

HP Route Analytics Management System

Software Version 8.10

Administrator Guide

Manufacturing Part Number: T9424-90006

Document Release Date: December 2008

Software Release Date: December 2008



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 1999–2008 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	9
	Route Analytics Management System Operation	10
	Key Components of Route Analytics Management System	10
	Using Route Analytics Management System	14
	The Web Interface	14
	The Application Interface	15
2	Configuration and Management	19
	Configuration Overview	19
	Connecting to the Home Page	20
	Logging In	22
	Applying License Keys	24
	Setting the Time and Date	28
	Designating the Master and Clients	30
	Assigning the Master Role to a RAMS Appliance	31
	Adding Clients to the Configuration	33
	Adding a Second Modeling Engine to the Configuration	34
	Relinquishing the Master Status	35
	Configuring the Network Interfaces	36
	Selecting the Administration Interface	39
	Configuring an Alias Interface	39
	Configuring a Static Route	40
	Configuring Multiple Port Options	41
	Configuring SNMP Agent security	42
	Viewing System Settings	43
	Configuring RAMS for Recording	43
	Creating a Configuration Hierarchy	44
	Configuring the Route Recorder	47

Adding Protocol Instances	48
Interconnection of BGP and IGP Protocol Instances	51
Configuring a BGP Confederation	52
Configuring Multiple EIGRP Autonomous Systems	52
Configure an IGP Instance	53
Configure a BGP Instance	59
Configuring the Route Recorder for Static Information Collection	64
Configuring SNMP v3 Profiles	68
Starting and Stopping the Route Recorder	70
Viewing and Modifying Route Recorder Settings	70
Changing the Area ID Format of an OSPF Protocol Instance	71
Deleting an Existing Domain or Protocol Instance	72
Removing an Interface from a Protocol Instance	72
Changing an OSPF Authentication Password	73
Deleting an OSPF Authentication Password	73
Configuring the Flow Collector	74
Starting and Stopping the Flow Collectors	77
Viewing Flow Collector Settings	78
Configuring Flow Analyzer Recording Status	83
Starting and Stopping the Flow Analyzer	84
Viewing Status of the Flow Analyzer	84
Deleting a Flow Analyzer	85
Additional Configuration Tasks	86
Configuring MPLS VPN-Aware LDP for Cisco Routers	86
Targeted LDP Configuration for Cisco Routers	86
Configuring MPLS-Aware NetFlow v9 on Cisco Routers	87
Configuring MPLS-Aware NetFlow v9 for Cisco Routers	87
Configuring GRE Tunnels	89
Configuring a Loopback Interface for Cisco Routers	93
Enabling Technical Support Access	93
3 Administration	95
Creating and Authenticating User Accounts	96
User Privileges	96
TACACS+ and RADIUS Parameters	97
TACACS+	97

RADIUS	98
User Administration Page	99
Selecting an Authentication Method	100
Creating New User Accounts	101
Updating an Existing Users Account	102
Update Login Attributes	103
Creating Traffic Groups	103
Editing Traffic Groups	107
Creating CoS Definitions	109
Configuring the VNC Server	112
Connecting to the VNC Persistent Session	114
Using On-Demand VNC Sessions	114
Managing Databases	115
Using Offline Databases	118
Deleting a Database	118
Renaming Databases	119
Using Online Databases	120
Backing Up and Restoring Data	120
Creating a Backup File	121
Saving a Backup File	125
Uploading a Backup File	126
Restoring a Backup File	127
Deleting a Backup File	128
Enabling SMB and Adding a Remote Server	128
Restoring a Backup File from a Remote Server	129
Transferring Backup Files Using FTP	131
Replacing Client and Master Appliances	131
Replacing a Client Appliance	131
Replacing a Master Appliance	133
Choosing a Data Source	136
Archiving Data	139
Configuring Automatic Archival Settings	140
Manually Archiving Data	141
Restoring Archived Data	142
Updating Software	144

Updating with Internet Access	145
Updating without Internet Access	147
Returning to a Previous Version	148
Using Top N Reports	149
Creating Daily Reports	151
Configuring the Mail System	152
Scheduling Daily Reports	154
Understanding Daily Report Contents	154
Viewing Saved Daily Reports	155
Configuring the FTP Server	155
Viewing and Exporting Log Pages	157
Uploading Layout Backgrounds	158
Using Diagnostic Functions	159
Pinging a Network Device	159
Running a Traceroute	160
Shutting Down	160
A License Feature Details	163
Index	167

1 Introduction

The Route Analytics Management System (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 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), IGP area, or BGP/MPLS 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 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 GUI-based reports for any recorded time period to obtain key information about network health.

Route Analytics Management System Operation

Route Analytics Management System 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 (OSPF or ISIS) 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 ISIS 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 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 System

RAMS includes 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, ISIS, BGP, and EIGRP) across multiple domains and ASs from a single appliance.

HP RAMS Flow Recorder—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 (DL380 G5 FC).

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 deployments, separate appliances should be installed for the Modeling Engine, Flow Analyzer, Flow Collectors, and Route Recorders.

With RAMS, 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 routing 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 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](#).

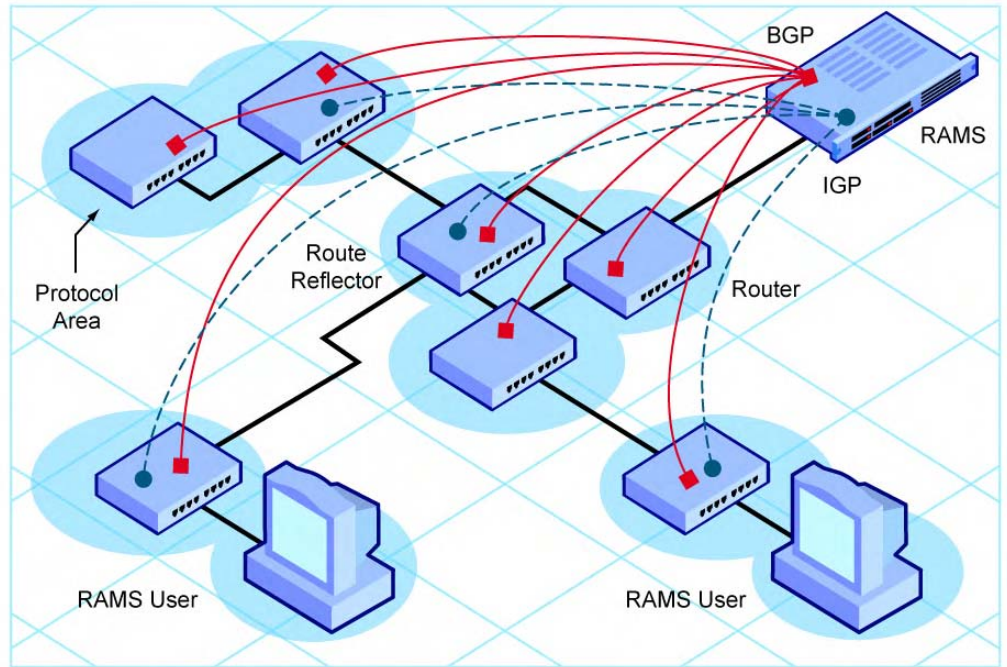


Figure 1 RAMS Data Flow

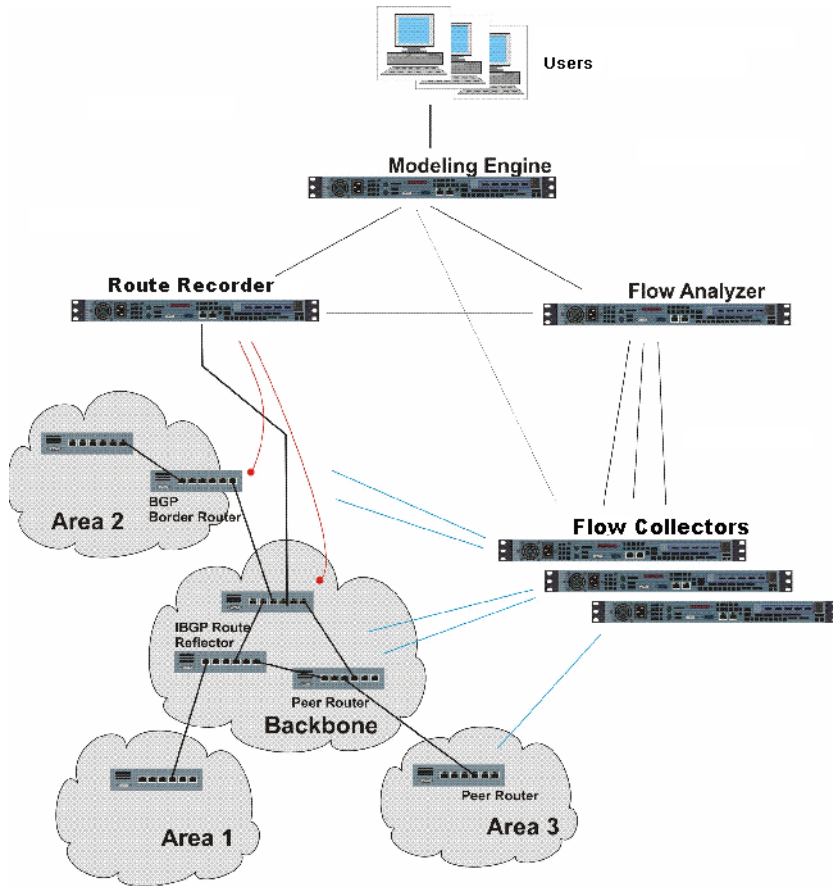


Figure 2 RAMS Traffic Data Flow

In a distributed environment where multiple appliances are installed on the network, one unit in the deployment will have a Master Capability license key. During the configuration process, you designate this unit as the master. The other appliances in the deployment act as clients of the master. For example, the Modeling Engine can be designated the master, while the Route Recorder is designated as a client. (For RAMS, the Route Recorder, Flow Collectors, and Flow Analyzer are 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, 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 System

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.
- A VNC or X Window System client for displaying the Route Analytics Management System 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 System 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 System 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 Recorder(s). 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 the hardware required to connect one or more appliances to the network is installed, the administrator can configure each appliance using the web-based *Administration* pages.

Configuration Overview

Proceed through the tasks described in this section for initial configuration. You perform the majority of these tasks on the appliance designated as the master system. Tasks that require you to access client machines individually are clearly noted.

- [Connecting to the Home Page](#) on page 20
- [Logging In](#) on page 22
- [Applying License Keys](#) on page 24
- [Setting the Time and Date](#) on page 28
- [Designating the Master and Clients](#) on page 30
- [Configuring the Network Interfaces](#) on page 36
- [Configuring SNMP Agent security](#) on page 42
- [Viewing System Settings](#) on page 43
- [Configuring RAMS for Recording](#) on page 43
- [Additional Configuration Tasks](#) on page 86
- [Enabling Technical Support Access](#) on page 93

In a distributed configuration, where multiple appliances are deployed, one of the appliances, RAMS or a Modeling Engine, must be designated as the “master” during the configuration process. The other units in the deployment become clients of the master.

The following descriptions apply to the master and client(s):

- **Master**—An appliance that allows centralized configuration of all client appliances in a multi-appliance deployment. You can monitor and manage these clients using the web-based *Administration* pages on the master.
- **Client(s)**—One or more appliances configured and monitored by the master in a distributed configuration. A client can be a Modeling Engine, 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. These tasks should be completed in the order in which they appear in this chapter.



[Designating the Master and Clients](#), does not apply to single-appliance configurations.

Many of the following configuration tasks are performed using the *Administration* pages. Access the *Administration* pages by clicking **Administration** on the *Home* page. The *View Configuration* page appears by default, with a Navigation Bar on the left side of the screen.



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.

Connecting to the Home Page

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

- Netscape 6.2 and 7.1
- Internet Explorer 5.5, 6.0, 6.22, and 7.0
- Firefox 2.0
- Macintosh Internet Explorer 5.2.1
- Mozilla 1.4, 1.5, and 2.0 (Linux)

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

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

In a distributed configuration, type 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 appears the first time you access the website.

