HP OpenView
Route Analytics Management System

User's Guide

Software Version: 3.7

Manufacturing Part Number: BA129-90011

Document Release Date: November 2005

Software Release Date: November 2005

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Contains software from 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

Visit the HP OpenView web site at:

http://www.managementsoftware.hp.com/

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1

Introduction

About Route Analytics Management System

Route Analytics Management System is an IP Route Analytics tool that listens to dynamic routing protocols and builds a real-time routing topology map. By leveraging the intelligence of the IP control plane, RAMS helps you visualize and understand the dynamic operation and view the inner workings of your IP network.

RAMS has several major areas of contribution:

- **Unified, real-time routing topology view**. Complex topologies can be viewed hierarchically, or by protocol, AS, or IGP area. The History Navigator lets you play back a history of your routing topology changes.

- **Monitoring and alerts**. RAMS can monitor vital service parameters (network churn, prefix flaps, and son), watch for changes in specific end-to-end service paths and prefixes, and look for degrading redundancy.

  Beyond monitoring, RAMS can raise alerts on all watched parameters to head off costly outages.

- **Interactive routing analysis**. With a comprehensive routing base and a complete event history, RAMS lets you do before and after comparisons and detailed event analysis to help you rapidly establish the cause of the problem.
- **Planning support**. RAMS can show you the traffic patterns to help you 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 would respond to specific failures or upgrades.
- **Reports**. RAMS reports give you a view on trends, and let you identify and analyze emerging issues before they become problems. Web-based reports can be generated for any recorded time period, which can show you key information about network health.

RAMS can concurrently monitor most major routing protocols (OSPF, IS-IS, BGP, and EIGRP) across multiple domains and autonomous systems from a single appliance. The RAMS map is updated whenever the routing topology changes, providing an accurate, real-time view of how the network is directing traffic. RAMS identifies unstable routes and other anomalies that are undetectable by SNMP-based management tools because they are not device-specific problems. RAMS stores this real-time information, and lets you later replay the historical data for forensic analysis. RAMS offers several powerful graphical tools that help you to analyze the real-time and historical data that it collects.

RAMS provides the following key benefits:

- Increases Network Availability
  - Detects disruptions in IP routing and common IP faults that many management tools cannot diagnose.
  - Prevents service outages by identifying IP layer anomalies before they become problems.
  - Provides an efficient top-down approach to determining the root cause of failures, rather than deducing the cause based on the volume of alarms.
  - Enables the diagnosis and elimination of intermittent problems.

  - Verifies changes to routing redundancy.
  - Prevents service outages by providing alerts on routing redundancy changes.
  - Reduces the time required to pinpoint and resolve network faults.
- Maximizes Network Performance
  - Accurately shows whether the network is operating as planned.
  - Monitors routing changes and provides alerts on changes that may degrade performance.
  - Identifies undetected routing instabilities that affect services.
  - Enables *“what-if”* analysis for route path optimization.
  - Correlates routing events with external performance data for root cause determination.
  - Minimizes common configuration errors during maintenance.
- Reduces Total Operating Cost
  - Reduces lost productivity and customer dissatisfaction due to network changes.
  - Improves the productivity of network operations staff by reducing the time spent in fault isolation and root cause analysis.
  - Reduces capital expenditures by maximizing existing network asset utilization.
  - Minimizes the demands on the engineering resources required to tackle routing problems.
  - Frees up IT resources to focus on strategic initiatives, rather than problem resolution.
  - Improves service assurances for reduced SLA penalties.

The RAMS appliance has the following key capabilities:

- IP routing (Layer 3) visualization, monitoring, and routing event data collection.
- Real-time and historical problem detection and diagnosis.
- Network change analysis and scenario planning.

- Proactive alerts to a network management system on IP layer changes, anomalies, or outages.
- Detailed reports for network routing analysis and long-term trending.

Table 1 lists the key features of the RAMS appliance.

Table 1 Key Features

Feature	RAMS
Multiprotocol	Concurrent support for OSPF, IS-IS, BGP, EIGRP
Multiuser	Accessed from any browser, anywhere
Administration	Web based (HTTPS)
Multidomain	Via multiple interfaces or GRE tunnels
Graphical Topology View	Shows current routing topology at a glance
Event logging	Via syslog and SNMP traps
API	Via XML-RPC
Memory Options	2 GB or 4 GB*
Built-in Network Interface	2-port 10/100/1000 Base-TX Copper
Optional Network Interfaces**	2 PCI-X slots (see HP Proliant DL360 documentation)

* 4 GB memory is available for very large networks and to support concurrent users.

** Only one PCI card may be added with optional ports.

The actual performance of RAMS in large networks depends on network characteristics such as protocols, the number of routers, the number of prefixes, the network organization in domains, and other parameters. A RAMS representative can run a standard RAMS performance estimator program that utilizes network characteristics as input to determine the most suitable RAMS configuration for your network.

Basic Operation

The RAMS appliance connects physically either directly to one of the router ports, as shown in Figure 1, or through a switch or hub. It establishes communication with several routers in the network via the routing protocol over this physical connection. As noted in the RAMS Appliance Setup Guide, you should connect the unit to the core routers. This is a *passive* neighbor relationship because RAMS listens to the routing updates but never sends any routes.

In a link-state protocol (OSPF or IS-IS), each router knows of all adjacencies in the network. This is because link-state protocol update messages provide the complete routing topology. It is only necessary to listen to the routing protocol in one location to get the topology information for the whole network (of one *area*).

