults and power off

Cancel

System uptime: 16 hours, 25 minutes

Figure 57 Shutdown Page

- **Shutdown and power off**—Click this button to shutdown the system and power off. A confirmation page appears. Click **Yes** to shutdown the system. The VNC server and data recording are stopped. To restart, press the power switch on the appliance.

- **Reset to factory defaults and reboot**—Click this button to restore the factory default settings and reboot the appliance. A confirmation page appears. Click **Yes** to reset the factory default settings and reboot the system. When the system reboots, use the serial console interface to reconfigure the network address and then connect to the Home page, and log-in as administrator. Restore the system configuration from a back-up file, or re-configure manually following the sequence of steps in [Applying License Keys](#) on page 28. If recording is enabled, verify on the Recorder Configuration page that Hellos and Events are being received from the monitored areas or levels.

If the factory settings are restored, the following information is lost:

- All configuration information, including Network, Route Recorder, user names and passwords.
- Data files, including databases, user time-series data files, and log files.

The current and alternate versions of the software and the installed licenses remain on the appliance.

- **Reset to factory defaults and power off**—Click this button to restore the factory default settings and power off the appliance. A confirmation page appears. Click **Yes** to reset the factory default settings and power off the system.

A Router Commands for the Collector

The Collector process uses SNMP, Telnet, and/or SSH to gather information on all topologies except EIGRP. (For EIGRP, the same interface parameters and static route information is collected using Telnet or SSH as part of acquiring the EIGRP topology.)

For instructions on configuring the Collector, refer to [Configuring the Route Recorder for the Collector](#) on page 73.

This appendix lists the following router commands:

- [Cisco IOS CLI Commands](#) on page 1
- [JunOSe CLI Commands](#) on page 2
- [JunOS CLI Commands \(Netconf/junoscript\)](#) on page 2

Cisco IOS CLI Commands

The following commands are used for the Cisco router configuration for the Collector.

```
terminal length 0
show inventory raw
show version
show ip route static
show ip route 0.0.0.0 255.255.255.255 longer-prefixes
show ip route connected
show snmp mib ifmib ifindex [ enable command ]
show interface
show ip interface show ip vrf detail
show route-map
show ip access-list
show ip prefix-list
```

```
show ip extcommunity-list
show ip community-list
show ip route vrf <vrf_name> static
show class-map
show policy-map
show policy-map interface
show table-map
```

JunOSe CLI Commands

The following commands are used for the Juniper router configuration for the Collector.

```
terminal length 0
show version
show ip route static | include Static
show ip route local | include Connect
show ip vrf detail
show ip interface vrf <vrf_name>
show ip route vrf <vrf_name> static | include Static
show ip route vrf <vrf_name> local | include Connect
show route-map
show access-list detail
show ip prefix-list
show ip prefix-tree
show ip community-list
show ip extcommunity-list
show ip route vrf <vrf_name> static | include Static
show ip route vrf <vrf_name> local | include Connect
show policy-list
show classifier-list detail
show mpls
```

JunOS CLI Commands (Netconf/junoscript)

```
Hello
```

```
<?xml version="1.0" encoding="UTF-8"?>
<hello>
<capabilities>
<capability>urn:ietf:params:xml:ns:netconf:base:1.0
</capability>
</capabilities>
</hello>
]]>]]>
```

Close

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="106"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<close-session/>
</rpc>
]]>]]>
```

get-software-information

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="113"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-software-information>
<brief/>
</get-software-information>
</rpc>
]]>]]>
```

get-chassis-inventory

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="113"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-chassis-inventory/>
</rpc>
]]>]]>
```

```
get-interface-information
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="113"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-interface-information/>
</rpc>
]]>]]>
```

get-iftype-query

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="113"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<walk-snmp-object>ifType</walk-snmp-object>
</rpc>
]]>]]>
```

get-static-route-query

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="113"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-route-information>
<terse/> // use "brief" for local
<table>inet.0</table>
<protocol>static</protocol> // static or direct or local
</get-route-information>
</rpc>
]]>]]>
```

get-vrf-info-query

```
<get-configuration database="committed"> //junoscript
<configuration>
<routing-instances/>
</configuration>
</get-configuration>
```



```
or
<?xml version="1.0" encoding="UTF-8"?> //netconf
<rpc message-id="111"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
<source><running/></source>
<filter type="subtree">
<configuration>
<routing-instances/>
</configuration>
</filter>
</get-config>
</rpc>
]]>]]>
```

get-policy-options-query

```
<get-configuration database="committed"> //junoscript
<configuration>
<policy-options/>
</configuration>
</get-configuration>
```

```
or
<?xml version="1.0" encoding="UTF-8"?> //netconf
<rpc message-id="111"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
<source><running/></source>
<filter type="subtree">
<configuration>
<policy-options/>
</configuration>
</filter>
</get-config>
</rpc>
]]>]]>
```

get-classifier-query

```
<get-configuration database="committed"> //junoscript
```

```

<configuration>
<firewall/>
</configuration>
</get-configuration>
or
<?xml version="1.0" encoding="UTF-8"?> //netconf
<rpc message-id="111"
xmlns="urn:iETF:params:xml:ns:netconf:base:1.0">
<get-config>
<source><running/></source>
<filter type="subtree">
<configuration>
<firewall/>
</configuration>
</filter>
</get-config>
</rpc>
]]>]]>

```

get-service-policy-query

```

<get-configuration database="committed">
<configuration>
<interfaces/>
</configuration>
</get-configuration>
or
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="111"
xmlns="urn:iETF:params:xml:ns:netconf:base:1.0">
<get-config>
<source><running/></source>
<filter type="subtree">
<configuration>
<interfaces/>
</configuration>
</filter>
</get-config>
</rpc>
]]>]]>

```