The secure web pages have self-signed certificates from the appliance.



If you are using Internet Explorer 7.0 to connect, and after you enter the IP address or hostname in Step 1, a window opens with the following 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 appears 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 Connect to the *Home* page as described in the previous section, [Connecting to the Home Page](#).

The *Login* page appears.

- 2 Type 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 appears as shown in [Figure 4](#).

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/hpsoftwaresupport>

Figure 4 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 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, it is recommended 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, then type the new password.
- 3 Click **Update**.

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

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 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 5: 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 A](#), “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 5 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 30.

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 re-deploy 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 will erase all licenses that have been applied and allow you to reapply the correct licenses.

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.

It is strongly recommended that the time and date for each appliance be synchronized with an NTP server to avoid ever 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 progress 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. Therefore, you should first 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, verify the results on the *View Configuration* page.



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

To set the time and date for each Route Analytics Management System, perform the following steps:

- 1 On the *Time and Date* page, shown in [Figure 6](#), select the time zone from the **Time Zone** drop-down list.
- 2 Choose whether to set the time and date from an NTP server or set it manually.
 - If time is to be obtained through NTP, type the primary and secondary NTP server (if necessary) in the **Primary NTP Server** and **Secondary NTP Server** text boxes, respectively.
 - If time is to be maintained manually, and needs to be corrected now, click the **Set time now** check box and adjust the time fields as necessary.
- 3 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

Designating the Master and Clients

Distributed configuration and management allows an administrator to configure and monitor a number of RAMS 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 36.

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

- **Route Recorder(s)**—Collects routing information and stores it in the database.
- **Modeling Engine**—Provides a synthesized view of all network data collected by the recorders. In a deployment with multiple Route Recorders, the centralized Modeling Engine 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 System User’s Guide* for more information.
- **Flow Recorder**—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.

Depending on the type of multi-appliance deployment you are configuring, a Modeling Engine or Route Recorder will typically act as the master appliance in your environment. Additional Route Recorders can be configured to listen to different protocols. For example, in new RAMS deployments, the Modeling Engine will usually become the master appliance. On the other hand, if you have migrated an existing single-appliance RAMS deployment to a multi-appliance, distributed configuration, the Route Recorder will be the master appliance.

Assigning the Master Role to a RAMS Appliance

The master in a distributed configuration allows you to view and manage multiple RAMS systems through its administration interface. You must designate which system (RAMS or a Modeling Engine) in the configuration will act 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 Access password. A default password is already set. If you want to choose a different password, use the Configure Master Password command on the master appliance and on each client appliance to set the new password. The Master Access password **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 From the Left Navigation Bar, choose **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

<h5 style="text-align: center; background-color: #e6e6fa; margin: 0;">Client List</h5> <div style="display: flex; align-items: center;"><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 10px;">Delete</div></div>	<h5 style="text-align: center; background-color: #e6e6fa; margin: 0;">Add New Client</h5> <div style="display: flex; align-items: center;"><div style="margin-right: 5px;">IP Address:</div><div style="border: 1px solid #ccc; width: 100px; height: 15px; background-color: #ffff00;"></div><div style="margin-left: 10px; border: 1px solid #ccc; padding: 2px 5px;">Add</div><div style="margin-left: 5px; font-size: small;">This may take several seconds</div></div>
---	---

Client Status

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

Refresh Client Status

Relinquish Master Role

Figure 7 Units Page

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

After you have assigned the configuration master, you must now designate each of the clients 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. Once a client is bound to the master, that client cannot be bound to another master until the master-client relationship is dissolved as described in [Relinquishing the Master Status](#) on page 35. License details are returned when a client is added successfully. For instance, a message indicating that two license keys were applied will appear on the master's *Units* page after you have added a client.



The clocks of the units must be in synch 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, type the IP address of a client in the *Add New Client* text box.
- 2 Click **Add**.

A success message appears. 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. Corresponding to the IP address of each client is its 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

Client Configuration

Client List

(192.168.0.165)

(192.168.0.148)

(192.168.0.160)

Add New Client

IP Address:

This may take several seconds

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

Figure 8 Client Status Section of Units Page

Adding a Second Modeling Engine to the Configuration

Having one Modeling Engine is sufficient for most networks. However, if you anticipate more than five users having 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, be sure that the master unit has all the necessary licenses.

To add a second modeling engine to your network, perform the following steps:

- 1 From the Administration page of the master unit, choose **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** displays in the Left Navigation Bar.

You now need to specify how the routing data for the Modeling Engine is obtained. 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 136 for more information.

Relinquishing the Master Status

If necessary, you can remove the master status from an appliance, and if desired, assign this function to another appliance 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 On the top navigation bar, choose **Recorder Configuration**.
 - b On the *Recorder Configuration* page, click **Stop All Recording**.
 - c Click the client to remove from the tree structure.

A pop-up menu appears.
 - d Click **Delete**.
 - e On the confirmation screen that opens, click **Yes**.
 - f Repeat Steps **c** through **e** 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. RAMS then allows you to 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 Return to the *Units* page by clicking **Administration** on the *Recorder Configuration* page, then clicking **Units** on the Left Navigation Bar.
 - b On the *Units* page, 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 30.

Configuring the Network Interfaces

Use the *Network and Interface Configuration* page, shown in [Figure 9](#), to set the RAMS IP address, the netmask, the default router, and primary and secondary DNS servers. To access this page, from the left navigation pane locate **System** → **Network and Interface**.

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:

WARNING: Before changing the IP address of the Admin interface, you must delete all Recorder Configuration, delete all Master-Client associations, and relinquish Master role. Failure to do so may require Reset to Factory Defaults on all units to recover.

Interface	Name	Use DHCP	IP Address	Netmask	Allow Admin	Status
Slot 0/Port 1 (00:30:48:70:B6:B0)	<input type="text"/>	<input type="checkbox"/>	65.192.41.145	255.255.255.0	<input checked="" type="radio"/>	Up
Slot 0/Port 2 (00:30:48:70:B6:B1)	<input type="text"/>	<input type="checkbox"/>	192.168.3.45	255.255.252.0	<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 type="radio"/> Half <input checked="" type="radio"/> Full

Alias Interfaces		
Interface	Alias Name	IP Address
Slot 0/Port 2 <input type="button" value="v"/>	ConfedAlias1	192.168.122.45
Slot 0/Port 2 <input type="button" value="v"/>	ConfedAlias2	192.168.122.90
Slot 0/Port 1 <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>

Static Routes		
Destination	Default Router	Netmask
192.168.0.0	192.168.0.2	255.255.0.0
25.0.0.0	192.168.0.2	255.255.255.0
0.0.0.0	65.192.41.1	0.0.0.0
<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 9 Network and Interface Configuration Page



Before you can change the IP address on a system, you must delete all recorder configurations, delete all associations between master and client, and relinquish the master role. Failure to do so may require reset to factory defaults on all units to recover.



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

Before you configure the network manually or using DHCP, type the hostname of the Route Analytics Management System 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 On the *Network & Interfaces Configuration* page, type the following information into the appropriate text boxes:
 - Domain Suffix
 - Primary DNS
 - Secondary DNS (optional)
 - Properties for each interface (name, IP address, and netmask)
 - Default router (Gateway Address)
- 2 Click **Update**.

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

- 1 On the *Network & Interface Configuration* page, select the **Use DHCP** check box.
- 2 In the *Name* text box, type a name to identify the interface.

- 3 Select the **Auto Negotiate** check box to use automatic speed and duplex settings.
- 4 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 only available 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. Click **Allow Admin** beside the interface that acts as the Administration Interface.

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

- As an FTP address for file transfer to RAMS.
- 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 an Alias Interface

An Alias Interface is used to add an additional IP address to an interface inside the netmask configured for that interface.

To configure an alias interface, perform the following steps:

- 1 On the *Network & Interfaces Configuration* page, and in the Alias Interfaces section, select the desired interface from the **Interface** drop-down list.
- 2 Type a name for the alias in the *Alias Name* text box.
- 3 Type the IP address in the *IP Address* text box.

- 4 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 manually configured (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. When multiple physical interfaces or tunnels are configured, a separate default route may be configured 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. If not, all the EIGRP peer routers on an interface are suitable for this purpose, then 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 Static Information Collection](#) on page 64 describes how to configure static information collection for non-EIGRP topologies.



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

To add a static route, perform the following steps:

- 1 On the *Network & Interfaces Configuration* page, in the Static Routes section, type the destination, default router, and netmask details in the appropriate text boxes.
- 2 Click **Update**.



Only one static route may be added at a time. After you click **Update**, a new row of blank fields is provided so you can add another route.



Override the default gateway 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.



It can take up to 30 seconds before the static route becomes visible while the new information is written to the system asynchronously. Be aware that 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.

To modify a static route, perform the following steps:

- 1 On the *Network & Interfaces Configuration* page, in the Static Routes section, make any required changes to the route details.
- 2 Click **Update**.

To delete a static route, perform the following steps:

- 1 On the *Network & Interfaces Configuration* page, in the Static Routes section, manually erase the route details.
- 2 Click **Update**.

Configuring Multiple Port Options

You can monitor a different OSPF or ISIS area or EIGRP autonomous system with each of the ports on the appliance, including those on a multiple port option card, if installed. Multiple area monitoring is also possible using tunnels. See [Configuring GRE Tunnels](#) on page 89 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 To use an expansion port as the Administrative Interface, click **Allow Admin** to switch the administrative interface to the desired port.
- 2 To use DHCP on the Administrative Interface, select the **Use DHCP** check box.



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

- 3 For each of the other interfaces on the card, type the following information in the appropriate text boxes:
 - **Name** (optional)
 - **IP address**
 - **Netmask**
- 4 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 SNMP agent running on the appliance by way of the SNMP Agent Configuration page. See [Configuring the Route Recorder for Static Information Collection](#) on page 64 for information on how SNMP is used for static information collection.

To configure SNMP agent security, perform the following steps:

- 1 Open the web interface.

- 2 Choose **Administration** → **SNMP Agent Configuration**.

The SNMP v3 Profiles page opens (Figure 10).

SNMP Agent Configuration

v2 community name

v3 user

v3 profile

* read-only access

** select 'none' to disable v3

Figure 10 SNMP Agent Configuration

- 3 Enter the SNMP v2 community name, if you plan to use SNMP v2.
- 4 Select an SNMP v3 profile, if you plan to use SNMP v3. See [Configuring SNMP v3 Profiles](#) on page 68 for instructions on defining SNMP v3 profiles.
- 5 Click **Save**.

Viewing System Settings

The settings configured in this chapter are listed on the *View Configuration* page for each appliance. To access the *View Configuration* page from the *Home* page, find the left navigation bar and select **Administration >View Configuration**.

Configuring RAMS for Recording

If you are working with a single-appliance configuration, proceed to [Configuring the Route Recorder](#) on page 47, where you'll configure the Route Recorder to listen to particular protocols.

In a multi-appliance deployment, RAMS components are configured and managed from a central location, the appliance designated as the master. All configuration tasks described in this section are performed on the *Recorder Configuration* page of the master appliance. You cannot configure or manage RAMS 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 Route Analytics Management System component management tasks in this order:

- 1 [Creating a Configuration Hierarchy](#) on page 44
- 2 [Configuring the Route Recorder](#) on page 47
- 3 [Adding Protocol Instances](#) on page 48
- 4 [Configuring the Flow Collector](#) on page 74 (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 77.

Additional configuration tasks include the following:

- [To listen to routing traffic on a network other than the local network, there are two options:](#) on page 89
- [Configuring a Loopback Interface for Cisco Routers](#) on page 93

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, the first step in managing RAMS components from the *Recorder Configuration* page of the master appliance. Use a configuration hierarchy to organize components into a tree structure, with each “branch” representing a different part of the

configuration. For example for RAMS in [Figure 11](#), branches exist 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.