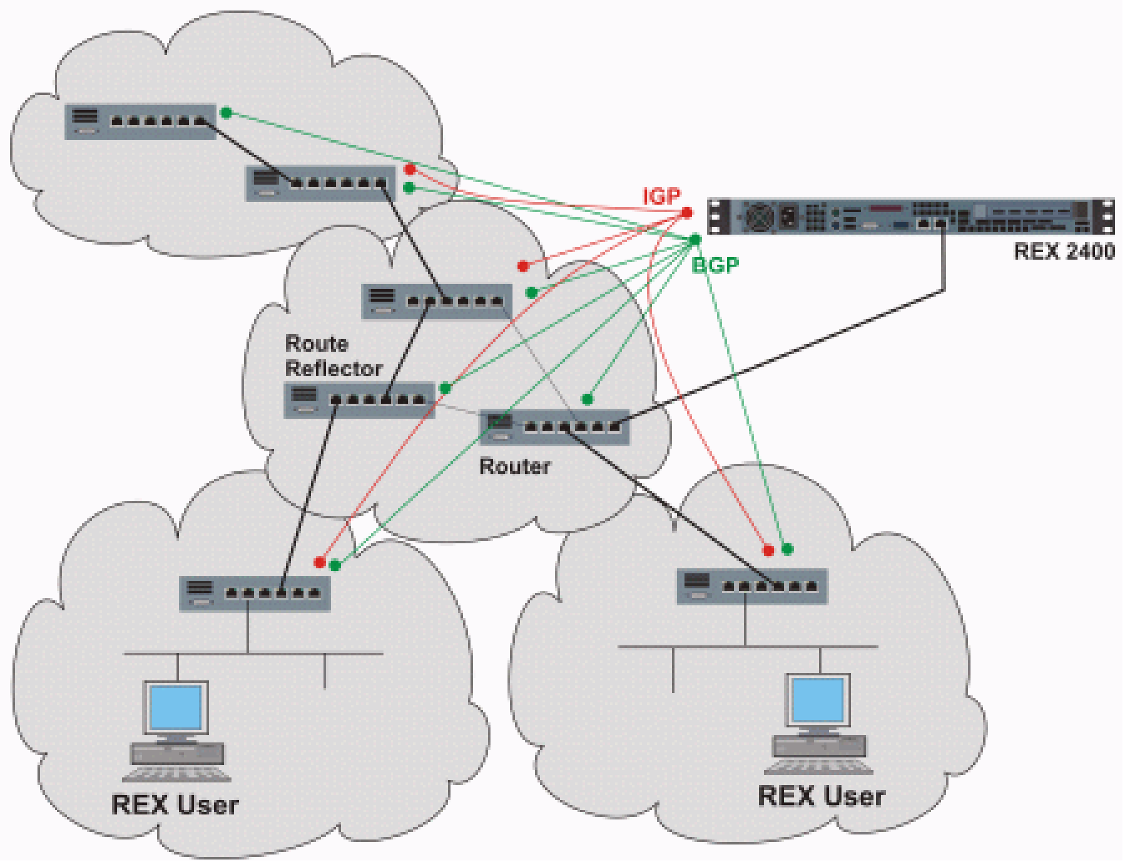


Figure 1 Basic RAMS Connection to a Network

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.

A network can be made up of numerous domains of autonomous systems (ASs). The ASs normally run one or more interconnected interior gateway protocols (IGPs). These ASs are referred to as *private enterprise internets* and RAMS can concurrently monitor all of the routing protocols within these private enterprise internets. Figure 1 shows how the RAMS appliance can connect to multiple areas to monitor all of the routing protocols within private enterprise internets. Thus, RAMS enables you to view the entire network as a single, integrated system. The RAMS 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.

A private enterprise internet often consists of multiple IP networks running separate IGPs. These are interconnected by using border gateway protocol (BGP) or route redistribution among the IGPs. In effect, it is a privately controlled internet. Private enterprise internets are used extensively in enterprises, government, education, and even service provider networks.

Similarly, RAMS supports major service provider networks, monitoring multiple BGP connections to peer and customer networks, while analyzing full Internet routing tables.

After RAMS acquires the network topology, it maintains a real-time topological view of the network. Initial network acquisition is accomplished in a matter of minutes in most cases, but can take up to approximately an hour for an EIGRP network. After RAMS acquires the network topology, you can easily display detailed data about routing events such as link status, link metrics, and new prefixes. This lets you diagnose and troubleshoot problems.

Users connect to the RAMS appliance by using the X Window system or Virtual Network Computing (VNC). VNC is a desktop remote-control application.

Installing the RAMS appliance is a simple process that consists of setting up the administration IP address and other basic parameters, and connecting to one or more routing domains or areas.

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*.

Chapter 2, “Configuring RAMS” explains how to set up user accounts, SNMP traps, and other features to complete the RAMS configuration.

2

Configuring RAMS

The RAMS appliance is configured using a standard Web browser interface. This chapter details the steps involved in the configuration process and also introduces certain administration functions, such as the software update facility and the log viewer.

Warning **The *RAMS Appliance Setup Guide* describes how to physically install the RAMS appliance, and perform basic configuration tasks, such as getting it networked. You must finish all of the tasks in that document before you use the tools described in this chapter to fully configure the system.**

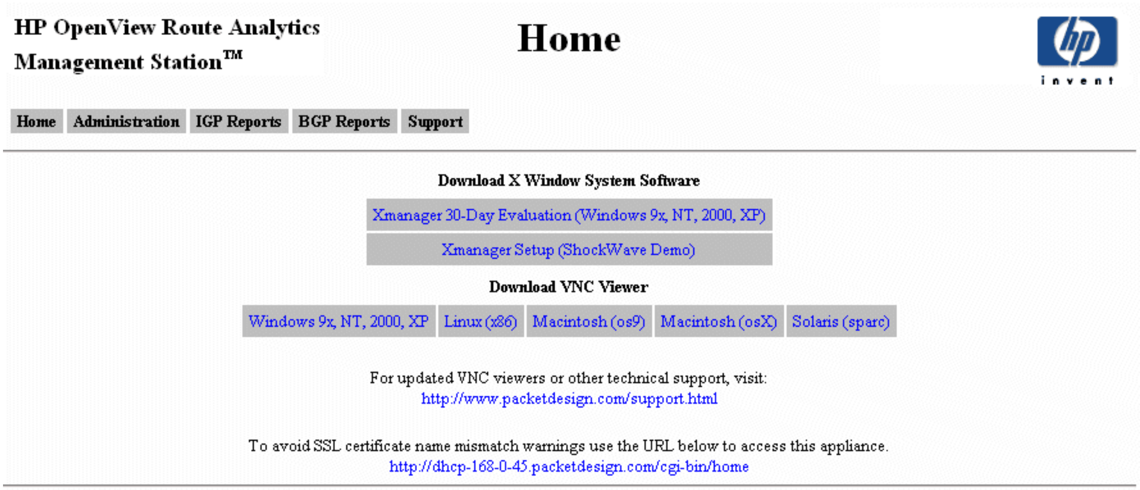
Connecting to the RAMS Home Page

RAMS has a built-in web server, and this provides the primary administrative access. The first configuration step is connecting to the RAMS Home page by using a supported browser.

RAMS supports the following browsers:

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

To connect to the RAMS Home page, open a standard web browser and enter the initially configured address or hostname. The Home page displays, as shown in Figure 2.



HP OpenView Route Analytics Management Station™

Home

Download X Window System Software

Xmanager 30-Day Evaluation (Windows 9x, NT, 2000, XP)

Xmanager Setup (ShockWave Demo)

Download VNC Viewer

Windows 9x, NT, 2000, XP | Linux (x86) | Macintosh (os9) | Macintosh (osX) | Solaris (sparc)

For updated VNC viewers or other technical support, visit:
http://www.packetdesign.com/support.html

To avoid SSL certificate name mismatch warnings use the URL below to access this appliance.
http://dhcp-168-0-45.packetdesign.com/cgi-bin/home

Figure 2 RAMS Home Page

The administration and report pages are accessed from the *Home* page. The X Window system or VNC is required to run the RAMS software, and the *Home* page provides download links to both types of 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.

Note The third-party X Window system software provided with RAMS comes with a 30-day evaluation license. After this initial 30-day period, you must purchase a license from NetSarang Computer, Inc., to continue using the software.