```
get-cos-info-query
```

```
<?xml version="1.0" encoding="UTF-8"?>  
<rpc message-id="113"  
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">  
<get-cos-information/>  
</rpc>  
]]>]]>
```


B SNMP MIBs

This appendix lists the SNMP MIBs:

- [SNMP MIBs Common to All Vendors](#) on page 1
- [Alcatel SNMP MIBs](#) on page 4

SNMP MIBs Common to All Vendors

IpAddressTable

```
"Snmpv2-SMI::mib-2.ip.ipAddrTable.ipAdEntAddr" =  
{1.3.6.1.2.1.4.20.1.1},  
  
"Snmpv2-SMI::mib-2.ip.ipAddrTable.ipAdEntIfIndex" =  
{1.3.6.1.2.1.4.20.1.2},  
  
"Snmpv2-SMI::mib-2.ip.ipAddrTable.ipAdEntNetMask" =  
{1.3.6.1.2.1.4.20.1.3},
```

InterfaceTable

```
"IF-MIB::ifIndex" = { 1.3.6.1.2.1.2.2.1.1},  
  
"IF-MIB::ifDescr" = { 1.3.6.1.2.1.2.2.1.2},  
  
"IF-MIB::ifType" = { 1.3.6.1.2.1.2.2.1.3},  
  
"IF-MIB::ifMtu" = { 1.3.6.1.2.1.2.2.1.4},  
  
"IF-MIB::ifSpeed" = { 1.3.6.1.2.1.2.2.1.5},
```

```
"IF-MIB::ifPhysAddress" = { 1.3.6.1.2.1.2.2.1.6},  
"IF-MIB::ifAdminStatus" = { 1.3.6.1.2.1.2.2.1.7},  
"IF-MIB::ifOperStatus" = { 1.3.6.1.2.1.2.2.1.8},
```

InterfaceIndex

```
"IF-MIB::ifIndex" = { 1.3.6.1.2.1.2.2.1.1},  
"IF-MIB::ifDescr" = { 1.3.6.1.2.1.2.2.1.2},
```

IfXTable

```
"IF-MIB::ifIndex" = { 1.3.6.1.2.1.2.2.1.1},  
"IF-MIB::ifHighSpeed" = { 1.3.6.1.2.1.31.1.1.1.15},
```

SysInfo

```
"Snmpv2-MIB::sysname" = {1.3.6.1.2.1.1.5.0},  
"Snmpv2-MIB::sysDescr" = {1.3.6.1.2.1.1.1.0},  
"Snmpv2-MIB::sysObjectID" = {1.3.6.1.2.1.1.2.0},
```

IpRouteTable

```
"RFC1213-MIB::ipRouteDest" = { 1.3.6.1.2.1.4.21.1.1},  
"RFC1213-MIB::ipRouteMask" = { 1.3.6.1.2.1.4.21.1.11},  
"RFC1213-MIB::ipRouteNextHop" = { 1.3.6.1.2.1.4.21.1.7},  
"RFC1213-MIB::ipRouteType" = { 1.3.6.1.2.1.4.21.1.8},  
"RFC1213-MIB::ipRouteProto" = { 1.3.6.1.2.1.4.21.1.9},
```

```
"RFC1213-MIB::ipRouteIfIndex" = { 1.3.6.1.2.1.4.21.1.2},  
"RFC1213-MIB::ipRouteMetric1" = { 1.3.6.1.2.1.4.21.1.3},
```

IpForwardTable

```
"ipForwardDest" = { 1.3.6.1.2.1.4.24.2.1.1},  
"ipForwardMask" = { 1.3.6.1.2.1.4.24.2.1.2},  
"ipForwardNextHop" = { 1.3.6.1.2.1.4.24.2.1.4},  
"ipForwardType" = { 1.3.6.1.2.1.4.24.2.1.6},  
"ipForwardProto" = { 1.3.6.1.2.1.4.24.2.1.7},  
"ipForwardIfIndex" = { 1.3.6.1.2.1.4.24.2.1.5},  
"ipForwardMetric1" = { 1.3.6.1.2.1.4.24.2.1.11},
```

IpCidrRouteTable

```
"ipCidrRouteDest" = { 1.3.6.1.2.1.4.24.4.1.1},  
"ipCidrRouteMask" = { 1.3.6.1.2.1.4.24.4.1.2},  
"ipCidrRouteNextHop" = { 1.3.6.1.2.1.4.24.4.1.4},  
"ipCidrRouteType" = { 1.3.6.1.2.1.4.24.4.1.6},  
"ipCidrRouteProto" = { 1.3.6.1.2.1.4.24.4.1.7},  
"ipCidrRouteIfIndex" = { 1.3.6.1.2.1.4.24.4.1.5},  
"ipCidrRouteMetric1" = { 1.3.6.1.2.1.4.24.4.1.11},
```

InetCidrRouteTable

```
"inetCidrRouteDest" = { 1.3.6.1.2.1.4.24.7.2 },
```

```
"inetCidrRoutePfxLen" = { 1.3.6.1.2.1.4.24.7.3 },
"inetCidrRouteNextHop" = { 1.3.6.1.2.1.4.24.7.6 },
"inetCidrRouteType" = { 1.3.6.1.2.1.4.24.7.8 },
"inetCidrRouteProto" = { 1.3.6.1.2.1.4.24.7.9 },
"inetCidrRouteIfIndex" = { 1.3.6.1.2.1.4.24.7.7 },
"inetCidrRouteMetric1" = { 1.3.6.1.2.1.4.24.7.12 },
```

Alcatel SNMP MIBs

AlcatelVrtrConfTableInfoUnit