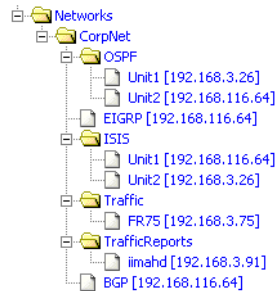


Figure 11 Configuration Hierarchy

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, like *CorpNet* in the following examples, so you can easily rename the complete hierarchy of recorded databases for backup purposes. You can add multiple administrative domains underneath 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 in a RAMS viewer as you can load the entire tree or focus only on particular branches. More information can be found in the “The Routing Topology Map” chapter in the *HP Route Analytics Management System 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, click **Recorder Configuration** on the top navigation bar.
The *Recorder Configuration* page appears.
- 2 Click **Networks**.
A pop-up menu appears.
- 3 On the pop-up menu, move the cursor to **Add**.

The **Administrative Domain** menu item appears as shown in [Figure 12](#).



Figure 12 Administrative Domain

- 4 Click **Administrative Domain**.

The **Name of new Administrative Domain** box appears as shown in [Figure 13](#).

Name of new Administrative Domain:

IP Address

Domain is a BGP AS Confederation

BGP AS Confederation Id:

Figure 13 Adding an Administrative Domain

- 5 Type a name for the administrative domain. The name must consist solely of alphanumeric characters, with an alphabetic character first.
Keep in mind that this should be the top-level domain under which you will create the rest of your hierarchy as recommended.
- 6 For 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.
- 7 If the administrative domain represents a BGP confederation, perform the following steps:
 - a Select the **Domain is a BGP AS Confederation** check box.
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 52.
 - b Type the confederation ID number in the *BGP AS Confederation Id* text box.
- 8 Click **Add Domain**.

- 9 Click the **+** symbol to the left of **Networks** to open the folder that shows the domain name you just entered.
- 10 Proceed to [Configuring the Route Recorder](#) 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 it to start recording. You must configure the Route Recorder before configuring other RAMS components.



Set the time and date on RAMS before configuring the recorder, per the instructions described in [Setting the Time and Date](#) on page 28. The date and time must be set before data recording begins because RAMS relies on accurate time stamps for generating report information. It is strongly recommended that NTP is used 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. Each Route Recorder can be configured to listen to one protocol or multiple protocols per area or Autonomous System (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 On the *Recorder Configuration* page of the master appliance, click the top-level domain name you added in [Creating a Configuration Hierarchy](#) on page 44 (for example, *CorpNet*).
- 2 Move the cursor to **Add**.
The option to add another level of domain name hierarchy appears, as shown in [Figure 12](#).
- 3 Click **Administrative Domain**.
The **Name of new Administrative Domain** box appears as shown in [Figure 13](#).
- 4 Type a name for the administrative domain. The name must consist solely of alphanumeric characters, with an alphabetic character first (for example, *IGPRecorders*).

- 5 For 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 can be used to organize the tree by protocol or by area. For example, imagine the *IGPRecorders* branch was added to the tree. In subsequent steps, you can add *OSPF* and *ISIS* branches under *IGPRecorders*. Then, under *OSPF* and *ISIS*, you can add one or more Route Recorders.
- 6 If the administrative domain represents a BGP confederation, perform the following steps:
 - a Select the **Domain is a BGP AS Confederation** check box.

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 52.
 - b Type the confederation ID number in the *BGP AS Confederation ID* text box.
- 7 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 database(s), proceed to [Adding Protocol Instances](#).

Adding Protocol Instances

RAMS 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 communicating directly with each other using that particular 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 (ISIS, OSPF, EIGRP, or BGP) and the network interface used to listen to the routing protocol packets.



For each interface, the RAMS supports an interface password and an area or domain password. If that interface is recording Level 1, the area password should be entered 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 RAMS 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 In the tree on the *Recorder Configuration* page of the master appliance, click the label you added in [Configuring the Route Recorder](#) (for example, *IGPRecorders*).
- 2 On the pop-up menu, click the desired type of protocol instance (BGP, OSPF, ISIS, or EIGRP).

One of the following options appears 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 53 or [Configure a BGP Instance](#) on page 59 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 3.
- 3 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 53 or [Configure a BGP Instance](#) on page 59 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 4.
- 4 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 53 or see [Configure a BGP Instance](#) on page 59.



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

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



Multiple different protocol instances can be added under one administrative domain, but only one instance of a particular protocol is allowed.

The structure of the administrative domain hierarchy also affects how RAMS associates the protocol instances to connect them in the routing topology map and to calculate routes across them. The next sections explain three 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.
- Multiple EIGRP autonomous systems can be configured in one administrative domain or 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 53.

The appliance supports up to 100 areas. This limitation applies to the total of OSPF areas, ISIS 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. RAMS 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, RAMS employs a heuristic algorithm to match routers.

A BGP node that peers with RAMS 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. RAMS 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, RAMS 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. In order to join the two autonomous systems by a link on the map, RAMS must consolidate this interface address with an IGP router in the other AS. To do this, RAMS first finds the BGP instance of the next-hop router using the AS number from the BGP AS path attribute, 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 was in its own administrative domain under the *Separate* domain rather than being paired in the *East* and *West* domains as shown, then both IGPs would be equally distant and either might have matched since 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 representing 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 59 for guidelines on configuring BGP.

Configuring Multiple EIGRP Autonomous Systems

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

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

Advantages: Fewer configuration steps are required, and the autonomous system configuration need only be entered once. In the table listing protocol events, the events from all autonomous systems within the instance are merged so you can view their relative timing.

- 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, ISIS, 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 14](#).

The following buttons and check boxes appear on-screen:

Save 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—Save events corresponding to the protocol packets in the list of events.

Configure—Choose this button to configure an interface. This button is enabled once you make a selection in either 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 generic routing encapsulation (GRE) tunnel is required to connect to a remote router. See [Configuring GRE Tunnels](#) on page 89 for instructions.

Stop Recording—Choose this button to stop recording.



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

Protocol OSPF	
Name : LabNetworksBGP.Domain1	
<input type="checkbox"/> Capture raw protocol packets	
<input type="checkbox"/> Record protocol packet events	
Interfaces	
Active	Not Active
Tunnel229_TO_ROUTER44 Tunnel229_To_Router26_OSPF_Area2	Slot 0/Port 1 Tunnel229_To_Router42
<input type="button" value="←"/> <input type="button" value="→"/>	
<input type="button" value="Configure"/> <input type="button" value="Delete"/> <input type="button" value="New Tunnel"/>	

Figure 14 Configuring an IGP Protocol Instance

- 1 To receive diagnostic trace information for your network, select **Save raw protocol packets**. The information is saved in a log file within the ftp directory.
- 2 Beneath the Interfaces section of this page, the configured network interfaces display 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 the “>” buttons.
- 3 If a generic routing encapsulation (GRE) tunnel is required to connect to a remote router, click **New Tunnel**, and then follow the instructions in [Configuring GRE Tunnels](#) on page 89 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 40.



The procedures for configuring an IGP instance vary between the protocols after Step 4. If you are configuring for ISIS protocol, continue to Step 5. If you are configuring for OSPF, continue to Step 6, and if you are configuring for EIGRP, continue to Step 8.

- 4 Enable authentication by selecting the desired interface from the “Active” column, and click **Configure**.

The Configure Interface page appears, as shown in [Figure 15](#).

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"/> <small>Tunnel Destination</small> 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"/>

Figure 15 Configure Interface Page for IGP (ISIS Protocol)

- 5 (For ISIS protocol only) Select the form of authentication you wish to use for either the interface or the area/domain for the interface. There are two types of 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)

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

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

- 6 (For OSPF protocol only) Select the form of authentication you wish to use for OSPF authentication. There are two types of 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. See [Configuring a Loopback Interface for Cisco Routers](#) on page 93.

- 7 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 6 through 11 are for configuring EIGRP protocol instances only.

- 8 (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 16](#).

For a network with more than one EIGRP AS, there are two configuration choices as explained in [Configuring Multiple EIGRP Autonomous Systems](#) on page 52.

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 16 Configuring an EIGRP Autonomous System

- 9 In the *Configure Autonomous System* table, fill in the following fields:
 - AS Number: Type either an explicit AS number or zero to allow RAMS 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.
 - 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.
- 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.
- Router Password, TACACS User name, and TACACS Password. If all routers use the same password or TACACS user name and password combination, type either the simple router login password or a TACACS user name and password combination, or both if some routers will use one and some routers will use the other. The TACACS fields can also be used for user name and password authentication configured through RADIUS or configured locally on the routers, although it must be the same for all routers in the AS.



See Step 12 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 RAMS 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.
- 10 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 should not attempt to log into, or to limit the scope of the RAMS topology exploration.
 - 11 Type an interface address, then click **Update AS**.
 - 12 Use the *Configure Interface Passwords* table to override the generic passwords specified in Step 9 for any router that has a password different from those specified in the *Configure AS* table. Type an interface address and its password or TACACS user name and password combination, then click **Update AS**.



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

- 13 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 48, the BGP configuration section appears on the *Recorder Configuration* page as shown in [Figure 17](#). Before getting to the detailed steps for configuring the BGP instance, this section presents some guidelines for choosing what peerings to establish between RAMS and the BGP routers.

For every BGP AS configured, the AS number and list of IP addresses of peers in the AS are required during configuration. Each peer should be configured to an IBGP peer with RAMS. It is important that no policies are applied to the routes sent to RAMS. RAMS 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 RAMS.

If multiple autonomous systems are monitored, an alias must be assigned for each additional AS. Aliases are logical interfaces created by the OS that are assigned their own IP Address and behave the same as any other physical interface. These aliases facilitate the multiple personalities required for participating in multiple autonomous systems. These additional addresses can be the tunnel end-point addresses or they can be configured in the Administration Interface as IP alias addresses as described in [Configuring an Alias Interface](#) on page 39. 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, meaning, 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.

There are three ways to configure a BGP instance in relation to the IBGP full mesh. In order of preference, these are the following:

- 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 RAMS to see all of the IBGP updates sent by all of the routers in the mesh. That is, RAMS sees the topology in exactly the same way that the other IBGP routers see it.
- If your network has route reflectors, you can set up a peer (neighbor) relationship among RAMS and all of the Route Reflectors in the network. Note that you are configuring the Route Reflectors to treat RAMS as a *peer*, not as a *client*. In this scenario, RAMS receives all of the updates from Route Reflector clusters. This provides RAMS with information about all routes being advertised, but the information is more limited than if RAMS were part of the full IBGP mesh. In particular, if some of the Route Reflector clusters have multiple exit points for the same route, RAMS might be able to see only a few (if there are multiple route reflectors present in the cluster), or only one of these exit points.
- The least preferred method is to configure RAMS as a Route Reflector client. This option gives RAMS only one view of the network, that of the Route Reflector. This limits the ability of RAMS to do some types of analysis, but route tracing should work correctly.

To increase the amount of routing information available to RAMS, you can configure RAMS 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 RAMS support no more than 10 Route Reflectors when RAMS is configured as a client.

You can choose the third option even if you do not currently have any Route Reflectors in your network. Any router can be configured to become a Route Reflector for the purpose of peering with RAMS. This does not affect the other BGP neighbors of the router, because being a Route Reflector is a per-neighbor setting. You might consider the third option if the first two options could entail

too much configuration effort. Note that 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 RAMS as a peer instead of a client.

Configuring RAMS 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, RAMS is unable to determine the correct exit routers or find correct paths for BGP prefixes.
- RAMS will learn from each of the EBGP peers one route for each prefix known in the autonomous system, rather than just those routes for which the peer is responsible, unless some policy filter is used to limit this information. If RAMS peers with many BGP routers in the AS, the total number of routes may exceed its capacity.
- Even though RAMS will be maintaining many more routes than with IBGP peering, the fidelity of the routing information is much less because of the missing attributes. Without those attributes, the routes passed to RAMS by different routers will be almost identical.