Using the Administration Pages

Use the administration pages to do the following types of tasks:

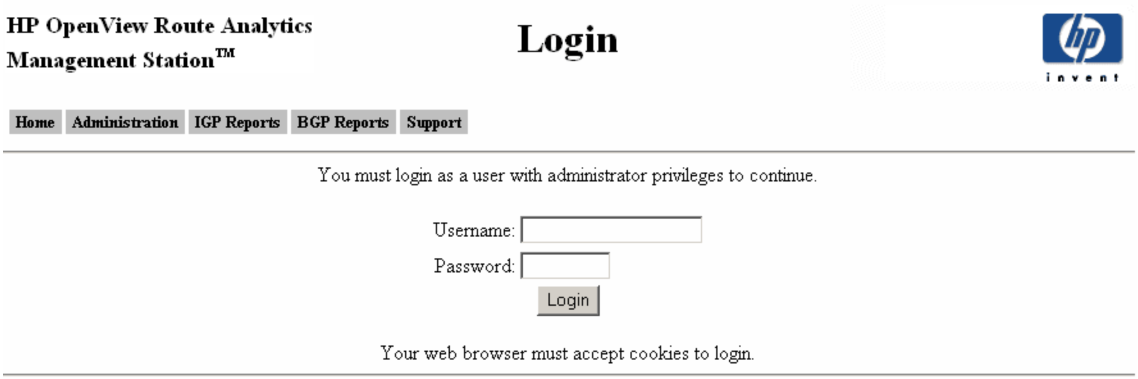
- Manage software licenses. See License Keys on page 88.
- Configure the Route Recorder, and start and stop the recording process. See Configuring the Route Recorder on page 56.
- Configure the VNC server. See VNC Server Configuration on page 31.
- Configure RAMS alerts. See Chapter , “Alerts.”
- Configure queries. See Appendix , “XML RPC Queries.”
- Configure the system settings. See System Configuration on page 35.
- Obtain software updates from HP. See Software Update on page 51.
- Give new users access to the RAMS appliance. See User Administration on page 29.
- View the log. See Viewing the Log on page 85.
- View the RAMS appliance configuration. See Viewing the Configuration on page 50.
- Delete and rename databases. See Database Administration on page 81.

Logging In for RAMS Administration

The first configuration step involves logging into the administration pages and setting the login parameters for RAMS users. When you configure the RAMS appliance for the first time, it is recommend that you configure all settings in the order outlined in this chapter. This ensures that all required functions are configured correctly.

The administration pages are password-protected and user input is encrypted using SSL. A confirmation security dialog appears the first time you enter the Web site. The secure Web pages have a certificate signed by HP. Click **Yes** to accept the certificate and allow the secure Web pages to open.

Click the **Administration** link on the *Home* page to open the Administrator *Login* page, shown in Figure 3.



You must login as a user with administrator privileges to continue.

Username:

Password:

Your web browser must accept cookies to login.

Figure 3 **Administrator Login Page**

Note Your browser must accept cookies to allow login.

To log in, enter the default administrator user name (`admin`) and the default password (`admin`), and click **Login**. After a period of inactivity, you must repeat this login to have continued access to the Administration pages. You can change the password at any time through the *User Administration* page described in the next section. For security reasons, HP recommends that you change the administrator password when you first log in, and on a regular schedule after that.

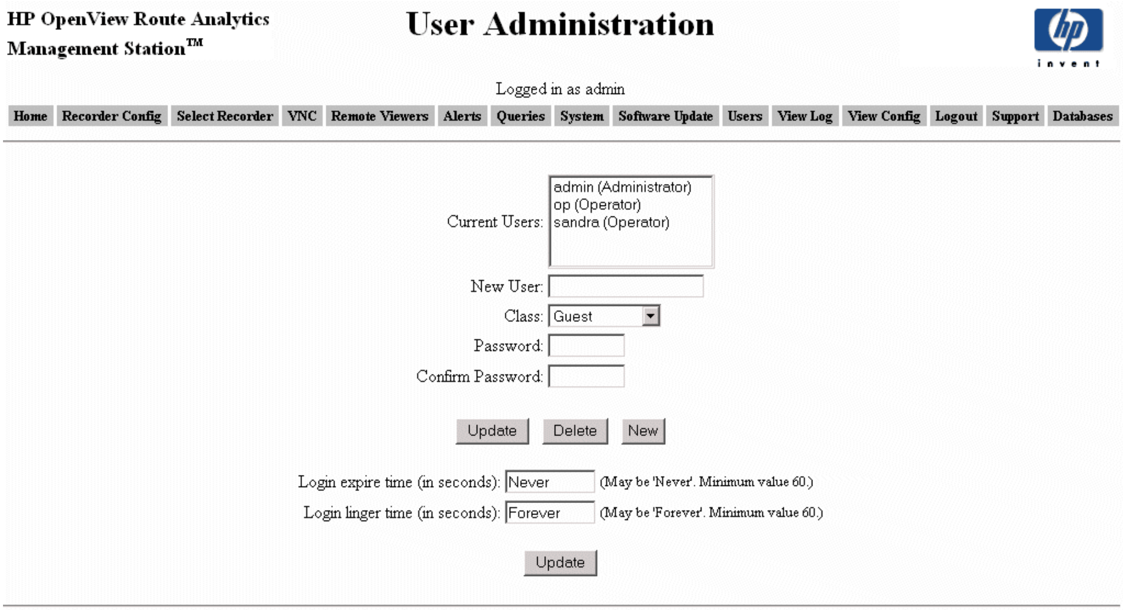
Note After you log in, the default page is either the *Route Recorder Configuration* page (for units licensed as Recorder) or the *Select Recorder* page (for units licensed as View Server only). The links and buttons on the administration pages might differ from those shown in the examples in this guide, depending on the functions for which your system is licensed. If your system is not licensed for a particular function (for example, the View Server function), the links or buttons related to that function do not appear on the administration pages.

User Administration

Click the **`Users`** button on the *Route Recorder Configuration* page to access the *User Administration* page, shown in Figure 4. Add users and set the login parameters on this page.

RAMS supports three types of users:

- Administrators, who have full access privileges, such as configuring other users and setting alerts.
- Operators, who can access the RAMS application and the report pages, but who do not have any administration privileges.
- Guests, who are view-only users, have the same access as operators but cannot save or delete routing topology map layouts. See Chapter 5, “The Routing Topology Map”.



Logged in as admin

Current Users: admin (Administrator)
op (Operator)
sandra (Operator)

New User:

Class: Guest

Password:

Confirm Password:

Login expire time (in seconds): Never (May be 'Never'. Minimum value 60.)

Login linger time (in seconds): Forever (May be 'Forever'. Minimum value 60.)

Figure 4 User Administration Page

To add a new user, complete the user name, class, and password fields, and click **New**.

Note If you change the class for the administrator user name you entered to log in, or if you delete that user, you will be automatically logged out.

Change a Password or Class

Select the user name to be changed from the Current Users list, then select the desired class for that user name or enter the new password. Click **Update** below the passwords to make the change.

User-Initiated Password Change

Users can change their passwords by using the **Change Password** link in the row at the top of the web page, after they are logged in.

Session Login Timers

As a security precaution, you can restrict the time between the start of login activity and entry to the interface. Set this value in the Login Expire Time box. After the value is set, a user must enter his or her password and click **Login** within the specified time period.