```
"vRtrRowStatus" = { 1.3.6.1.4.1.6527.3.1.2.3.1.1.2 },
"vRtrAdminState" = { 1.3.6.1.4.1.6527.3.1.2.3.1.1.3 },
"vRtrName" = { 1.3.6.1.4.1.6527.3.1.2.3.1.1.4 },
"vRtrDescription" = { 1.3.6.1.4.1.6527.3.1.2.3.1.1.25 },
"vRtrRouteDistinguisher" = { 1.3.6.1.4.1.6527.3.1.2.3.1.1.19
},
"vRtrVpnId" = { 1.3.6.1.4.1.6527.3.1.2.3.1.1.23 },
"vRtrVrfTarget" = { 1.3.6.1.4.1.6527.3.1.2.3.1.1.33 },
"vRtrVrfExportTarget" = { 1.3.6.1.4.1.6527.3.1.2.3.1.1.34 },
"vRtrVrfImportTarget" = { 1.3.6.1.4.1.6527.3.1.2.3.1.1.35 },
"vRtrImportPolicy1" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.1 },
"vRtrImportPolicy2" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.2 },
```


"vRtrImportPolicy3" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.3 },
"vRtrImportPolicy4" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.4 },
"vRtrImportPolicy5" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.5 },
"vRtrExportPolicy1" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.6 },
"vRtrExportPolicy2" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.7 },
"vRtrExportPolicy3" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.8 },
"vRtrExportPolicy4" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.9 },
"vRtrExportPolicy5" = { 1.3.6.1.4.1.6527.3.1.2.3.16.1.10 },

AlcatelVrtrIfTableInfoUnit

"vRtrIfRowStatus" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.2},
"vRtrIfType" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.3},
"vRtrIfName" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.4},
"vRtrIfPortId" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.5},
"vRtrIfEncapValue" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.7},
"vRtrIfAdminState" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.8},
"vRtrIfOperState" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.9},
"vRtrIfPhysicalAddress" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.11},
"vRtrIfMtu" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.25},
"vRtrIfQosPolicyId" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.26},
"vRtrIfDescription" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.34},

```
"vRtrIfServiceId" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.37},  
"vRtrIfGlobalIndex" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.63},  
"vRtrIfDelaySeconds" = {1.3.6.1.4.1.6527.3.1.2.3.4.1.64},
```

AlcatelVrtrIpAddrTableInfoUnit

```
"vRiaRowStatus" = {1.3.6.1.4.1.6527.3.1.2.3.6.1.2},  
"vRiaIpAddress" = {1.3.6.1.4.1.6527.3.1.2.3.6.1.3},  
"vRiaNetMask" = {1.3.6.1.4.1.6527.3.1.2.3.6.1.4},
```

AlcatelVrtrStaticRouteTableInfoUnit

```
"vRtrStaticRouteDest" = {1.3.6.1.4.1.6527.3.1.2.3.9.1.1},  
"vRtrStaticRouteMask" = {1.3.6.1.4.1.6527.3.1.2.3.9.1.2},  
"vRtrStaticRouteRowStatus" =  
{1.3.6.1.4.1.6527.3.1.2.3.9.1.4},  
"vRtrStaticRouteStaticType" =  
{1.3.6.1.4.1.6527.3.1.2.3.9.1.7},  
"vRtrStaticRouteMetric" = {1.3.6.1.4.1.6527.3.1.2.3.9.1.9},  
"vRtrStaticRouteNextHop" = {1.3.6.1.4.1.6527.3.1.2.3.9.1.12},
```

AlcatelDscpNameTableInfoUnit

```
"tDSCPNameRowStatus" = { 1.3.6.1.4.1.6527.3.1.2.16.1.1.1.2 },  
"tDSCPNameStorageType" = { 1.3.6.1.4.1.6527.3.1.2.16.1.1.1.3  
,  
"tDSCPNameDscpValue" = { 1.3.6.1.4.1.6527.3.1.2.16.1.1.1.4 },
```

```
"tDSCPNameLastChanged" = { 1.3.6.1.4.1.6527.3.1.2.16.1.1.1.5
},
```

AlcatelFCNameTableInfoUnit

```
"tFCRowStatus" = { 1.3.6.1.4.1.6527.3.1.2.16.2.1.1.2 },
"tFCStorageType" = { 1.3.6.1.4.1.6527.3.1.2.16.2.1.1.3 },
"tFCValue" = { 1.3.6.1.4.1.6527.3.1.2.16.2.1.1.4 },
"tFCNameLastChanged" = { 1.3.6.1.4.1.6527.3.1.2.16.2.1.1.5 },
```

AlcatelSapBaselInfoUnit

```
"sapRowStatus" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.3 },
"sapType" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.4 },
"sapDescription" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.5 },
"sapAdminStatus" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.6 },
"sapOperStatus" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.7 },
"sapIngressQosPolicyId" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.8
},
"sapEgressQosPolicyId" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.11
},
"sapIesIfIndex" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.15 },
"sapLastMgmtChange" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.16 },
"sapVpnId" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.19 },
"sapCustId" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.20 },
"sapOperFlags" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.27 },
```

```
"sapLastStatusChange" = { 1.3.6.1.4.1.6527.3.1.2.4.3.2.1.28 },
```

AlcatelSapIngressInfoUnit

```
"tSapIngressRowStatus" = { 1.3.6.1.4.1.6527.3.1.2.16.3.1.1.2  
,
```

```
"tSapIngressScope" = { 1.3.6.1.4.1.6527.3.1.2.16.3.1.1.3 },
```

```
"tSapIngressDescription" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.1.1.4 },
```

```
"tSapIngressDefaultFC" = { 1.3.6.1.4.1.6527.3.1.2.16.3.1.1.5  
,
```

```
"tSapIngressDefaultFCPriority" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.1.1.6 },
```

```
"tSapIngressMatchCriteria" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.1.1.7 },
```

```
"tSapIngressLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.1.1.8 },
```

AlcatelSapIngressDscplInfoUnit

```
"tSapIngressDscplRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.3.1.2 },
```

```
"tSapIngressDscplFC" = { 1.3.6.1.4.1.6527.3.1.2.16.3.3.1.3 },
```

```
"tSapIngressDscplPriority" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.3.1.4 },
```