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

In a BGP confederation, RAMS should be configured to peer with each member AS using one of the three approaches described earlier in this section for a non-confederated BGP AS. That is, separately for each member AS, RAMS should be configured as an IBGP peer participating in the full mesh of IBGP routers in the member AS, or as a Route Reflector peer or client. A different alias must be assigned to RAMS for each member AS.

If your RAMS appliance has a license for both BGP and VPN protocols, and you want to monitor VPN routing, then in order to collect complete routing you should configure peering from RAMS either to all of the provider's edge (PE) routers or as a peer to all of the Route Reflectors serving the VPN routes in the AS. As each peering is configured, you must enable BGP extensions for MPLS VPNs, as indicated in the detailed instructions that follow. See the "VPN

Routing” chapter in the *HP Route Analytics Management System User’s Guide* for more information about configuring customer/Route Target (RT) associations for routing reports.

Once you have decided what BGP peerings you want to configure, you can type the appropriate information in the BGP configuration section as shown in Figure 17.



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.

REX	Peers						
<p>BGP Id: 192.168.122.90 Confed Id: 65533 Member AS: 65510 Name: LabRight_ConfedsTest_ConfedTestTop: BGP Interface: <input type="text" value="ConfedAlias2"/> <input type="checkbox"/> Log Traces</p> <p><input type="button" value="Save"/></p>	<table border="1"><tr><td>25.0.0.1</td><td><input type="button" value="Add"/></td></tr><tr><td>25.0.0.21</td><td><input type="button" value="Edit"/></td></tr><tr><td></td><td><input type="button" value="Delete"/></td></tr></table>	25.0.0.1	<input type="button" value="Add"/>	25.0.0.21	<input type="button" value="Edit"/>		<input type="button" value="Delete"/>
25.0.0.1	<input type="button" value="Add"/>						
25.0.0.21	<input type="button" value="Edit"/>						
	<input type="button" value="Delete"/>						

Figure 17 Configuring a BGP Instance

To configure a BGP instance, perform the following steps:

- 1 Type the BGP IP address in the **BGP Id** box.
- 2 Type the autonomous system number in the **AS** box. If the BGP protocol instance is within a confederation, type the AS number of the member in the **Member AS** box. This is *not* the confederation ID, which is shown separately.
- 3 From the **Interface** drop-down list, select the physical interface slot and port or select the logical interface alias.
- 4 To receive diagnostic trace information for your network, select **Save raw protocol packets**. The information is saved in a log file within the ftp directory.
- 5 In the **Peers** column, click **Add** to add peers.

The peer configuration table appears at the left side of the screen as shown in [Figure 18](#).

Peer Information	Options
IP Address(es) or Prefix(es): <input type="text"/> AS: <input type="text" value="65510"/> MD5 Password: <input type="text"/>	<input checked="" type="radio"/> Internal <input type="radio"/> External <input type="checkbox"/> BGP ext for MPLS VPNs
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 18 BGP Peer Configuration

- 6 In the **Peer Information** column, type the IP address(es) of the peer(s), 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.
- 7 In the **Options** column, specify whether the peer(s) is internal or external.
 If you enter multiple peers at once, all of the peer addresses must share the same internal or external setting.
- 8 If this BGP topology is a BGP MPLS VPN, select **BGP ext for MPLS VPNs**. Otherwise, leave this check box empty.
- 9 When you have entered all information for the peer(s), click **Update Peer** to return to the BGP instance configuration.
- 10 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 17](#), 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 Static Information Collection

This section describes how to configure the Route Recorder to collect information on static routes in addition to connected routes and router interface information. The process uses SNMP to gather information on all topologies except EIGRP. (For EIGRP, static information is collected using telnet or ssh and CLI commands.)

Connected routes are derived automatically from the prefixes that are assigned to interfaces on the router. Any device on the subnet connected to an interface will have an address assigned within the prefix of the interface and will be accessed through the connected route. Static routes are entered manually. A static route specifies a destination prefix and the next hop to which a packet should be sent towards that destination.

Collecting static route information can consume substantial resources on the routers because it requires retrieving the full routing table. You can configure collection of interface parameters without static routes on all the routers of interest, and then separately configure static route collection on just a subset of the routers where static routes are present and the routing table is not too large.

You can configure static information collection on any appliance that performs route recording. The scope of the static information collection is determined by the location in the hierarchy that you choose when configuring the recorder and applies to the selected subtree (Figure 19). You can configure multiple static information collection 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.

Recorder Configuration

the network or networks to be monitored here. Click on the network in the hierarchy (left) to open the network configuration page, or define a new one. Only protocols for which a software license has been installed may be configured here. To install new software licenses, go to [Maintenance->License](#).

Figure 19 Choosing Scope for Static Information Collection

Each router included in the static information collection must have a compatible SNMP v2 or v3 configuration.

Before you configure the static information collection, you must configure a query server on the Route Recorder or Modeling Engine.

To configure a query server, perform the following steps:

- 1 Open the web interface on the appliance.
- 2 Choose **Administration** → **Queries**.
- 3 Select the **XML-RPC Query Server** and **Enable remote access** check boxes.
- 4 Enter and confirm the password for query access.
- 5 Click **Update**.

To configure static information collection, perform the following steps:

- 1 Verify that the routers to be included in the static information collection are configured for SNMP v2 or v3.
- 2 Open the web interface on the appliance.
- 3 Choose **Recorder Configuration**.
- 4 Click the desired level in the recorder hierarchy in the left navigation bar and choose **Add** → **Static**.

- 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 20). If you have a single appliance, it is not necessary to select the appliance to open the Recorder Configuration window.



A query server must be configured on the Router Recorder or Modeling Engine. Choose **Administration** → **Queries** in the web interface, and

Recorder Configuration

Unit: 10.26.15.226

SNMP Configuration

Domain	LOCALNETWORK
Router list query server	<input type="text" value="10.64.15.226"/>
Router list query server password	<input type="password" value="•••••"/>
Router list refresh time (hours)	<input type="text" value="1"/>
SNMP discovery schedule	<input type="text" value="Daily"/> Day <input type="text" value="Saturday"/> Hour <input type="text" value="0"/>
SNMP discovery at next start recording	<input type="checkbox"/>
Number of routers to query in parallel	<input type="text" value="50"/>
Interval between queries to a router (seconds)	<input type="text" value="1"/>

SNMP Security Configuration

Routers (Prefix)	Black List	v2 Community	v3 Profile	Collect static routes*	Delete
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="none"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="none"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="none"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="none"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="none"/>	<input type="checkbox"/>	<input type="checkbox"/>

*Warning: Collecting static routes is not advised for routers with large routing tables

Figure 20 Recorder Configuration Window for Static Information Collection

- Make changes as needed to the following SNMP 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 the query server is configured on this appliance. If not, select the IP address of the query server. See the previous procedure in this section for instructions on configuring a query server.
 - **Router List refresh time**—Indicates how often the static router list is refreshed.
 - **SNMP Discovery Schedule**—Specifies the schedule used by SNMP to search for routers that match the static information collection requirements.
 - **SNMP Discovery at next start recording**—If selected, indicates that the appliance performs SNMP discovery when it is booted.
 - **Number of Routers to query in parallel**—Indicates the number of routers that will be queried for new information at the same time.
- 7 For each router or subnet that you want to include, enter the following information:
- **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.
 - **Blacklist**—Select the check box if you want to explicitly exclude the specified routers from static information collection.
 - **v2 Community**—Enter the SNMP community for the router, if SNMP v2 is used.
 - **v3 Profile**—Choose the SNMP v3 profile, if SNMP v3 is used. See [Configuring SNMP v3 Profiles](#) on page 68 for instructions on creating SNMP v3 profiles.
 - **Collect Static Routes**—Select the check box to collect the 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 Click **Save**.

Static information collection is now configured. When you start recording the information is collected.

To view collected static route information, perform the following steps:

- 1 Open the client application as described in the “Viewers” chapter in the in the *HP Route Analytics Management System 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 Static tab. You may need to click the right-facing arrow near the top of the panel to find the Static tab.

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

Configuring SNMP v3 Profiles

To define SNMP v3 profiles for static information collection, use the SNMP v3 Profiles page. When you define a profile, it becomes available for selection on the Recorder Configuration page. See [Configuring the Route Recorder for Static Information Collection](#) on page 64.

To configure an SNMPv3 profile, perform the following steps:

- 1 Open the web interface.
- 2 Choose **Administration** → **SNMP v3 Profiles**.
- 3 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 21](#)).

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 21 SNMP v3 Profile Configuration

- 4 Enter or confirm the profile name. The name is used when you select a profile for static information collection.
- 5 Enter the name of the SNMP user.
- 6 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 MD5 (default) or 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 DES (default) or AES privacy protocol and enter a privacy passphrase. This option is recommended for full protection.
- 7 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 47, 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 85.

- 1 In the configuration hierarchy tree, click the protocol instance where you'll start recording routing data.

A blue pop-up menu appears.

- 2 In the configuration hierarchy tree, click the protocol instance where you'll start recording routing data.

A pop-up menu appears.

- 3 Click **View**.

If the protocol instance 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 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 70, RAMS 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 In the configuration hierarchy tree, click a protocol instance.
A pop-up menu appears.
- 2 Click **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 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 Follow Steps 1 and 2 in the previous section to navigate to the *Recorder Configuration* page *Status* table.
- 2 From the **Area ID Format** drop-down list, choose Decimal or Dotted Decimal.
- 3 Click **Submit**.
- 4 Click the **Administration** link at the top of the *Recorder Configuration* page.
- 5 Click **VNC Configuration** in the left navigation bar.

- 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 Navigate to the *Recorder Configuration* page *Status* table.
- 2 Click **Stop Recording**.
- 3 Click an existing instance from the tree structure on the left side of the screen.
A pop-up menu appears.
- 4 On the pop-up menu, click **Delete**.
- 5 Click **Yes** on the confirmation screen that opens.

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

Removing an Interface from a Protocol Instance

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

- 1 On the *Recorder Configuration* page, select the protocol instance name on the tree.
- 2 From the pop-up menu, click **View** to see the protocol configuration.
- 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 On the *Recorder Configuration* page, select the protocol instance name on the tree.
- 2 From the pop-up menu, click **View** to see the protocol configuration.
- 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 type 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 On the *Recorder Configuration* page, select the protocol instance name on the tree.
- 2 From the pop-up menu, click **View** to see the protocol configuration.
- 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. Information for configuring NetFlow for Cisco routers can be found on [page 87](#).

In MPLS VPN deployments, you need to establish 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. Information for configuring LDP for Cisco routers can be found on [page 86](#).

LDP peering is established in two phases. The first is the establishment of a hello adjacency (UDP), and then a session is established which works over TCP.



You must configure the Route Recorder as described in [Configuring the Route Recorder](#) on page 47 before you begin configuration of the Flow Collectors.

To configure a Flow Collector, 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 44 (for example, *CorpNet*).
- 2 Move the cursor to **Add**.
A list of options appears on the pop-up menu.
- 3 Click **Traffic** near the bottom of the list.
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 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 22](#).

Recorder Configuration

Flow Collector Configuration

Domain	HPOspfTest
Flow Collector Id	FR
UDP Port	<input type="text" value="9991"/>
Sampling	<input type="text" value="1000"/>
Prefix Source*	<input type="text" value="(192.168.1.31)"/>

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="Slot0/Port 1"/>	<input type="button" value="X"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Slot0/Port 1"/>	<input type="button" value="X"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Slot0/Port 1"/>	<input type="button" value="X"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Slot0/Port 1"/>	<input type="button" value="X"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Slot0/Port 1"/>	<input type="button" value="X"/>

* 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 22 Configuring a Flow Collector

Domain is pre-populated with the name of the administrative domain.

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

RAMS Traffic 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, edit the UDP port number if necessary. 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, type 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, type 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, type the Sampling Rate 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 the Delete box to 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 Collector(s). 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.

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.

- 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 additional, more detailed status messages about the traffic database by clicking **Show Detailed Status**. 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. These details are useful in troubleshooting and are described in Table 1 .

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.