Another security setting is the time period between keystrokes after a user logs in. Set this time in the Login Linger Time box. If the specified time elapses without a keystroke from the user, the user is automatically logged out.

These two timeouts can be changed using the entry boxes and **Update** button at the bottom of the page.

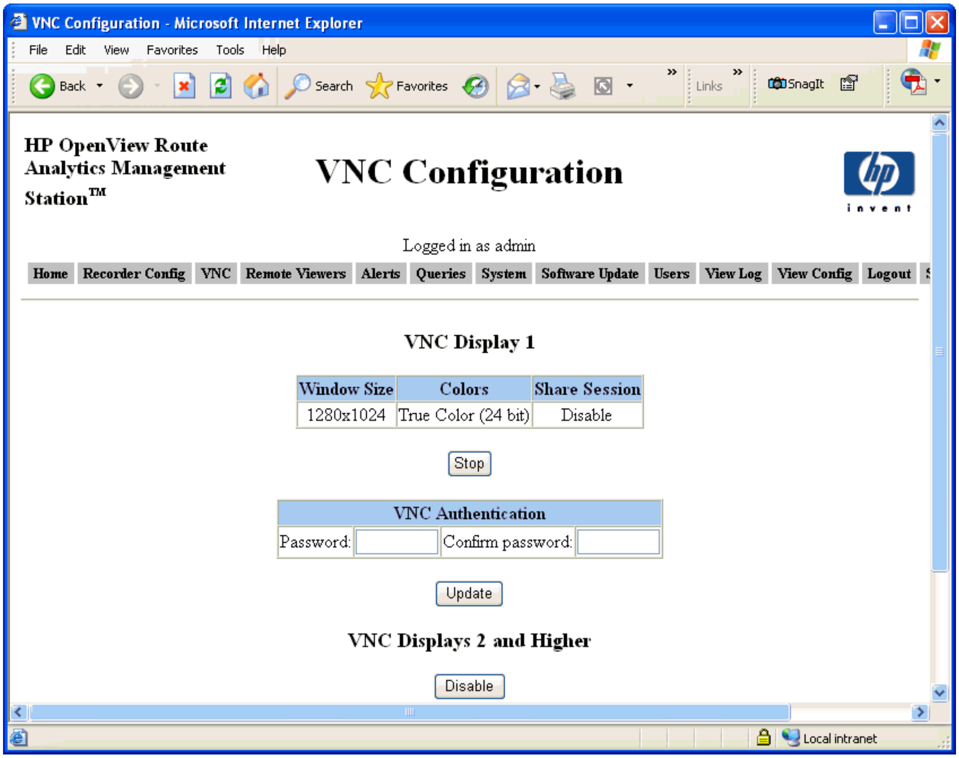
VNC Server Configuration

If you plan to use a VNC client to access RAMS (see Chapter 3, “RAMS Clients”), you need to configure the VNC server before users can access RAMS using the VNC viewer on a desktop machine. Alternatively, if all RAMS users will use the X Window system rather than VNC, you might wish to stop the VNC server.

You can log into a persistent VNC session that is shareable by multiple operators, or you can log into a session created on demand if both session types are enabled.

Click the **`VNC`** link on the *Route Recorder Configuration* page to access the *VNC Configuration* page, shown in Figure 5.

Note 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.



HP OpenView Route Analytics Management Station™

VNC Configuration

Logged in as admin

VNC Display 1

Window Size	Colors	Share Session
1280x1024	True Color (24 bit)	Disable

VNC Authentication

Password: Confirm password:

VNC Displays 2 and Higher

Figure 5 VNC Server Configuration Page

Configure the following on the *VNC Configuration* page:

- The window size, which is the size of the VNC viewer’s virtual screen.
- The number of colors displayed.
- The settings to enable or disable session sharing.
- The VNC authentication password for the persistent session (VNC display 1).
- The availability of on-demand sessions using VNC displays 2 and higher.

All users who access RAMS using VNC share the settings configured on this page.

After configuring the VNC settings, set a VNC authentication password. Enter the password information in the fields provided and click **`Update`**.

After clicking **`Start`** to start the VNC server, the button toggles to **`Stop`**. If VNC server changes are required in the future, stop the VNC server before making the changes.

Note 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 client, 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 RAMS 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.

Note 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 to RAMS, use the **`Stop/Start`** button on the *VNC Configuration* page to stop and restart the VNC Server.

On-Demand VNC Sessions

RAMS allows multiple operators to log into their own sessions initiated on demand and not shared.

After you start the VNC client, specify the VNC display window size by typing the hostname, a colon, and the VNC display number that corresponds with the window size you want, as shown in Table 2. For example, type *hostname*:8 to connect to the VNC session with a 1280 × 1024 pixel window size. All of the window sizes will display in 24-bit true color. The VNC client will display a login window where you should log in using a user name and password you configured on the *User Administration* page (see page 29).

Table 2 **VNC Configuration Window Settings**

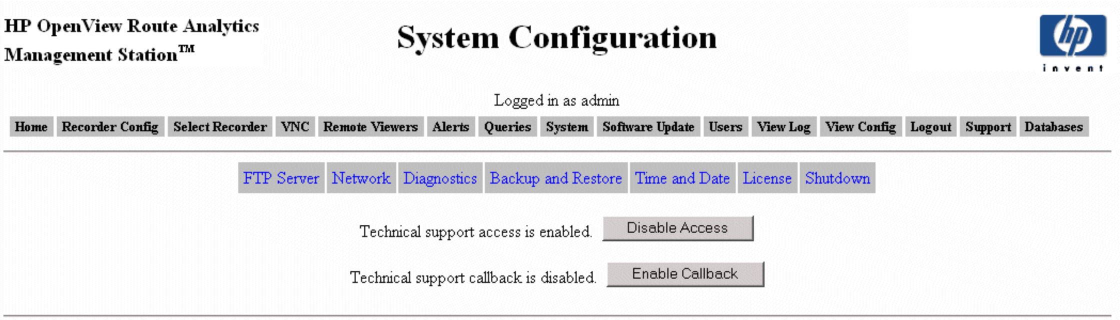
VNC Display Number	Window Size (Pixels)
1	Configure on VNC Configuration Page
2	1016 × 700
3	1024 × 768
4	1152 × 768
5	1152 × 864
6	1152 × 900
7	1280 × 864
8	1280 × 1024
9	1400 × 1050
10	1600 × 1200

If you and another user connect to the same display number, such as *hostname*:8 as in the example above, RAMS creates separate VNC sessions so that both users can operate independently. RAMS allows multiple users to connect to on-demand VNC sessions up to the user count limit displayed on the License page.

Note When you disconnect from an on-demand VNC session, RAMS terminates the session immediately.

System Configuration

The next step in the configuration process is system configuration. Click the **System** link to open the *System Configuration* page, shown in Figure 6.



Technical support access is enabled.

Technical support callback is disabled.