```
"tSapIngressDscplLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.3.1.5 },
```

AlcatelSapIngressIPCriteriaInfoUnit

```
"tSapIngressIPCriteriaRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.2 },
```

```
"tSapIngressIPCriteriaDescription" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.3 },

"tSapIngressIPCriteriaActionFC" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.4 },

"tSapIngressIPCriteriaActionPriority" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.5 },

"tSapIngressIPCriteriaSourceIpAddr" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.6 },

"tSapIngressIPCriteriaSourceIpMask" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.7 },

"tSapIngressIPCriteriaDestIpAddr" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.8 },

"tSapIngressIPCriteriaDestIpMask" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.9 },

"tSapIngressIPCriteriaProtocol" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.10 },

"tSapIngressIPCriteriaSourcePortValue1" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.11 },

"tSapIngressIPCriteriaSourcePortValue2" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.12 },

"tSapIngressIPCriteriaSourcePortOperator" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.13 },

"tSapIngressIPCriteriaDestPortValue1" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.14 },

"tSapIngressIPCriteriaDestPortValue2" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.15 },

"tSapIngressIPCriteriaDestPortOperator" = {
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.16 },
```

```
"tSapIngressIPCriteriaDSCP" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.17 },  
  
"tSapIngressIPCriteriaLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.5.1.19 },
```

AlcatelSapIngressFCInfoUnit

```
"tSapIngressFCRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.7.1.2 },  
  
"tSapIngressFCLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.7.1.7 },  
  
"tSapIngressFCInProfRemark" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.7.1.8 },  
  
"tSapIngressFCInProfDscp" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.7.1.9 },  
  
"tSapIngressFCInProfPrec" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.7.1.10 },  
  
"tSapIngressFCOutProfRemark" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.7.1.11 },  
  
"tSapIngressFCOutProfDscp" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.7.1.12 },  
  
"tSapIngressFCOutProfPrec" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.7.1.13 },  
  
"tSapIngressFCProfile" = { 1.3.6.1.4.1.6527.3.1.2.16.3.7.1.14  
},
```

AlcatelSapIngressPrecInfoUnit

```
"tSapIngressPrecRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.8.1.2 },  
  
"tSapIngressPrecFC" = { 1.3.6.1.4.1.6527.3.1.2.16.3.8.1.3 },  
  
"tSapIngressPrecFCPriority" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.8.1.4 },  
  
"tSapIngressPrecLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.3.8.1.5 },
```

AlcatelSapEgressInfoUnit

```
"tSapEgressRowStatus" = { 1.3.6.1.4.1.6527.3.1.2.16.4.1.1.2 },  
  
"tSapEgressScope" = { 1.3.6.1.4.1.6527.3.1.2.16.4.1.1.3 },  
  
"tSapEgressDescription" = { 1.3.6.1.4.1.6527.3.1.2.16.4.1.1.4  
},  
  
"tSapEgressLastChanged" = { 1.3.6.1.4.1.6527.3.1.2.16.4.1.1.5  
},  
  
"tSapEgressMatchCriteria" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.1.1.7 },
```

AlcatelSapEgressFCInfoUnit

```
"tSapEgressFCRowStatus" = { 1.3.6.1.4.1.6527.3.1.2.16.4.3.1.2  
},  
  
"tSapEgressFCLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.3.1.5 },  
  
"tSapEgressFCInProfDscp" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.3.1.12 },  
  
"tSapEgressFCOutProfDscp" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.3.1.13 },
```

```
"tSapEgressFCInProfPrec" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.3.1.14 },
```

```
"tSapEgressFCOutProfPrec" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.3.1.15 },
```

AlcatelSapEgressDscpInfoUnit

```
"tSapEgressDscpRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.5.1.2 },
```

```
"tSapEgressDscpLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.5.1.3 },
```

AlcatelSapEgressPrecInfoUnit

```
"tSapEgressPrecRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.6.1.2 },
```

```
"tSapEgressPrecLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.6.1.3 },
```

AlcatelSapEgrIPCritInfoUnit

```
"tSapEgrIPCritRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.3 },
```

```
"tSapEgrIPCritLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.4 },
```

```
"tSapEgrIPCritDescription" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.5 },
```

```
"tSapEgrIPCritSourceIpAddrType" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.7 },
```

```
"tSapEgrIPCritSourceIpAddr" = {  
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.8 },
```



```
"tSapEgrIPCritSourceIpMask" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.9 },

"tSapEgrIPCritDestIpAddrType" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.10 },

"tSapEgrIPCritDestIpAddr" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.11 },

"tSapEgrIPCritDestIpMask" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.12 },

"tSapEgrIPCritProtocol" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.13 },

"tSapEgrIPCritSourcePortValue1" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.14 },

"tSapEgrIPCritSourcePortValue2" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.15 },

"tSapEgrIPCritSourcePortOperator" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.16 },

"tSapEgrIPCritDestPortValue1" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.17 },

"tSapEgrIPCritDestPortValue2" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.18 },

"tSapEgrIPCritDestPortOperator" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.19 },

"tSapEgrIPCritDSCP" = { 1.3.6.1.4.1.6527.3.1.2.16.4.7.1.20 },

"tSapEgrIPCritFragment" = {
1.3.6.1.4.1.6527.3.1.2.16.4.7.1.21 },
```

AlcatelNetworkPolicyInfoUnit

```
"tNetworkPolicyRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.1.1.2 },  
  
"tNetworkPolicyScope" = { 1.3.6.1.4.1.6527.3.1.2.16.5.1.1.5 },  
  
"tNetworkPolicyDescription" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.1.1.6 },  
  
"tNetworkPolicyIngressDefaultActionFC" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.1.1.7 },  
  
"tNetworkPolicyIngressDefaultActionProfile" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.1.1.8 },  
  
"tNetworkPolicyEgressRemark" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.1.1.9 },  
  
"tNetworkPolicyLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.1.1.10 },  
  
"tNetworkPolicyIngressLerUseDscp" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.1.1.11 },
```

AlcatelNetworkIngressDscpInfoUnit

```
"tNetworkIngressDscpRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.2.1.2 },  
  
"tNetworkIngressDscpFC" = { 1.3.6.1.4.1.6527.3.1.2.16.5.2.1.3  
,  
  
"tNetworkIngressDscpProfile" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.2.1.4 },  
  
"tNetworkIngressDscpLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.2.1.5 },
```

AlcatelNetworkIngressLspExpInfoUnit

```
"tNetworkIngressLspExpRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.4.1.2 },  
  
"tNetworkIngressLspExpFC" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.4.1.3 },  
  
"tNetworkIngressLspExpProfile" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.4.1.4 },  
  
"tNetworkIngressLspExpLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.4.1.5 },
```

AlcatelNetworkEgressFCInfoUnit

```
"tNetworkEgressFCDscpInProfile" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.7.1.2 },  
  
"tNetworkEgressFCDscpOutProfile" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.7.1.3 },  
  
"tNetworkEgressFCLspExpInProfile" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.7.1.4 },  
  
"tNetworkEgressFCLspExpOutProfile" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.7.1.5 },  
  
"tNetworkEgressFCDot1pInProfile" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.7.1.6 },  
  
"tNetworkEgressFCDot1pOutProfile" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.7.1.7 },  
  
"tNetworkEgressFCLastChanged" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.7.1.8 },  
  
"tNetworkEgressFCForceDEValue" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.7.1.9 },
```

```
"tNetworkEgressFCDEMark" = {  
1.3.6.1.4.1.6527.3.1.2.16.5.7.1.10 },
```

AlcatelRPOperASPathInfoUnit

```
"tRPOperASPathRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.17.1.1.2.1.2},
```

```
"tRPOperASPathRegEx" = {  
1.3.6.1.4.1.6527.3.1.2.17.1.1.2.1.3},
```

AlcatelRPOperCommunityInfoUnit

```
"tRPOperCommunityRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.17.1.1.4.1.3},
```

AlcatelRPOperPrefixListInfoUnit

```
"tRPOperPrefixListRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.17.1.1.8.1.4},
```

```
"tRPOperPrefixListThroughLength" = {  
1.3.6.1.4.1.6527.3.1.2.17.1.1.8.1.6},
```

```
"tRPOperPrefixListBeginLength" = {  
1.3.6.1.4.1.6527.3.1.2.17.1.1.8.1.8},
```

AlcatelRPOperPolicyStmt

```
"tRPOperPolicyStatementRowStatus" = {  
1.3.6.1.4.1.6527.3.1.2.17.1.1.10.1.2},
```

```
"tRPOperPolicyStatementDescription" = {  
1.3.6.1.4.1.6527.3.1.2.17.1.1.10.1.3},
```

```
"tRPOperPolicyStatementDefaultAction" = {  
1.3.6.1.4.1.6527.3.1.2.17.1.1.10.1.4},
```

AlcatelRPOperPSParams

```
"trPOperPSParamsRowStatus" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.14.1.2},

"trPOperPSParamsDescription" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.14.1.3},

"trPOperPSParamsAction" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.14.1.4},
```

AlcatelRPOperPSFromCriteria

```
"trPOperPSFromCriteriaRowStatus" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.2},

"trPOperPSFromCriteriaProtocol" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.3},

"trPOperPSFromCriteriaNeighborIpAddr" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.4},

"trPOperPSFromCriteriaNeighborPrefixList" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.5},

"trPOperPSFromCriteriaPrefixList1" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.6},

"trPOperPSFromCriteriaPrefixList2" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.7},

"trPOperPSFromCriteriaPrefixList3" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.8},

"trPOperPSFromCriteriaPrefixList4" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.9},

"trPOperPSFromCriteriaPrefixList5" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.10},
```

```
"tRPOperPSFromCriteriaASPath" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.11},

"tRPOperPSFromCriteriaCommunity" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.12},

"tRPOperPSFromCriteriaOrigin" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.13},

"tRPOperPSFromCriteriaTag" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.24},

"tRPOperPSFromCritNbrInetAddrType" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.25},

"tRPOperPSFromCritNbrInetAddr" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.26},

"tRPOperPSFromCriteriaFamily" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.29},

"tRPOperPSFromCriteriaInstanceId" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.20.1.30},
```

AlcatelIRPOperPSToCriteriaTableInfoUnit

```
"tRPOperPSToCriteriaRowStatus" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.2 },

"tRPOperPSToCriteriaProtocol" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.3 },

"tRPOperPSToCriteriaNeighborIpAddr" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.4 },

"tRPOperPSToCriteriaNeighborPrefixList" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.5 },

"tRPOperPSToCriteriaPrefixList1" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.8 },
```

```
"tRPOperPSToCriteriaPrefixList2" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.9 },

"tRPOperPSToCriteriaPrefixList3" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.10 },

"tRPOperPSToCriteriaPrefixList4" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.11 },

"tRPOperPSToCriteriaPrefixList5" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.12 },

"tRPOperPSToCritNbrInetAddrType" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.13 },

"tRPOperPSToCritNbrInetAddr" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.14 },

"tRPOperPSToCriteriaInstanceId" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.18.1.15 },
```

AlcatelRPOperPSDefaultActionParamsTableInfoUnit

```
"tRPOperPSDefaultActionASPath" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.1 },

"tRPOperPSDefaultActionASPathName" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.2 },

"tRPOperPSDefaultActionASPathPrependAS" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.3 },

"tRPOperPSDefaultActionASPathPrependCount" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.4 },

"tRPOperPSDefaultActionCommunity1" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.5 },

"tRPOperPSDefaultActionCommunityName1" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.6 },
```