Table 1 Detailed Status Table (cont'd)

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).
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.

Table 1 Detailed Status Table (cont'd)

NetFlow records sampled	<p>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.</p> <p>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).</p>
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.

Table 1 Detailed Status Table (cont'd)

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.
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. RAMS Traffic 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 77.
- 2 On the *Recorder Configuration* page of the master appliance, click the Flow Collector to delete in the tree.
A pop-up menu appears.
- 3 On the pop-up menu, click **Delete**.
- 4 On the confirmation screen that appears, click **Yes**.

This deletes the instance, but the database remains in RAMS Traffic 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 Collector(s) 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 44 (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 appears.

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 In the configuration hierarchy tree, 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 display:

- **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.
- 2 On the *Recorder Configuration* page of the master appliance, click the Flow Analyzer to delete in the tree.
A pop-up menu appears.
- 3 On the pop-up menu, click **Delete**.
- 4 On the confirmation screen that appears, click **Yes**.

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

Additional Configuration Tasks

Configuring MPLS VPN-Aware LDP for Cisco Routers

Label Distribution Protocol (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 need to set up a targeted LDP session. This session forces the router to send you all the labels 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 Type the following command in global configuration mode:

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

The `mpls ldp neighbor <flow-recorder-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 is an open but proprietary network protocol used to collect IP traffic information. 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 only available in certain IOS versions. You should 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 generic routing encapsulation (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, there are two options:

- Remotely connect that network to a secondary network interface on the appliance.

You can use a GRE tunnel to form the adjacency.

The GRE tunnel follows standard routing across the network to the destination, so that 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 the tunnel must be configured both 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.

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

Table 2 Required Tunnel Information on Remote Router

Table 3

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>

Table 3

Item	Example of Command
Tunnel Source	tunnel source loopback 0
Tunnel Destination	tunnel dest <RAMS IP address>
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: router ospf <n> network 10.0.1.0 0.0.0.3 area <area to be monitored>

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 23](#).

Configure 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"/>
<input type="button" value="Update"/> <input type="button" value="Cancel"/>	

Figure 23 Configuring a GRE Tunnel Interface

- 4 In the *Interface* text box, type a descriptive name for the tunnel.
- 5 If 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, type a password in the Password text box that matches the password in the remote area.

- For MD5 authentication, type both a password and an 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, type 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, type the IP Address assigned to the tunnel on RAMS.

Using the example addresses listed above, this would be 10.0.1.2

- 8 In the *Netmask* text box, type 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 23](#):

- 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.)
- 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 Type 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 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, from the left navigation pane, locate **System** → **Support Access**. The *Technical Support Configuration* page displays as shown in [Figure 24](#).



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

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, the “Technical support callback” feature can be enabled by clicking **Enable Callback**. This feature is disabled by default and your explicit action is required to enable it. Doing so 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 tunnelled 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 24 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 *Home* page for each appliance.

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 96
- [Creating Traffic Groups](#) on page 103
- [Creating CoS Definitions](#) on page 109
- [Configuring the VNC Server](#) on page 112
- [Managing Databases](#) on page 115
- [Backing Up and Restoring Data](#) on page 120
- [Replacing Client and Master Appliances](#) on page 131
- [Choosing a Data Source](#) on page 136
- [Archiving Data](#) on page 139
- [Updating Software](#) on page 144
- [Using Top N Reports](#) on page 149
- [Creating Daily Reports](#) on page 151
- [Configuring the FTP Server](#) on page 155
- [Viewing and Exporting Log Pages](#) on page 157
- [Uploading Layout Backgrounds](#) on page 158

- [Using Diagnostic Functions](#) on page 159
- [Shutting Down](#) on page 160



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; however, 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 associated with one of the following privileges:

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

— Configure alerts, as described in the “Alerts” chapter of the *HP Route Analytics Management System User’s Guide*.

- Operators, who 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, who are view-only users, 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, who 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 8.

TACACS+ and RADIUS Parameters

An existing TACACS+ or RADIUS server that is configured for user accounts can be used; 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 not meaningful and 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 SFTP access, it should be additionally assigned `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 called “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

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

Access the User Administration page by selecting **Users** from the left navigation bar from the Administration page. The top portion of the User Administration page displays the following authentication information:

- **TACACS Server—TACACS+** (Terminal Access Controller Access Control System) is a security system that can provide centralized validation of users.
- **RADIUS Server—RADIUS** (Remote Authentication Dial-In User Service) is a database 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 Open the web application and choose **Users** from the left navigation pane. The User Administration page opens as shown in [Figure 25](#).

The screenshot shows the 'User Administration' page with a section titled 'Authentication Type'. It contains four radio button options: 'TACACS+ Server', 'RADIUS Server', 'Local Authentication', and 'Authenticate via Master'. Each option has a corresponding text input field for a shared secret. The 'Local Authentication' option is selected, and its shared secret field contains six asterisks. Below these options is a checkbox labeled 'Show Shared Secret' which is unchecked. At the bottom of the section is an 'Update' button.

Figure 25 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.
- 3 If you have a master/client configuration and the master appliance has been 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.
- 4 Select the **Show Shared Secret** check box if you want the shared secret to be displayed.
- 5 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.

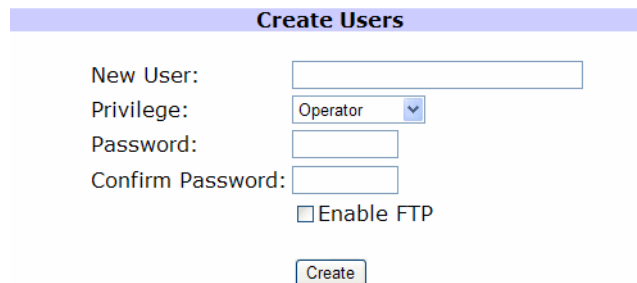
Use the Create Users section of the User Authentication page, you can create and assign privileges to a user.

Creating New User Accounts

User accounts 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 Open the web application and choose **Users** from the left navigation pane.
- 2 Enter the user name in the *New User* text box in the Create Users section of the *User Administration* page. This portion of the window is shown in [Figure 26](#).



The screenshot shows a web form titled "Create Users" with a light blue header. Below the header, there are four input fields: "New User:" (a text box), "Privilege:" (a dropdown menu with "Operator" selected), "Password:" (a text box), and "Confirm Password:" (a text box). Below these fields is a checkbox labeled "Enable FTP" which is currently unchecked. At the bottom of the form is a button labeled "Create".

Figure 26 Create Users Section of User Administration Window

- 3 Select the Privilege level of the user from the **Privilege** drop-down list:
 - **Guest**

- **Operator** (this is the default selection)
 - **Administrator**
 - **CLI Access**
- 4 Enter the password for the user in the **Password** text box.
 - 5 Confirm the users' password by entering it in the **Confirm Password** text box.
 - 6 Click the **Enable FTP** checkbox to allow the new account to access the FTP server on the appliance. See [Configuring the FTP Server](#) on page 155 for more information.
 - 7 Click **Create** to save the information. Select **Cancel** to dismiss the window.

Updating an Existing Users Account

You can update an existing user account in the Update Accounts section of the *User Administration* page. The parameters in this portion of the window are the same as in the Create Users section of the *User Administration* page.

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

- 1 Open the web application and choose **Users** from the left navigation pane.
- 2 In the *Update Accounts* section of the window (shown in [Figure 27](#)), click on a user from the **Current Users** box.

Update Accounts

Current Users: admin
op
sandra

Privilege: Guest ▼

Password:

Confirm Password:

Enable FTP

Figure 27 Update Accounts Portion 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 Open the web application and choose **Users** from the left navigation pane.
- 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 28](#).

The minimum value is 60 seconds, the maximum is calculated in years (roughly 4,000 years).

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.)

Update Login Timeouts

Figure 28 Update Login Attributes Section of User Authentication Window

- 3 Enter the desired value in the Login Idle Timeout (in seconds) text box.
- 4 Click **Update Login Timeouts** to save the information.

Creating Traffic Groups



This section applies to RAMS Traffic only.

RAMS Traffic increases the visibility into the traffic flowing through the network core by classifying traffic into user-defined groups.

The network administrator can create groups in a flexible manner. The rules of the group can be 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 from, or to, specific locations per application(s) and/or class(es) of service.

Further, if a traffic class is specified, it matches a subset of traffic associated with a particular Class of Service (CoS) defined by ToS or DSCP bits in the IP header. A traffic deployment can only have ToS or DSCP at one time, not both.

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

- To or from specific application servers (based on prefixes). For specific services like "Voice Premium" or "Voice Gold" (based on ToS and DSCP: AF or EF classes).
- Determine (via reports and GUI) per traffic flow, the application or CoS that it belongs to.
- Alert (SNMP Trap) when %utilization (or bps) exceeds (or falls below) a specified threshold per traffic group.

To access traffic groups, perform the following steps:

- 1 Open the web application and choose **Traffic Groups** from the left navigation pane.

The *View Group* window opens, as shown in [Figure 29](#).

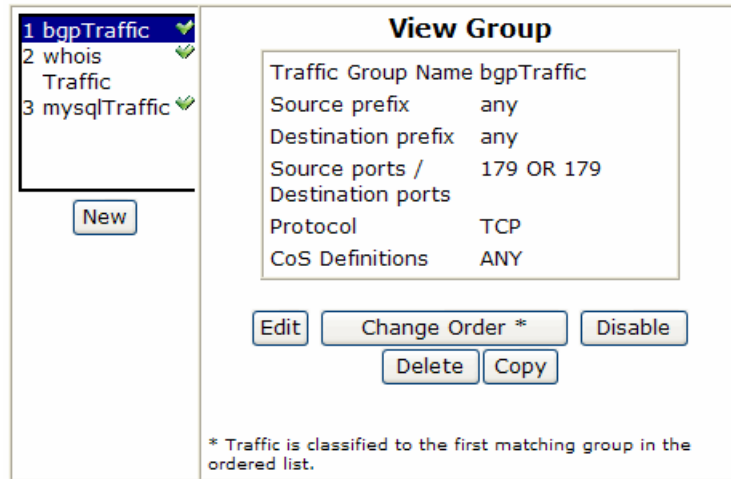


Figure 29 View Group window

- 2 To perform a task on this page, choose from the following list of buttons:
 - **New**—Select this to create a new traffic group (see the next procedure).
 - **Edit**—Select this to edit a previously created traffic group.
 - **Change Order***—Select this to set the priority of the traffic group the Flow Collector will track traffic for.
 - **Enable/Disable**—Select this to enable or disable a group.
 - **Delete**—Select this to delete a group.
 - **Copy**—Select this to 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 Open the web application and choose **Traffic Groups** from the left navigation pane.
- 2 In the *View Traffic Groups* window, click **New**.

The *New Group* window appears as shown in [Figure 30](#).

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-test1
kruti-test2
kruti-test3

CoS1

Figure 30 Create New Traffic Group Page

The following is a list of fields you will need to enter information 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.

In the **CoS Groups** section of this page, select the Class of Service you want associated with traffic group you are creating by clicking once on the class, and then clicking on the arrow button to move the class to the Selected column.

Below this field are the following buttons:

Submit—Saves the information entered.

Reset—Returns the values to what they were before creating this group.

Cancel—Cancels the operation.

- 3 Enter the name, source and destination prefix, source and destination ports, and the protocol for the traffic group you are creating.
- 4 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.
- 5 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 In the *View Traffic Group* page, and in the left navigational pane, select the traffic group you wish to edit by clicking once on the group, and select **Edit**. The *Edit Group* window opens as shown in [Figure 31](#).

1 ARVIND_ANY_ANY ✓

2 TGroup1 ✓

Edit 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

ARVIND_DSCP_EXP_ALL

kruti-tes1

kruti-test2

kruti-test3

Selected

CoS1

Figure 31 Edit Group Page



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

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

Creating CoS Definitions



This section applies to RAMS only.