Figure 6 System Configuration Page

System Configuration Overview

System configuration involves the following high-level steps:

1 Setting the time and date (page 36).

2 Configuring the network interfaces (page 37).

3 Configuring the FTP Server (page 48).

4 Enabling and disabling Technical Support access (page 49).

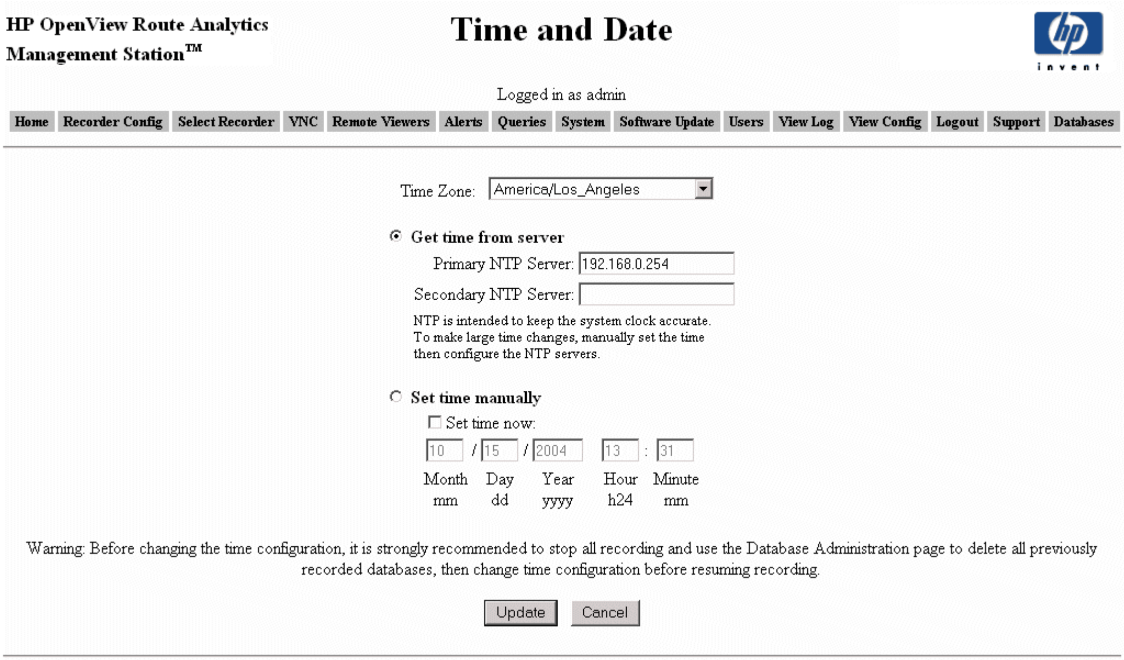
Other functions available on the *System Configuration* page are:

- Scheduling a time to send a daily e-mail report summarizing network activity (see page 42).
- Backing up and restoring data (see page 45).
- Running system diagnostics (see page 47).
- Shutting down the system (page 91).

Setting the Time and Date

Click **`Time and Date`** on the *System Configuration* page to access the *Time and Date* page, shown in Figure 7. The *Time and Date* page lets you change the time zone and specify whether the internal RAMS clock is set manually, or sets its time from an NTP server.

Note Access to the *Time and Date* page is not permitted if recording is in progress.



HP OpenView Route Analytics Management Station™

Time and Date

Logged in as admin

Time Zone: America/Los_Angeles

● Get time from server

Primary NTP Server: 192.168.0.254

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:

Month mm	Day dd	Year yyyy	Hour h24	Minute mm
10	15	2004	13	31

Warning: Before changing the time configuration, it is strongly recommended to stop all recording and use the Database Administration page to delete all previously recorded databases, then change time configuration before resuming recording.

Figure 7 Time and Date Page

To set the time and date:

1. Select the time zone.
2. Choose whether to set the time and date from an NTP server or set it manually.

- If time is to be obtained via NTP, you can specify either one or two NTP servers.
- If time is to be maintained manually, and needs to be corrected now, click the **`Set time now`** checkbox and adjust the time fields as necessary.

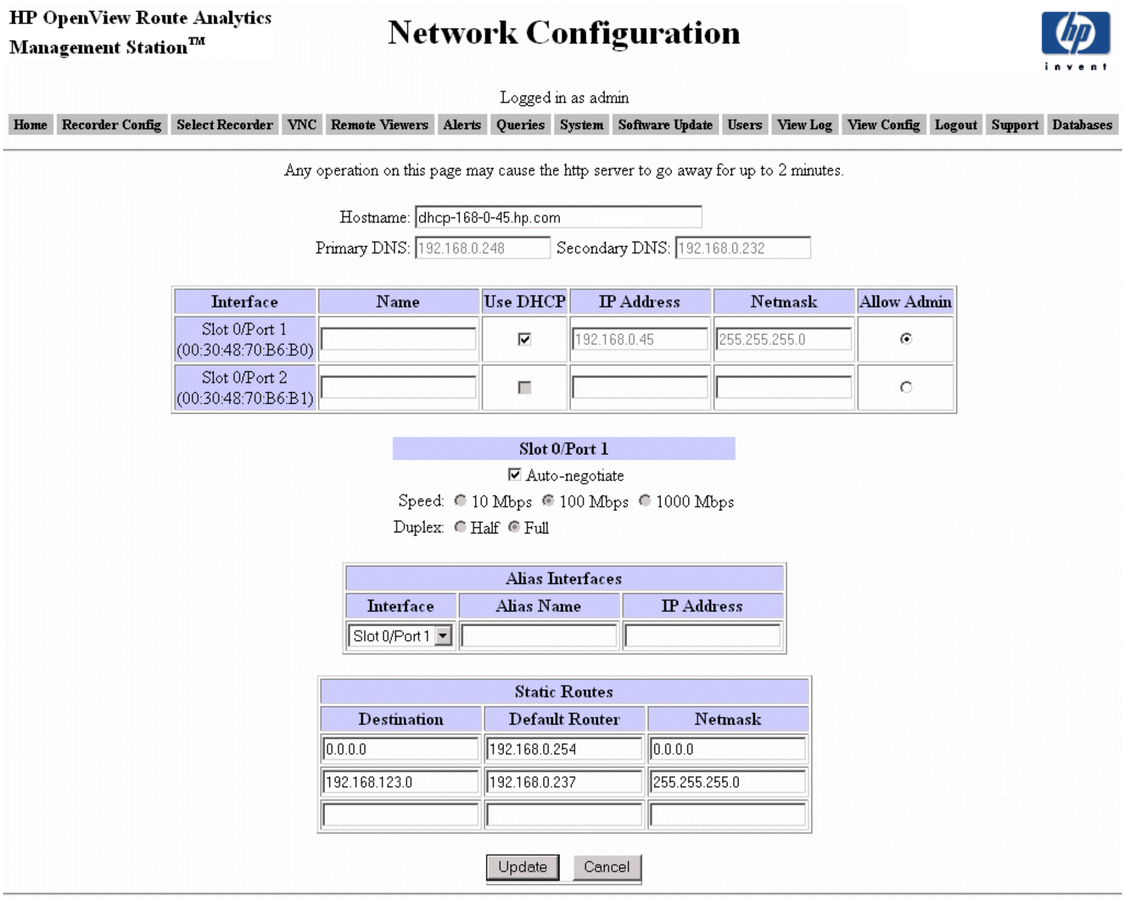
3 Click **`Update`**.