```
"tRPOperPSDefaultActionCommunity2" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.7 },

"tRPOperPSDefaultActionCommunityName2" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.8 },

"tRPOperPSDefaultActionOrigin" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.9 },

"tRPOperPSDefaultActionLocalPreferenceSet" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.10 },

"tRPOperPSDefaultActionLocalPreference" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.11 },

"tRPOperPSDefaultActionMetric" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.12 },

"tRPOperPSDefaultActionMetricValue" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.13 },

"tRPOperPSDefaultActionPreference" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.15 },

"tRPOperPSDefaultActionNextHopSelf" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.17 },

"tRPOperPSDefaultActionNextHop" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.18 },

"tRPOperPSDefaultActionTag" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.19 },

"tRPOperPSDefaultActionOspfType" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.20 },

"tRPOperPSDefActInetNextHopType" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.22 },

"tRPOperPSDefActInetNextHop" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.12.1.23 },
```


AlcatelRPOperPSAcceptActionParamsTableInfoUnit

```
"trPOperPSAcceptActionASPath" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.1 },

"trPOperPSAcceptActionASPathName" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.2 },

"trPOperPSAcceptActionASPathPrependAS" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.3 },

"trPOperPSAcceptActionASPathPrependCount" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.4 },

"trPOperPSAcceptActionCommunity1" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.5 },

"trPOperPSAcceptActionCommunityName1" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.6 },

"trPOperPSAcceptActionCommunity2" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.7 },

"trPOperPSAcceptActionCommunityName2" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.8 },

"trPOperPSAcceptActionOrigin" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.9 },

"trPOperPSAcceptActionLocalPreferenceSet" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.10 },

"trPOperPSAcceptActionLocalPreference" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.11 },

"trPOperPSAcceptActionMetric" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.12 },
```

```
"tRPOperPSAcceptActionMetricValue" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.13 },

"tRPOperPSAcceptActionPreference" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.15 },

"tRPOperPSAcceptActionNextHopSelf" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.17 },

"tRPOperPSAcceptActionNextHop" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.18 },

"tRPOperPSAcceptActionTag" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.19 },

"tRPOperPSAcceptActionOspfType" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.20 },

"tRPOperPSAcptActInetNextHopType" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.22 },