Class of Service (CoS) specifies a priority value carried on 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 these 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 Type of Service (ToS) byte or Diff-Serv Code Point (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 Click **New** to define a CoS. The New CoS Definitions window opens as shown in [Figure 32](#)

CoS Definitions

The screenshot shows a 'New' dialog box for defining CoS. It features a list of existing definitions on the left, a text field for the name, and two columns for selecting traffic values. The 'Unselected' column lists DSCP values from 1 to 13, and the 'Selected' column is currently empty, showing 'None'. Navigation buttons are provided between the columns, and 'Save' and 'Cancel' buttons are at the bottom.

DSCP ToS

Mode is common for all CoS definitions.
Note: ToS is only used without MPLS transport.

Figure 32 New CoS Definition Window

DSCP mode is the default value.



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

- 2 Type the name to define the CoS in the **Name** field.
- 3 Select a traffic value from the Unselected column by using the “>” button to toggle the value to the Selected column. This will associate the value to the name entered in Step 2.
- 4 Click **Save** to define the CoS value. A confirmation message displays, along with the new CoS definition and its value as shown in [Figure 33](#).

CoS Definitions

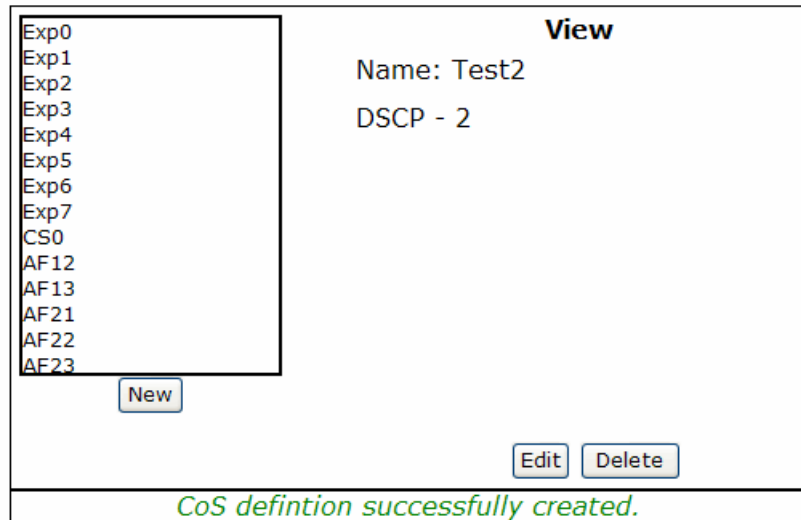


Figure 33 Confirming window for CoS Definitions

To edit a Cos Definition, perform the following steps:

- 1 Choose **CoS Definition** from the left navigation pane.
- 2 Select the CoS definition you need to edit from the column displaying the CoS definitions, 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 need to 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 System 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 Open the web interface and choose **Administration** → **VNC Configuration** (Figure 34).

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

Start

VNC Authentication

Password: Confirm password:

Update

VNC Displays 2 and Higher

	Width	Height
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Update Disable

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

Figure 34 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, type *hostname:1*, and then log in using the password you entered in the *VNC Configuration* page. The VNC session displays 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, type *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, rename, or automatically trim an existing database. To access this page, locate **Maintenance** on the left navigation bar of an individual appliance, then click **Databases**. The *Database Administration* page opens as shown in [Figure 35](#).

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 **106528MB** 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 35 Database Administration Page

Database administration is usually performed for housekeeping reasons — for example, when the disk is becoming full. Deleting unneeded databases and trimming active databases can help you to gain disk space. Since 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.

It is recommended 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 155 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. See [Figure 36](#) to view this portion of the window.

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"/>	Trimming databases may take some time, depending on the amount of data to be removed.

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

Figure 36 Online Databases Page



Before performing any database operations, you must quit all running instances of the client, including stopping the VNC server.

Using Offline Databases

Offline databases contain data from administrative domains that are not currently being recorded. These databases can be deleted to save disk space, or renamed 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 On the top navigation bar, click **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.
- 4 Click the node on the tree that corresponds to the database to be deleted and choose **Delete** from the pop-up menu.
- 5 If you are not working with a distributed configuration, proceed directly to Step 8. 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.
- 6 In the *Client Status* section of the *Units* page, click the client where the database was recorded to access the Home page of that client.
- 7 On the Home page of the client, click **Administration** on the top navigation bar.
- 8 Click **Databases** on the left navigation bar.
- 9 Select the check box(es) to the left of the database(s) to be deleted.
- 10 Click **Delete Selected Databases**.
A confirmation page opens displaying the names of the selected databases.
- 11 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 where the database is being recorded and click **Administration** on the top navigation bar.
- 3 Click the **Recorder Configuration** link on the top navigation bar to display the *Recorder Configuration* page.
- 4 If the database you want to delete is currently recording, stop recording on that database.
- 5 Click **Databases** on the left navigation bar.
- 6 Select the check box(es) to the left of the database(s) to be deleted.
- 7 Click **Delete Selected Databases**.
A confirmation page opens displaying the names of the selected databases.
- 8 Click **Yes** if you want to delete the selected databases.
The selected databases are deleted.
- 9 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 where the database is being recorded and click **Administration**.
- 3 Click the **Recorder Configuration** link on the top navigation bar to display the *Recorder Configuration* page.
- 4 If the databases you want to rename are currently recording, stop recording on these databases.
- 5 Click **Databases** on the left navigation bar.

- 6 Select the check box(es) to the left of the database(s) to be renamed to a single, new name (typically, only databases that have a common first-level administrative domain name already).
- 7 Type 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.
- 8 Click **Rename Selected Databases**.
A confirmation page opens displaying the names of the selected databases.
- 9 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 topology in databases, and also stores system configuration files. 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 128.

You can save the backup file through the administration interface or by using File Transfer Protocol (FTP). Since most web 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 131.

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. This metadata header contains database and/or system configuration information as well as 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.

This information opens in the Restore from Backup on This appliance's Disk section at the bottom of the *Backup and Restore* page. See [Restoring a Backup File](#) on page 127.

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, locate **Maintenance** on the left navigation bar, then click **Backup and Restore** (shown in [Figure 37](#)).

Backup and Restore

Create Backup on This Unit's Disk

	Administrative Domain	Protocol	Area ID	Size
<input checked="" type="checkbox"/>	Layouts and other properties			
<input type="checkbox"/>	System Configuration			
Data				
<input checked="" type="checkbox"/>	Lab240.domain1	Static	snmp	1.2M
<input type="checkbox"/>	Lab240.domain1.domain5	Static	snmp	284K
<input type="checkbox"/>	Lab240.domain1.domain5	Static	static	816K
<input type="checkbox"/>	Lab240.domain3	BGP	AS234	6.9M
<input type="checkbox"/>	Lab240.domain3	Static	static	1.6M
<input type="checkbox"/>	Lab240.domain3	Static	snmp	1.1M
<input type="checkbox"/>	Lab240.domian2	ISIS	270001	26M
<input type="checkbox"/>	Lab240.domian2	ISIS	Backbone	44M
<input type="checkbox"/>	Lab240.domian2	BGP	AS12	556K
<input type="checkbox"/>	REP1220894949ME204	RFRG	FR1	1.6M
<input type="checkbox"/>	REP1220894949ME204	RFRG	FR204	13M
<input type="checkbox"/>	REP1220894949ME204	TrafficReports	FR1	1.6M
<input type="checkbox"/>	REP1220894949ME204	TrafficReports	FR204	13M
<input type="checkbox"/>	REP1221167294ME204	RFRG	FR1	1.3M
<input type="checkbox"/>	REP1221167294ME204	TrafficReports	FR1	1.3M

Figure 37 Backup and Restore Page

This page contains two sections:

- The Create Backup section, which contains a list of all system configurations and databases in the system.

- **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.

The 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 appliance's Disk**—This section contains the backup file information and the database(s) 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 38 Restore from Backup Section

To create a backup file, perform the following steps:

- 1 On the Backup and Restore page, 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. 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 144.

- 2 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.

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

The *Backup and Restore* page displays the new backup file(s) in the *Restore from Backup on This appliance's Disk* table at the bottom of the page, as shown in [Figure 38](#).



Depending on the size of the database and on the Login Idle-Timeout settings, the Administration login might 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 operating system (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.
- 4 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 131.

To save a backup file, perform the following steps:

- 1 After creating a backup file, click **Backup and Restore**.
- 2 On the *Backup and Restore* page, click the **Download Backup File** button.
A *File Download* dialog box appears.
- 3 Click **Save**.
- 4 Type 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 131.

To upload a backup file, perform the following steps:

- 1 Go to the *Backup and Restore* page.
- 2 Click **Upload Backup File**, which appears below the Restore from Backup on This appliance's Disk section.
The *Restore Backup from File* window appears.
- 3 Type 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 database(s) 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

The Restore from Backup on This appliance's Disk section of the *Backup and Restore* page contains the most recent backup file information in the table.

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 126.
- 2 On the *Backup and Restore* page, select one or more checkboxes 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 144.

- 3 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.
- 4 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.
- 5 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.

- 6 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 Go to the *Backup and Restore* page.
- 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 Server Message Block (SMB) to create backup files on, and restore backup files from, 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 On the left navigation bar, locate **System** and click **Archival Configuration**. The *Archival Configuration and Remote Storage* page appears as shown in Figure 44.

- 2 Select the **Enable SMB** check box to create or restore backup files from a remote storage server.
- 3 Type 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 Type the remote server password in the *Remote password* text box.
- 5 Type the remote server IP address in the *Remote server IP* text box.
- 6 Type the remote server share name in the *Share name* text box.
- 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 operating system (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 name(s) 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 On the Backup and Restore page, select the option button in the left column of the backup file.
- 2 Click **Select Backup File**.

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

- 3 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 144.

- 4 Select the **Overwrite layouts and other properties** check box if you want to restore a backup set of layouts and properties.
- 5 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.

- 6 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 File Transfer Protocol (FTP). You must enable the FTP server to transfer backup files using FTP. See [Configuring the FTP Server](#) on page 155.

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 121 and [Saving a Backup File](#) on page 125. 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 140.

To replace a client appliance, perform the following steps:

- 1 Open the web interface on the master unit.

- 2 Choose **Recorder Configuration** and click **Stop All Recording**.

Recording is stopped and the Recorder Configuration page refreshes.

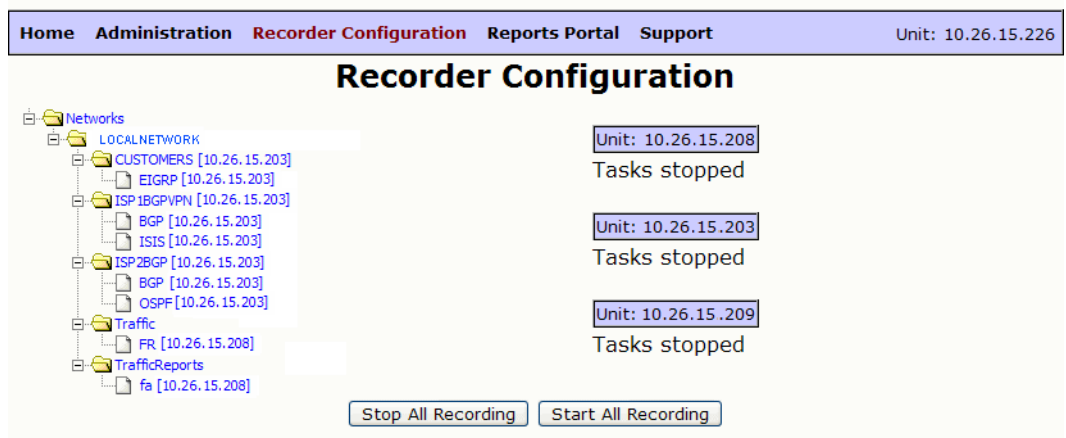


Figure 39 Stopping Recording

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

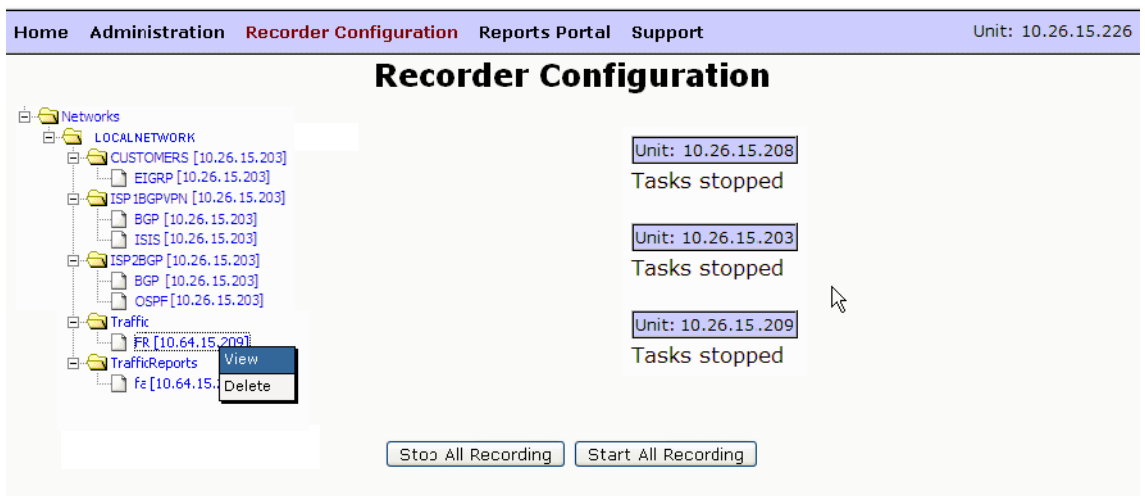


Figure 40 Deleting Units

- 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 the **Overwrite layouts and other properties** check box 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.