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

Note HP strongly recommends that the RAMS clock be synchronized with an NTP server to avoid ever having to make manual time adjustments, potentially backwards in time. Because the recorded routing topology database requires that time progress monotonically, the RAMS NTP dæmon 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 getting time from the NTP server. After the time is set using the NTP server option, verify the results on the *View Configuration* page.

Configuring the Network Interfaces

Click **`Network`** on the *System Configuration* page to access the *Network Configuration* page, shown in Figure 8. Use the *Network Configuration* page to set the RAMS IP address, the netmask, default router, and primary and secondary DNS servers.



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

Hostname: dhcp-168-0-45.hp.com

Primary DNS: 192.168.0.248 Secondary DNS: 192.168.0.232

Interface	Name	Use DHCP	IP Address	Netmask	Allow Admin
Slot 0/Port 1 (00:30:48:70:B6:B0)		☑	192.168.0.45	255.255.255.0	●
Slot 0/Port 2 (00:30:48:70:B6:B1)		□			○

Slot 0/Port 1

☑ Auto-negotiate

Speed: ○ 10 Mbps ● 100 Mbps ○ 1000 Mbps

Duplex: ○ Half ● Full

Alias Interfaces		
Interface	Alias Name	IP Address
Slot 0/Port 1		

Static Routes		
Destination	Default Router	Netmask
0.0.0.0	192.168.0.254	0.0.0.0
192.168.123.0	192.168.0.237	255.255.255.0

Figure 8 Network Configuration Page

Before configuring the network manually or using DHCP, enter the hostname of RAMS in the *Hostname* field.

To configure the network using DHCP, perform the following steps:

1. Check the **`Use DHCP`** check box.
2. Enter a name to identify the interface.
3. Check **`Auto-negotiate`** 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.

To configure the network manually, perform the following steps:

1 Enter the following information:

- Primary DNS
- Secondary DNS (optional)
- Properties for each interface (name, IP address, and netmask)
- Default router (Gateway Address)

2 Click **`Update`**.

Selecting the Administration Interface

Administrative access to the RAMS 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* on the RAMS appliance (Port 1 by default). If you have a multiple port option card, any of the interfaces can act as the Administration Interface. Check the **`Allow Admin`** radio button 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:

- FTP address for file transfer to RAMS.
- Address where XML queries are sent.
- Address that technical support requires when any request for assistance is made.
- Address for the X-Windows 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 In the Alias Interfaces section, select the desired interface from the Interface drop-down list.

2 Enter a name for the alias in the Alias Name field.

3 Enter the IP address in the IP Address field.

4 Click **`Update`**.

Configuring a Static Route

A static route is used to route packets directly to a specific router in a particular network area. If the address of the Administration Interface is manually configured (rather than using DHCP), then you must also configure a default static route.

For EIGRP topologies, the default route configured on an interface must be suitable for telnet or ssh 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.

Note 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 In the Static Routes section, enter the destination, default router, and netmask details in the fields provided.

2 Click **`Update.`**

Note Only one static route may be added at a time. After clicking **Update**, a new row of blank fields is provided for another route to be added.

Tip To override the default gateway inserted by DHCP, you can add two static routes 0.0.0.0/128.0.0.0 and 128.0.0.0/128.0.0.0.

Caution 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 will be 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. Make any required changes to the route details in the Static Routes section.
2. Click **`Update`**.

To delete a static route, perform the following steps:

1. Manually erase the route details from the Static Routes section.
2. Click **`Update`**.

Configuring Expansion Port Options

A different OSPF or IS-IS area or EIGRP autonomous system can be monitored with each of the ports on the RAMS appliance, including those on a multiple port option card if installed. Multiple area monitoring is also possible using tunnels. Tunnels are discussed in more detail in GRE Tunnels on page 73.

Here are some tips for setting up expansion port monitoring:

1. The default router must be on the same network as the Administration Interface.
2. One of the interfaces must be the Administration Interface. RAMS defaults to slot 0 port 1.
3. You can use DHCP to set the IP address on the Administration Interface.

4 You must assign an IP address to each of the ports or interfaces.

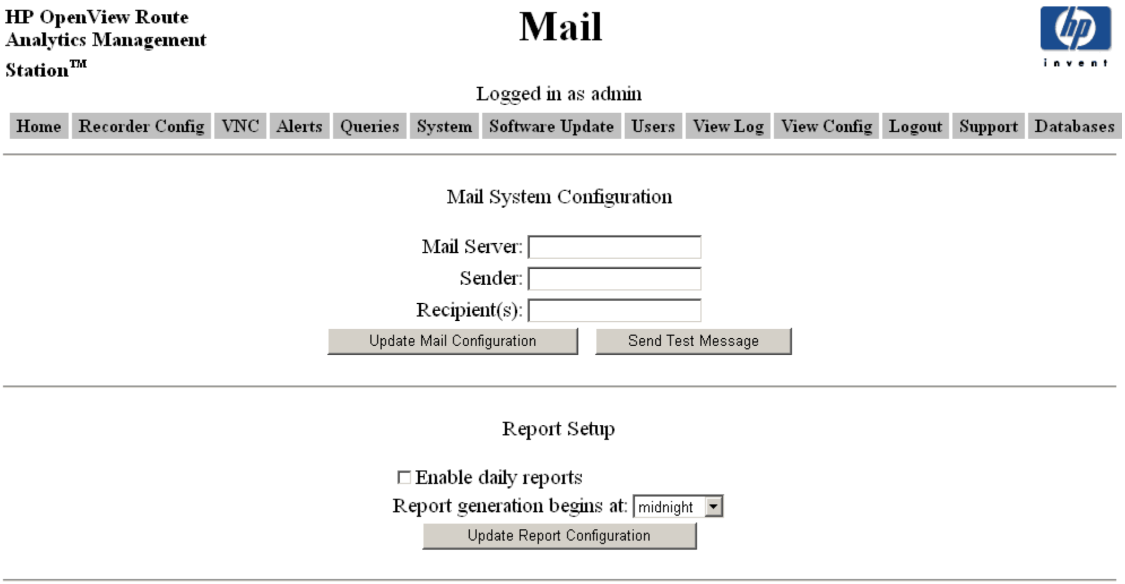
To configure an expansion port, do the following steps:

1. You can use an expansion port as the Administrative Interface if desired. Click the **`Allow Admin`** radio button to switch the Administrative Interface to the desired port.
2. To use DHCP on the Administrative Interface, check the **`Use DHCP`** checkbox.
3. For each of the other interfaces on the card, fill in the following information:
    - 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. Use the *View Configuration* page to check the network settings. For more information on the *View Configuration* page, see Viewing the Configuration on page 50.

Configuring Daily Reports

Click **Mail** in the *System Configuration* page to access the *Mail* page as shown in Figure 9. Use the *Mail* page to schedule a time to send a daily report summarizing network activity via e-mail to the configured recipients.