"tRPOperPSAcptActInetNextHop" = {
1.3.6.1.4.1.6527.3.1.2.17.1.1.16.1.23 },
```

C License Feature Details

This appendix describes the license features associated with Route Analytics Management Software. For information on how to apply license features to an appliance, see [Chapter 2, “Configuration and Management”](#)

Each license includes an expiration date, or “--” for a permanent license. In a typical installation, all licenses will show the same expiration date. However, if you purchase an incremental license, that license will have a different expiration date. A license with a short-duration expiration date is often provided during product evaluations. When the license expires, data recording is disabled, protocol configuration is disabled, and a warning message is displayed.

Table 3 Available License Features

Feature Name	Description
Protocol Licenses	Required for an appliance to monitor particular protocols. If the license for a given protocol (OSPF, IS-IS, EIGRP, BGP, or MPLS VPN) is not enabled, an instance of that protocol cannot be created on the <i>Recorder Configuration</i> page. If you attempt to add or edit a protocol instance that does not have a license, you will receive an error message indicating the lack of license.
Route Recorder	Required for an appliance to act as a Route Recorder, which stores information obtained from the licensed routing protocols (OSPF, IS-IS, EIGRP, BGP, or MPLS VPN).
Flow Collector	Required for an appliance to collect traffic flow data, which is then analyzed by the Flow Analyzer. (RAMS Traffic only)
Flow Analyzer	Required for an appliance to generate reports using data collected from Flow Collectors and Route Recorders. (RAMS Traffic only)

Table 3 Available License Features (cont'd)

Feature Name	Description
GUI	Required for an appliance to accept s or X Window System connections to display the graphical user interface.
MPLS VPN	Required for network service providers to collect the VPN-IPv4 prefixes for all of their VPN customers. Enables features to make sure that the prefixes are correctly distributed among a given customer's sites and do not leak between customers.
MPLS WAN	Required for an appliance to support enterprises that have multiple sites that are connected by a WAN through ISPs that use MPLS within their own networks.
RAMS Traffic SPI	Applied to the Modeling Engine to enable viewing of traffic and routing data and traffic reports.
Route Analyzer Alerts and Reports	Required for an appliance to act as a Route Analyzer. Route Analyzer generates reports using data collected from Route Recorders. The licenses for Alerts and Reports are typically enabled in an appliance that is configured as a Route Recorder.
VPN Customer Reports	Enables generation of per-customer traffic report data for your customers if you are a VPN service provider. This requires a system system with a MPLS-VPN license.
Database Server	Required for an appliance that records data to act as a database server. Machines that are configured to act as database clients can connect to this machine.
Database Client	Required for an appliance to act as a database client which can then connect to a database server.
Master Capability	Required for an appliance to be designated as the master appliance in a distributed configuration environment. The master is then used to configure a set of clients.

Table 3 Available License Features (cont'd)

Feature Name	Description
Router Count	Sets the number of routers you are able to monitor. When the number of routers you are monitoring exceeds the number of routers allowed by the license, a warning message is displayed. Sets the number of routers you are able to monitor. When the number of routers you are monitoring exceeds the number of routers allowed by the license, the system displays a warning message. If you exceed the number by more than 10, then the Open Topology operation in the GUI will abort unless you select a subset of the databases containing a smaller number of routers.
MPLS VPN Prefix Count	Sets the number of VPN prefixes you are able to monitor. If you exceed the number supported by the license, a warning message is displayed. Count Sets the number of VPN prefixes you are able to monitor. If you exceed the number supported by the license, a warning message is displayed. If you exceed the number by more than 10%, then the Open Topology operation in the GUI will abort unless you deselect all VPN databases.
Software Update	Indicates whether the appliance can obtain software updates from HP. Software Update is enabled with all licenses, including the temporary license that can be activated on a new appliance. HP provides software updates for <major number>.<minor number> versions of the software (for example, version 6.0) using the Software Update feature.

Index

A

- add
 - client, 35
- adding clients, considerations for, 34
- administration interface, selecting, 41
- Administration pages, 21, 109
 - logging in, 23
- administrative domain
 - creating, 53
 - deleting, 83
 - top-level, 53
- administrator default user name and password, 24
- Administrator password
 - changing, 26
- Administrators, 111
- alias
 - BGP AS, 68
 - interface, 42
- Analysis mode, 19
- appliance
 - reboot, 178
 - reset, 179
 - shutdown, 178
- application interface, 19
- Archival Configuration and Remote Storage page, 154

- archiving, 153
 - automatic, 153
 - configuration, 154
 - enable, 155
 - end time, 157
 - filename format, 156
 - frequency of, 153
 - manual, 156
 - restoring data, 157
 - start time, 157
- areas
 - contiguous, 61
 - multiple, 61
- AS
 - BGP, 68
 - configuring for EIGRP protocol instance, 66
- authentication
 - local, 113
 - MD5, 104
 - OSPF, 84, 104
 - type, 114
 - user, 24
- autonomous system
 - see AS

B

- backing up
 - client unit, 145
 - master appliance, 147
- Backup and Restore page, 134

- backup file
 - creating, 134, 137
 - deleting, 141
 - downloading, 139
 - FTP, 145
 - restoring, 140
 - restoring from remote server, 143
 - saving, 139
 - transferring, 145
 - uploading, 139
- backup on unit's disk, 136
- BGP
 - aliases, AS, 68
 - autonomous system (AS), 68
 - configuring, 68
 - protocol
 - instances, 68
- BGP Reports, 20
- browsers
 - Firefox, 22
 - Safari, 22
 - supported, 22
- button
 - Make Master, 34
 - Re-apply All, 32
 - Relinquish Master Role, 37, 38
 - Remove all licenses on this unit, 32
 - Restore Now, 158

C

- CA
 - CSR, 47
- callback, enable, 106
- Cisco router loopback interface, 105
- CLI Access, 111
- CLI Access users, 111

- client, 22
 - adding, 34
 - removing, 37
- client list, 34
- client unit
 - backing up, 145
- clock
 - setting, 27
- Collector
 - configuring, 73
 - router commands, 1
- components
 - data flow, 14
- configuration
 - additional tasks, 98
 - administration interface, 41
 - BGP, 68
 - client, 22
 - database
 - deleting, 131
 - renaming, 133
 - DHCP, 41
 - Flow Analyzer, 95
 - Flow Collector, 85
 - for recording, 51
 - FTP server, 171, 172
 - GRE tunnels, 101
 - hierarchy, 52, 53
 - hostname, 40
 - loopback interface, 105
 - master, 22
 - option card, 45
 - Route Recorder, 51, 69
 - static route, 43
 - support access, 106
 - traffic instance, 86
 - tree, 52
 - users, 26
 - VNC, 125

considerations for, 45

cookies, 23

CoS groups, 120

CSR

CA request, 47

obtaining and installing, 47

D

daily reports

creating, 165

scheduling, 167

understanding contents, 168

viewing saved, 170

database

administration page, 129

archiving, 155

backing up, 134

deleting, 131

deleting and start recording to new, 132