10.20.15.207 ▼ Make Master

Figure 41 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.

Restore Selection

Figure 42 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 to 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. In previous versions, users obtained routing data by querying each Route Recorder individually. Users could configure Generic Routing Encapsulation (GRE) tunnels to connect Route Recorders deployed to remote areas of the network. Each Route Recorder provided reports specific to the local areas and protocols where it was listening.

You can still obtain reports from individual Route Recorders. However, using a centralized Modeling Engine to generate reports not only provides a global view of the network, but also 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.



You will need at least 1 MB of bandwidth between the Route Recorders and the replicating Modeling Engine.

Choose a data source using the *Data Source Configuration* page. To access this page, locate **Maintenance** on the left navigation bar, then click **Data Source Configuration**. The *Data Source Configuration* page appears as shown in [Figure 43](#).

Data Source Configuration

Data Source Configuration

Get data from Route Recorders

Connect to a Replicating Modeling Engine

Enable Replication

Bring back data for the past

Enable Centralized Report Server

Report Server is required to run Alerts and IGP Reports

Replication Status		
IP Address	Databases	Status

Figure 43 Data Source Configuration Page

The *Data Source Configuration* page provides the following three options:

- **Get data from Route Recorders**—Use this option to disable replication of data on the Modeling Engine. To obtain network information, you must query individual Route Recorders.
- **Connect to a Replicating Modeling Engine**—Use this option in a deployment 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.
- **Enable Replication**—Use this option to begin replicating data from all Route Recorders in the deployment.

When you enable replication, you choose the amount of data to be copied from the network's Route Recorders to the centralized Modeling Engine. For example, choose **One Week** from the drop-down list to obtain data recorded over the last 7 days. You can bring back one week, two weeks, one month, or a maximum of 2 months of data.

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. This option allows you 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 120. First, you can archive data without stopping the recording process or requiring users to log off. Second, 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 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 System 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.

Note that unlike using 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 will not be archived until the following Monday, July 3 at 0:00. However, an “archive now” feature is available to capture data between intervals. This manual option requires you to stop recording on the database before archiving, and is described in [Manually Archiving Data](#) on page 141.



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. To access this page, locate **System** on the left navigation bar, then click **Archival Configuration**. The *Archival Configuration and Remote Storage* page appears as shown in [Figure 44](#).

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**
- FTP Server
- 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 44 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 128.
- 2 On the *Archival Configuration and Remote Storage* page, select the **Enable Archival** check box.
- 3 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, you can use the **Archive Selected Databases** button on the *Database Administration* page. Only offline databases can be archived. Therefore, 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 Locate **Maintenance** on the left navigation bar, then click **Databases**.

The *Database Administration* page is displayed as shown in [Figure 35](#).

- 2 From 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. To access this page, locate **Maintenance** on the left navigation bar, then click **Restore Archives**. The *Restore from Archive* page is displayed.

On the *Restore from Archive* page, the following text boxes appear:

- *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 119, 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 On the *Restore from Archive* page, supply 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, type 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.

- 2 Click to select one or more databases in the *Databases to Restore* list box that corresponds to the database to restore.
- 3 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 1, 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 6.0) 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, locate **Maintenance** on the left navigation bar and click **Software Update**. The *Software Update* page appears, as shown in [Figure 45](#).



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			
	Software Version	OS Version	
Installed Software and OS:	6.1.9-R	6.1.9	Installed: Mon Jun 2 14:05:01 2008
Alternate Software and OS:	6.0.82-R	6.0.82	<input type="button" value="Install Alternate Software and OS"/>

Note: Installing an alternate Software and OS will cause the system to be rebooted.

Operators currently connected: 0

Download Software Update			
URL:	<input type="text"/>		
Key:	<input type="text"/>		
<input type="checkbox"/> Use Proxy			
Host:	<input type="text"/>	Port:	<input type="text"/>
Username:	<input type="text"/>	Password:	<input type="text"/>

Figure 45 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 145.
- 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 147.

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 147.



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 On the *Software Update* page of the appliance where you are updating software, select the **Use Proxy** check box.
- 2 Type the host and port details for the proxy server.
- 3 If the proxy server is password protected, type the user name and password.
- 4 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 On the *Software Update* page, click **Check for Update**.

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, type the Update key provided by HP customer support.
- 3 Click **Update** to begin download and installation of the update.

This can take some time, depending on your connection speed, since well over 100 MB of data is transferred.

- 4 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**.

- 5 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 server, and then install the update from the local FTP 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:

- 1 Go to the HP Route Analytics Management System 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 155.
- 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 160, 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 From the *Home* page, click **Administration**, then click **Software Update** on the left navigation bar.

- 2 On the *Software Update* page, 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 161](#) for re-set instructions.

Using Top N Reports

The Top N Report provides a convenient way to run reports automatically and unattended in the background. It then conveniently delivers these reports at pre-configured time periods that suits your needs.

The Top N Report provides the following:

- Selection from a set of redefined reports
- Ability to set a time range and frequency of these reports
- List of scheduled reports, reports being generated, and reports that are currently generating
- Convenient email delivery of these reports to those needing them.

To configure Top N Reports, perform the following steps:

- 1 From the left navigation menu in the *Administration* page, find **System** and select **Reports**.

The *Top N Reports* window opens as shown in [Figure 46](#).

Top N Reports

Global Configuration Parameters

Database Name

Recipients

Report Configuration Parameters

Report Name	Report Type	Number of Elements
Traffic Groups	none ▾	100 <input type="text"/>
BGP Destination AS	none ▾	100 <input type="text"/>
BGP Exit Router	none ▾	100 <input type="text"/>
BGP Neighbor AS	none ▾	100 <input type="text"/>
Summary Exporters	none ▾	100 <input type="text"/>
Summary Link	none ▾	100 <input type="text"/>
VPN CoS	none ▾	100 <input type="text"/>
VPN Customer	none ▾	100 <input type="text"/>
VPN Egress PE	none ▾	100 <input type="text"/>
VPN Ingress P	none ▾	100 <input type="text"/>
VPN Ingress PE	none ▾	100 <input type="text"/>

Figure 46 Top N Reports Window

- 2 Type the name of the database that you opened when you started the client application.
- 3 Enter the email addresses of those needing these reports in the Recipients 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.

- 4 In the Report Type column, select the frequency of reports. The options you can choose from are none, daily, weekly, and monthly.
- 5 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.

- 6 After entering the report name, type, and number of elements, click on **Update** to activate Top N Report generation.

Creating Daily Reports

You can schedule a time for Route Analytics Management System to send daily reports summarizing the health of a unit and its recording processes along with BGP and IGP activity using the Mail page. The reports arrive via email. To access the *Mail* page, locate **System** on the left navigation bar, then click **Mail**. The *Mail* page appears as shown in [Figure 47](#).



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 System appliances.

Mail

Mail System Configuration

Mail Server:

Sender:

Recipient(s):

Report Setup

Configure daily generation and emailing of Health and Routing Reports or generate one of these reports now.

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.

Enable Health Report

Email

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 and standalone units with Route Analyzer enabled.

Enable Routing Report

Email

Report generation begins at:

Figure 47 Mail 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 On the *Mail* page, type the outbound mail server or relay in the **Mail Server** box using either a DNS name or an IP address. If you do not specify a mail server, the system attempts to send directly to the mail server(s) of the recipient(s).
- 2 In the Sender text box, type 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.
- 3 Type the recipient(s) e-mail address(es) in the **Recipient(s)** box. If you have more than one recipient, separate each recipient address with a comma.
- 4 Click **Update Mail Configuration**.

You can send a test message to the recipient(s) to verify receipt by clicking **Send Test Message**.

- 5 In the Report Setup portion of this screen, check the **Enable Health Report** to initiate the health report.
- 6 Click the **Email** box to have the report sent to the recipient.
- 7 Check the **Enable Routing Report** to initiate the routing report.
- 8 Check the **Email** box to have this report sent to the recipient.
- 9 Select the time you want the report to generate in the Report generation begins at: drop down menu.
- 10 Click **Update Report Configuration**.

Scheduling Daily Reports

To schedule daily reports, perform the following steps:

- 1 On the *Mail* page, select the **Enable daily reports** check box to send reports to the configured recipient(s) at a specific time each day.
- 2 Select the time to generate and send reports from the **Report generation begins at** drop-down list.
- 3 Click **Update Report Configuration**.

Understanding Daily Report Contents

The Health Report summarizing appliance health 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.

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 On the *Home* page, click the **Reports Portal** button at the top of the Home Page.
- 2 Click **Daily Reports** on the navigation bar.
- 3 Click on a report file name to download or view that report.



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.

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 MRTG files onto the appliance using FTP for correlation with routing events (see "The History

Navigator” chapter in the *HP Route Analytics Management System 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 101).
- 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 97).

To access the *FTP Server Configuration* page, find the left navigation pane and locate **System** → **FTP Server**.

The FTP Server Configuration window opens, as shown in [Figure 48](#).

FTP Server Configuration

Enable FTP Server

Update

Figure 48 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.

Viewing and Exporting Log Pages

You can view and export log files to help diagnose problems on a particular appliance. To access the *View Log* page, locate **Diagnostics** on the left navigation bar and then click **View Log**. This screen is shown in [Figure 49](#).

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) Type the page number to view in the **Page** text box. If you leave the text box empty, page 1 displays by default.

The screenshot shows the 'View Log' interface. At the top, there is a 'Remote Syslog Collector' field containing '192.168.0.104' and a 'Set Collector' button. Below this is a 'Filter' section with a 'Component' dropdown set to 'All', a 'Lines' dropdown set to '25', and a 'Page' text box containing '1' followed by 'of 362'. There is a checked checkbox for 'Show most recent first'. Below the filter section are three buttons: 'Apply Filter', 'Next Page', and 'Export Log as Plain Text' (which is located below a horizontal line and the word 'Log').

Figure 49 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 Type 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 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, the SVG format (Scalable Vector Graphic), 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 On the left navigation bar, locate **Application**, then click **Layout Backgrounds** to access the *Layout Backgrounds* page.
- 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**.



Note that binary images should not exceed 12 MB in size, and all 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 System User’s Guide*.

Using Diagnostic Functions

The system supports the diagnostic functions *ping* and *traceroute*. Use these functions to investigate network failures or outages. To access the *System Diagnostics* page, locate Diagnostics on the left navigation bar, then click **System Diagnostics**.