Mail

Logged in as admin

Mail System Configuration

Mail Server:

Sender:

Recipient(s):

Report Setup

□ Enable daily reports

Report generation begins at: midnight

Figure 9 **Mail page**

To configure the mail system, perform the following steps:

1. Enter the outbound mail server or relay in the **Mail Server** box using either a DNS name or an IP address enclosed in square brackets (for example, [192.168.0.200]). If you do not specify a mail server, RAMS attempts to send directly to the mail server(s) of the recipient(s).
2. In the **Sender** box, type the full e-mail address to be shown as the sender of mail sent from RAMS. Bounced e-mail messages may be sent to this address, so this address should be valid.
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**.

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

To schedule daily reports, perform the following steps:

1. 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**.

Daily Report Contents

The daily report contains several sections summarizing network activity:

- Networks Monitored: Lists all databases and their current status: online, offline, or offline in the last 24 hours.
- IGP Summary: If RAMS records IGP data, this section lists the following results in all monitored databases:
  - Counts of the number of routers, adjacencies and prefixes
  - Top 5 flapping links
  - Top 5 flapping prefixes
  - Top 5 active routers
  - Withdrawn prefixes on the watch list
- BGP Summary: If RAMS records BGP data, this section lists the following results in all monitored databases:
  - Top 5 BGP route flaps
  - Top 5 prefix redundancy divergence
  - Top 5 AS reachability divergence
- The last section of the report contains information about the RAMS system including the license status and amount of disk space currently in use.

View Saved Daily Reports

RAMS stores the daily reports for the past 30 days so that you can compare to an earlier report when there has been a change.

To view saved daily reports, perform the following steps:

1. Click **Home** to access the *Home* page.
2. Click **Saved Files** to access the *Saved Files* page.
3. Click **Daily Reports**.
4. Click on a report filename to download or view that report.

Backing Up and Restoring Data

The route topology information recorded by RAMS is stored in databases. The *Backup and Restore* page lets you selectively save any or all of the data files on the RAMS appliance, including databases and system configuration files. These data files are saved into a single backup file, which can easily be downloaded from the RAMS appliance to your desktop computer.

To create a backup, perform the following steps:

1. You cannot back up an actively recording database. If the database you want to back up is recording, stop recording for that database by using the *Recorder Configuration* page. See Configuring the Route Recorder on page 56.
2. Click **`Backup and Restore`** from the *System Configuration* page to access the *Backup and Restore* page.
3. Select the databases and configuration files you want to back up.
4. Click **`Create Backup`**.

   The backup process begins. Depending on the size of the database, the backup process can take several minutes. The *Backup in Progress* page appears and periodically updates with the file size as it progresses.
5. When the backup completes, the **Finished** button appears on the *Backup and Restore* page. Click the **`Finished`** button to continue.

   The *Backup and Restore* page now lists the new backup file in the Restore section at the bottom of the page.

   Any earlier backup file for a given database or system configuration file is automatically overwritten when you create a new backup file of that database or system configuration file.

Note Depending on the size of the database and on the Login Linger Timer 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.

6 If you stopped recording before the backup, start recording data again by using the *Recorder Configuration* page.

To save a backup, perform the following steps:

1 After creating a backup file, click **`Download Backup`** on the *Backup and Restore* page

A *File Download* dialog appears.

2 Click **`Save`**.

3 Enter a filename for the backup or accept the default filename (`backup.dat`), and select a destination for the backup file.

To restore a backup, perform the following steps:

1 You cannot restore a backup of an actively recording database. If the database is recording, stop recording for that database by using the *Recorder Configuration* page.

2 Click **`Backup and Restore`** from the *System Configuration* page to access the *Backup and Restore* page.

3 If the desired backup file is stored on your desktop computer, click **`Upload File`**, and enter the file name for the backup or click **`Browse`** and select the desired file from the local file system.

If the desired backup file is already stored on the RAMS appliance, the contents of the backup are listed in the Restore section of the *Backup and Restore* page.

4 Check items to restore, and then click **`Restore Selection`**.

Note 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 RAMS does not respond to the browser, wait approximately three minutes for the boot process to complete, and log in again.

5. If you want to append new data to the restored database, start recording again by using the *Recorder Configuration* page.

To delete the backup file from the RAMS appliance, perform the following steps:

1. Go to the *Backup and Restore* page.
2. Click **`Delete Backup File`**. This operation removes the backup file from the RAMS hard disk to free up space.

Running Diagnostics

In the current release, the only diagnostic supported by RAMS is the *ping* function.

To ping another network device, perform the following steps:

1. Go to the *System Configuration* page and click **`Diagnostics`** to access the *Diagnostics* page, shown in Figure 10.

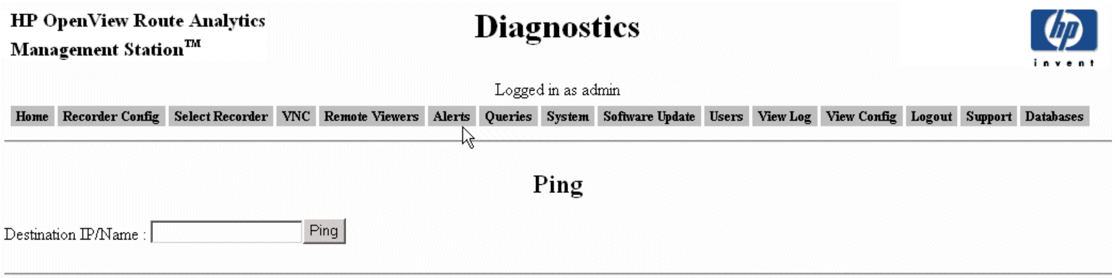


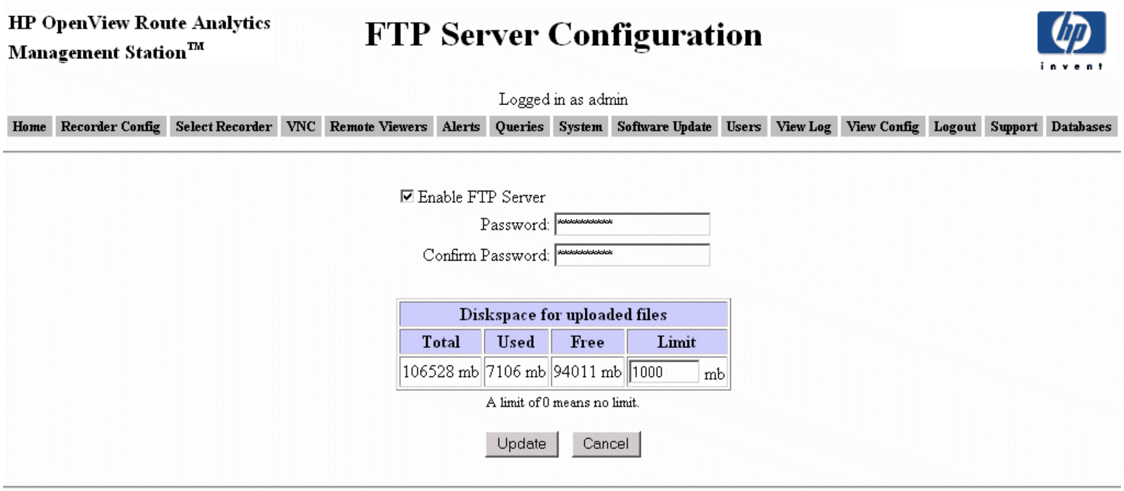
Figure 10 Diagnostics Page

2. In the Destination IP/Name text entry box, enter the IP address or DNS name of the destination device.
3. Click **`Ping`** to send the ping.
4. The results of the ping are displayed on the *Diagnostics* page.