online vs. offline, 131

renaming, 133, 158

restored filename, 159

restoring, 134

restoring archived, 157

unarchived, 155

using offline, 131

using online, 133

Database Client, 24

Database Server, 24

Data Configuration page, 151

data source

choosing, 151

default, factory, 178

DHCP, 41

diagnostics, 176

ping, 176

traceroute, 177

distributed configuration

applying license keys, 29

archival settings for, 155

archiving data for, 154

choosing data source for, 150

configuring route recorder in, 18

deleting a database within, 131

designating master and client roles for,
32

IGP and BGP reports for, 20

updating software for, 159

updating software with internet access
for, 161

updating software without internet
access, 163

distributed configuration

description, 21

DNS

server, 41

downloading

software updates, 159

E

EIGRP

multiple areas, ASs, 61

multiple interfaces, coverage and, 63

protocol instance, configuring ASs, 61

enable archival, 155

export

log, 175

F

factory defaults, 178

features, 11

filename, restored database, 159

Firefox, 22

- Flow Analyzer, 14, 32, 96, 23
 - configuration, 95
 - starting and stopping, 96

- Flow Collector, 13, 32, 23
 - configuration, 85
 - starting and stopping, 89

- flow fanout, 172

FTP

- file transfer, 172
- file upload, enabling, 172
- file uploads, 172
- server configuration, 171, 172

G

- GRE tunnels, 14, 101

- Guests, 111

H

- hierarchy
 - configuration, 52, 53

- History Navigator, 19

- Home page, 22

- HTTP POST, 33

I

- ICMP redirects, 44

- IGP Reports, 20

- image, importing
 - importing
 - background image, 176

- interface
 - administration, 41
 - alias, 42
 - application, 19
 - removing from protocol instance, 83
 - VLAN, 42
 - web, 21

- Internet Explorer, 22

- IP address, 41
 - before you change on a system, 40

K

- keys, license, 23

L

- layout
 - uploading backgrounds
 - backgrounds, 175

- LDP, in IPv4 deployments, 88

- LDP peering sessions
 - establishing, 85

- license
 - applying, 28
 - install new key, 30
 - key, 28
 - remove all, 32
 - updating licenses, 28

- license key, 23
 - database client, 24
 - database server, 24
 - flow analyzer, 23
 - flow collector, 23
 - master capability, 24
 - Modeling Engine, 24
 - MPLS VPN prefix count, 25
 - MPLS WAN, 24
 - protocol, 23
 - route analyzer, 24
 - router count, 25
 - Route Recorder and GUI, 23
 - software update, 25
 - VPN customer reports, 24
- license reapplying, 28
- list
 - client, 34
- local authentication, 113
- log
 - export as plain text, 175
 - viewing, 174
- logging in, 24
- login attributes, 116
- login page, 24
- loopback
 - interface, 65, 105
 - interface, on Cisco router, 105

M

- Mail page, 165
- mail system
 - configuring, 167
- map
 - Routing Topology, 19

- master, 22
 - assigning, 33
 - assigning appliance as master, 21
 - license key, 24
 - relinquish, 37
 - removing client, 37
- master appliance
 - backing up, 147
 - relinquishing master status, 37
- Master Capability, 24
- master-client shared secret, 33
- MD5 authentication, 104
- mode
 - Analysis, 19
 - Monitoring, 19
 - Planning, 19
- Modeling Engine
 - adding an additional, 36
 - as master appliance, 21
 - description, 14
 - in distributed configuration, 32
 - license key, 24
- Monitoring mode, 19
- MPLS VAN WAN site, 56
- MPLS VPN
 - deployments, 85
- MPLS VPN Prefix Count, 25
- multiple port options, 45

N

- NetFlow
 - and flow fanout, 172
 - and recording, 13
- network
 - configuration, 39
 - DHCP, 40
- Network & Interface Configuration page, 39

NTP server, 26, 27

O

online/offline databases, 131

Operators, 111

option cards, configuring, 45

OSPF

- area ID format, 82

- authentication, 84, 104

- contiguous areas, 59

- loopback interface, 65

overwrite layouts, 140, 144, 149

P

password

- master-client shared secret, 33

Path Reports, 20

ping, 176

Planning mode, 19

Planning Reports window, 20

prefix source, defined, 88

previous version, revert to, 164

privileges, 115

protocol

- BGP, 68

- instance, deleting, 83

- instance, VPN, 71

- license keys, 23

- link-state, 12

- supported, 13

Protocol Licenses, 23

Q

queries, configuring server, 75

query server, 75

R

RADIUS Server, 113

RAMS

- components of, 13

- reverting to previous version, 164

- web server, 22

re-apply all, 32

reboot, 178

rebooting the system, 178

recorder

- NetFlow, 13

- routing, 13

Recorder Configuration page, 51

recording, configuration, 51

remote server, adding, 141

remove all licenses, 32

replacing

- client unit, 145

- master appliance, 147

reports

- and mail, 167

- BGP, 20

- daily, 165

- deleting instance, 97

- IGP, 20

- Path, 20

- Planning, 20

- scheduling daily, 167

- Traffic, 20

- using top N, 169

reset to factory defaults, 179

restore

- archived data, 157

- databases, 157

- from backup on unit's disk, 136

revert to previous version, 164

- route
 - static, configuring, 43

- Route Analyzer, 24

- router
 - count, 25
 - login for EIGRP, 67

- router commands
 - Cisco IOS, 1
 - for Collector, 1
 - JunOS CLI, 2
 - JunOSe, 2

- Router Count, 25

- Route Recorder, 13, 32
 - Collector, 73
 - configuration page, 51

- Route Recorder and GUI license, 23

- route reflectors, 69

- Router Recorder
 - starting and stopping, 81

- Routing Topology Map, 19

S

- Safari, 22

- server
 - database, 24
 - DNS, 41
 - FTP, 171, 172
 - NTP, 26, 27
 - remote, 141
 - VNC, 125

- SFTP, as alternative to FTP, 171

- shutdown
 - options, 178
 - page, 178

- site, MPLS VPN WAN, 56

- SMB, enabling, 141

- SNMP, 80
 - Agent configuration, 46
 - and the Collector, 73

- software
 - reinstalling previous version, 164
 - updating, 25

- Software Update
 - license, 25
 - page, 159

- SSH, 43, 67, 106, 111

- SSL certificate
 - and CSR, 47

- static information collection, 75

- static route, 44
 - adding, 44

- static route, configuration, 43

- static route information, 73

- status table, 90

- support access, configuring, 106

- supported, 176

- system
 - reboot, 178
 - shutdown, 178

- System Diagnostics page, 176

- system settings, viewing, 50

T

- TACACS, 67

- TACACS+
 - class of users, 111

- TACACS Server, 113

- time
 - setting, 26, 27

- time and date
 - synchronizing with NTP server, 26

- Time and Date page, 26
- top N reports, 169
- topology
 - map, 19
- traceroute, 177
- traffic
 - configuration status, 90
 - deleting instance, 94
 - instance, 86
- Traffic Groups
 - creating, 117
- traffic groups
 - creating, 117
 - editing, 120
- Traffic Reports, 20
- tree, configuration, 52
- tunnels
 - GRE, 14, 101
- U**
- Units page, 34
- updating software, 159
- upload
 - FTP, 172
- User accounts, updating existing, 116
- User Administration page, 26
- user interface
 - application, 19
 - web, 17
- user name and password, default, 24
- User privileges, 111

- users
 - adding, 26
 - CLI access class, 111
 - creating accounts, 115
 - login attributes, 116
 - privileges, 115
 - updating accounts, 116
- uses of by the appliance, 41

V

- v3 profiles, configuring, 80
- View Configuration page, 50
- viewer, 17
 - VNC
 - recommended use of, 25
 - X Window System
 - recommended use of, 25
- visibility of, 44
- VLAN
 - interface, 42
- VLAN, configuring interface, 42
- VNC, 17, 25
 - configuration, 125
 - connecting to persistent session, 127
 - on-demand sessions, 128
 - server, 125
 - start, stop server, 125
 - viewer, 127

W

- web browser
 - supported
 - browsers
 - Internet Explorer, 22
- web browser, cookies, 23
- web interface, 17, 21
- web server, 22

X

X Window System, 17, 25
evaluation license, 25