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 On the *System Diagnostics* page, type the IP address or DNS name of the destination device.
- 2 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 On the *System Diagnostics* page, type the IP address or DNS name of the destination device.
- 2 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, shown in [Figure 50](#).

To access the *Shutdown* page, locate **Maintenance** on the left navigation bar, then click **Shutdown**.

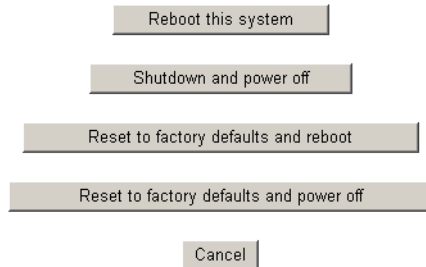
The following options are available on the *Shutdown* page:

- **Reboot this system**—Click this button to reboot the system. A confirmation page appears. 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. Then, using the previous system settings, the VNC server and recorders are automatically restarted. The message “Please wait for the system to reboot then click on Home” appears.

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



System uptime: 16 hours, 25 minutes

Figure 50 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 24. 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 License Feature Details

This appendix describes the license features associated with Route Analytics Management System. 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 4 Available License Features

Feature Name	Description
Protocol Licenses	Required for an appliance to monitor particular protocols. If the license for a given protocol (OSPF, ISIS, 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, ISIS, 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 4 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.
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 4 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, 33
- adding clients, considerations for, 33
- administration interface, selecting, 39
- Administration pages, 19, 95
 - logging in, 22
- administrative domain
 - creating, 45
 - deleting, 72
 - top-level, 45
- administrator default user name and password, 22
- Administrator password
 - changing, 24
- Administrators, 97
- alias
 - BGP AS, 59
 - interface, 39
- Analysis mode, 15
- appliance
 - reboot, 160
 - reset, 161
 - shutdown, 160
- application interface, 15
- Archival Configuration and Remote Storage page, 140

- archiving, 139
 - automatic, 139
 - configuration, 140
 - enable, 141
 - end time, 143
 - filename format, 142
 - frequency of, 139
 - manual, 141
 - restoring data, 142
 - start time, 143
- areas
 - contiguous, 52
 - multiple, 52
- AS
 - BGP, 59
 - configuring for EIGRP protocol instance, 57
- authentication
 - local, 99
 - MD5, 92
 - OSPF, 73, 91
 - type, 100
 - user, 22
- autonomous system
 - see AS

B

- backing up
 - client unit, 131
 - master unit, 133
- Backup and Restore page, 120

- backup file
 - creating, 121, 124
 - deleting, 128
 - downloading, 126
 - FTP, 131
 - restoring, 127
 - restoring from remote server, 129
 - saving, 125
 - transferring, 131
 - uploading, 126
- backup on unit's disk, 122
- BGP
 - aliases, AS, 59
 - autonomous system (AS), 59
 - configuring, 59
 - protocol
 - instances, 59
- BGP Reports, 16
- browsers
 - supported, 20
- button
 - Make Master, 32
 - Re-apply All, 28
 - Relinquish Master Role, 35, 36
 - Remove all licenses on this unit, 28
 - Restore Now, 144

C

- callback, enable, 94
- Cisco router loopback interface, 93
- CLI Access, 97
- CLI Access users, 97
- client, 20
 - adding, 33
 - removing, 36
- client list, 32

- client unit
 - backing up, 131
- clock
 - setting, 29
- collector
 - traffic flow, 11
- components
 - data flow, 11
 - RAMS, 10
- configuration
 - additional tasks, 86
 - administration interface, 39
 - BGP, 59
 - client, 20
 - database
 - deleting, 118
 - renaming, 119
 - DHCP, 38
 - Flow Analyzer, 83
 - Flow Collector, 74
 - for recording, 43
 - FTP server, 155
 - GRE tunnels, 89
 - hierarchy, 44, 45
 - hostname, 38
 - loopback interface, 93
 - master, 20
 - option card, 41
 - overview, 19
 - Route Recorder, 44, 60
 - static route, 40
 - support access, 93
 - traffic instance, 74
 - tree, 44
 - users, 24
 - VNC, 112
- considerations for, 41
- cookies, 22
- CoS groups, 107

D

daily reports

- creating, 151
- scheduling, 154
- understanding contents, 154
- viewing saved, 155

database

- administration page, 115
- archiving, 141
- backing up, 120
- deleting, 118
- deleting and start recording to new, 119
- online vs. offline, 117
- renaming, 119, 143
- restored filename, 144
- restoring, 120
- restoring archived, 143
- unarchived, 141
- using offline, 118
- using online, 120

Database Client, 164

Database Server, 164

Data Configuration page, 137

data source

- choosing, 137

default, factory, 160

DHCP, 38

diagnostics, 159

- ping, 159
- traceroute, 160

distributed configuration

- applying license keys, 24
- archival settings for, 141
- archiving data for, 140
- choosing data source for, 136
- configuring route recorder in, 15
- deleting a database within, 118
- designating master and client roles for, 30
- IGP and BGP reports for, 16
- updating software for, 144
- updating software with internet access for, 146
- updating software without internet access, 147

distributed configuration

- defined, 20

DNS

- server, 39

downloading

- software updates, 144

E

EIGRP

- multiple areas, ASs, 52
- multiple interfaces, coverage and, 54
- protocol instance, configuring ASs, 52

enable archival, 141

export

- log, 158

F

factory defaults, 160

features, 9

filename, restored database, 144

Flow Analyzer, 11, 31, 84, 163

- configuration, 83
- starting and stopping, 84

Flow Collector, 11, 31, 163
configuration, 74
starting and stopping, 77

FTP
file transfer, 156
file upload, enabling, 156
file uploads, 156
server configuration, 155

G

GRE tunnels, 11, 89

Guests, 97

H

hierarchy
configuration, 44, 45

History Navigator, 16

Home page, 20

HTTP POST, 32

I

ICMP redirects, 40

IGP Reports, 16

image, importing
importing
background image, 159

interface
administration, 39
alias, 39
application, 15
removing from protocol instance, 72
web, 19

Internet Explorer, 21

IP address, 39
before you change on a system, 38

K

keys, license, 163

L

layout
uploading backgrounds
backgrounds, 158

LDP, in IPv4 deployments, 76

LDP peering sessions
establishing, 74

license
applying, 24
install new key, 26
key, 24
remove all, 28
updating licenses, 24

license key, 163
database client, 164
database server, 164
flow analyzer, 163
flow collector, 163
master capability, 164
modeling engine, 164
MPLS VPN prefix count, 165
protocol, 163
route analyzer, 164
router count, 165
Route Recorder and GUI, 163
software update, 165
VPN customer reports, 164

license reapplying, 24

list
client, 32

local authentication, 99

log
export as plain text, 158
viewing, 157

logging in, 22

- login attributes, 103
- login page, 22
- loopback
 - interface, 56, 93
 - interface, on Cisco router, 93

M

- Mail page, 151
- mail system
 - configuring, 152
- map
 - Routing Topology, 15
- master, 20
 - assigning, 31
 - license key, 164
 - password, 32
 - relinquish, 35
 - removing client, 36
- master access password, 32
- Master Capability, 164
- master status, relinquishing, 35
- master unit
 - backing up, 133
- master unit in, 20
- MD5 authentication, 92
- mode
 - Analysis, 15
 - Monitoring, 15
 - Planning, 15
- Modeling Engine, 11, 31, 164
- Modeling engine
 - adding a second modeling engine, 34
- Monitoring mode, 15
- Mozilla, 21

- MPLS VPN
 - deployments, 74
- MPLS VPN Prefix Count, 165
- multiple port options, 41

N

- NetFlow, 11
- Netscape, 21
- network
 - configuration, 36
 - DHCP, 38
- Network & Interface Configuration page, 36
- NTP server, 28, 29

O

- online/offline databases, 117
- Operators, 97
- option cards, configuring, 41
- OSPF
 - area ID format, 71
 - authentication, 73, 91
 - contiguous areas, 51
 - loopback interface, 56
- overwrite layouts, 127, 130, 135

P

- password
 - Master Access, 32
- Path Reports, 16
- ping, 159
- Planning mode, 15
- Planning Reports window, 16
- prefix source, defined, 76
- previous version, revert to, 148

privileges, 101

protocol

 BGP, 59

 instance, deleting, 72

 instance, VPN, 61

 license keys, 163

 link-state, 10

 supported, 10

Protocol Licenses, 163

Q

queries, configuring server, 65

query server, 65

R

RADIUS, 58

RADIUS Server, 99

RAMS

 components of, 10

 reverting to previous version, 148

 web server, 20

re-apply all, 28

reboot, 160

rebooting the system, 160

recorder

 NetFlow, 11

 routing, 10

Recorder Configuration page, 44

recording, configuration, 43

remote server, adding, 128

remove all licenses, 28

replacing

 client unit, 131

 master unit, 133

reports

 and mail, 152

 BGP, 16

 daily, 151

 deleting instance, 85

 IGP, 16

 Path, 16

 Planning, 16

 scheduling daily, 152

 Traffic, 16

 using top N, 149

reset to factory defaults, 161

restore

 archived data, 142

 databases, 143

 from backup on unit's disk, 123

Restore from Archive page, 142

revert to previous version, 148

route

 static, configuring, 40

Route Analyzer, 164

router

 count, 165

 login for EIGRP, 58

Router Count, 165

Route Recorder, 10, 31

 configuration page, 44

 static information collection, 64

Route Recorder and GUI license, 163

route reflectors, 60

Router Recorder

 starting and stopping, 70

Routing Topology Map, 15

S

- server
 - database, 164
 - DNS, 39
 - FTP, 155
 - NTP, 28, 29
 - remote, 128
 - VNC, 112
- SFTP, as alternative to FTP, 156
- shutdown
 - options, 160
 - page, 160
- SMB, enabling, 128
- SNMP, 68
 - Agent configuration, 42
 - and static information collection, 64
- software
 - reinstalling previous version, 148
 - updating, 165
- Software Update
 - license, 165
 - page, 144
- SSH, 40, 58, 93, 97
- static information collection, 64, 65
- static route, 41
 - adding, 41
 - deleting, 41
- static route, configuration, 40
- status table, 78
- support access, configuring, 93
- supported, 159
- system
 - reboot, 160
 - shutdown, 160
- System Diagnostics page, 160
- system settings, viewing, 43

T

- TACACS, 58
- TACACS+
 - class of users, 97
- TACACS Server, 99
- time
 - setting, 28, 29
- time and date
 - synchronizing with NTP server, 28
- Time and Date page, 28
- top N reports, 149
- topology
 - map, 15
- traceroute, 160
- traffic
 - configuration status, 78
 - deleting instance, 82
 - instance, 74
- Traffic Groups
 - creating, 103
- traffic groups
 - creating, 103
 - editing, 107
- Traffic Reports, 16
- tree, configuration, 44
- tunnels
 - GRE, 11, 89

U

- Units page, 32
- updating software, 144
- upload
 - FTP, 156
- User accounts, updating existing, 102
- User Administration page, 24

- user interface
 - application, 15
 - web, 14
- user name and password, default, 22
- User privileges, 97
- users
 - adding, 24
 - CLI access class, 97
 - creating accounts, 101
 - login attributes, 103
 - privileges, 101
 - updating accounts, 102
- uses of by the appliance, 39

V

- v3 profiles, configuring, 68
- View Configuration page, 43
- viewer, 14
 - VNC
 - recommended use of, 23
 - X Window System
 - recommended use of, 23
- visibility of, 41
- VNC, 14, 23
 - configuration, 112
 - connecting to persistent session, 114
 - on-demand sessions, 114
 - server, 112
 - start, stop server, 112
 - viewer, 114

W

- web browser
 - supported, 20
- web browser, cookies, 22
- web interface, 14, 19
- web server, 20

X

- X Window System, 14, 23
 - evaluation license, 23