Configuring the FTP Server

A portion of the hard disk on the RAMS appliance is available for the storage of users' files in the FTP server's directory. Time series files and MRTG files can be uploaded onto the RAMS appliance using FTP for correlation with routing events (see Correlating Time Series Data on page 224). Backed-up database files are also stored there.

Click **FTP Server** on the *System Configuration* page to access the *FTP Server Configuration* page, shown in Figure 11. The *FTP Server Configuration* page enables the uploading of files to the RAMS hard disk. It also lets you set the password for FTP file operations.



Logged in as admin

☑ Enable FTP Server

Password: **********

Confirm Password: **********

Diskspace for uploaded files			
Total	Used	Free	Limit
106528 mb	7106 mb	94011 mb	1000 mb

A limit of 0 means no limit.

Figure 11 FTP Server Configuration Page

To enable FTP file uploads, perform the following steps:

1 Check the **Enable FTP Server** check box.

2 Enter a password in the *Password* text box.

3 Repeat the password in the *Confirm Password* text box.

4 You can also set a size limit for the total amount of data that can be accepted in file uploads. A value of zero (0) implies no limit.

5 Click **Update** to complete configuration.

Caution If the file size exceeds the amount of free space available on the RAMS hard disk, the upload fails. Be aware of the amount of available free space prior to setting this limit.

After the FTP server is enabled, you can login for FTP file transfer as follows:

1. Start the FTP client software.
2. Enter the following values:
   - The IP address of the RAMS appliance.
   - The login name: `rexftp`
   - The password set on the *FTP Server Configuration* page.
3. Change directory to *pub* when uploading time series and MRTG files.

Technical Support Access

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

Caution Disabling Technical Support Access makes it impossible for HP to reset the password or perform diagnostic services without you returning the unit.

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

Viewing the Configuration

The *View Configuration* page displays the status of the various RAMS components. Table 3 lists the settings that appear on the *View Configuration* page and the page where you can update the settings.

Table 3 Settings on the View Configuration Page

Setting	Page
Hostname	*Network Configuration* page
RAMS Version and Operating System	*Software Update* page
Technical Support Access	*System Configuration* page
Gateway Primary DNS Secondary DNS Option Cards Interface	*Network Configuration* page
FTP	*FTP Server Configuration* page
Time*	*Time and Date* page

*If the time is set using an NTP server, some additional information appears in the Time table on the *View Configuration* page.

Software Update

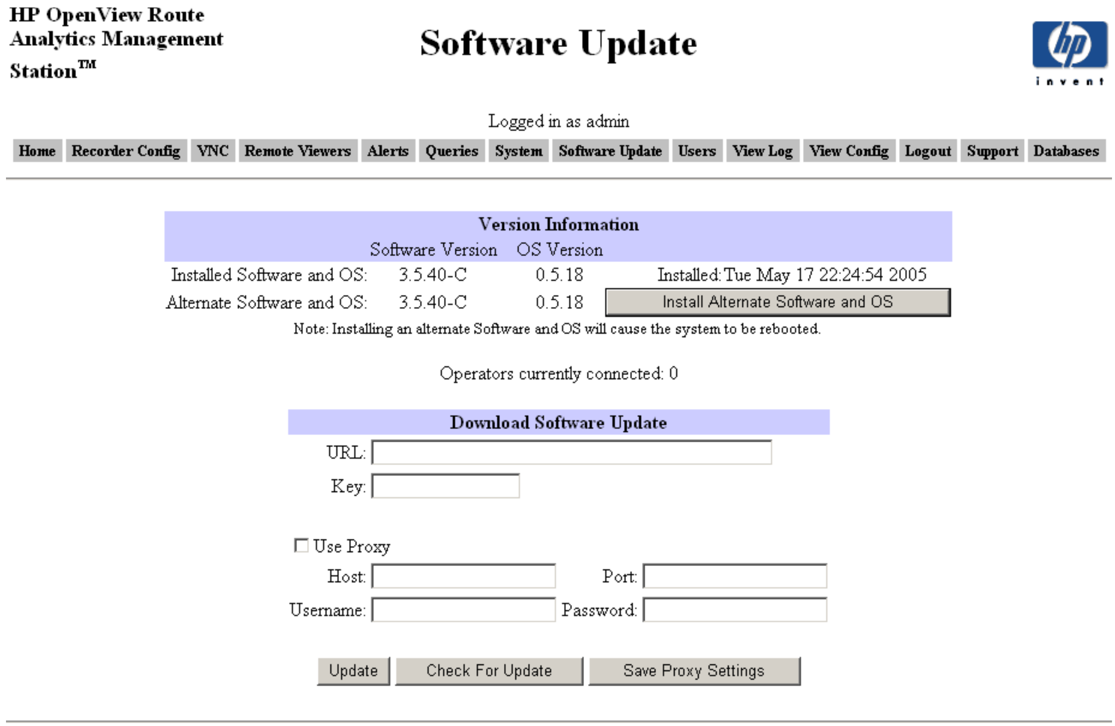
HP provides software updates for RAMS. You can download software updates directly from the HP FTP site. To download a new update, click the **`Software Update`** link. The *Software Update* page, shown in Figure 12, opens.

Note RAMS must have a license that enables software updates before you can download updates. Contact HP customer service for a license. See License Keys on page 88 for more information about licenses.

Update Options

RAMS has its own operating system software and application software. How you update the RAMS software depends on how it is connected to the Internet:

- The download process is easiest when RAMS is connected to the Internet, either directly or via a proxy server. See Updating with Internet Access on page 52.
- If the RAMS appliance cannot get access to the Internet, you can download an update, move it to a local FTP server that the appliance can access, and update the appliance from there. See Updating without Internet Access on page 53.



HP OpenView Route Analytics Management Station™

Software Update

Logged in as admin

Version Information

	Software Version	OS Version	
Installed Software and OS:	3.5.40-C	0.5.18	Installed: Tue May 17 22:24:54 2005
Alternate Software and OS:	3.5.40-C	0.5.18	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:

Key:

□ Use Proxy

Host: Port:

Username: Password:

Figure 12 Software Update Page

Updating with Internet Access

If your RAMS appliance can access the Internet directly or via a proxy server, follow the steps in this section. Otherwise, proceed to Updating without Internet Access on page 53.

To download updates when connected to Internet via a proxy server, perform the following steps to set up the proxy configuration first, and then the subsequent steps for downloading the update:

1 Check the **`Use Proxy Server`** check box.

2 Enter the Host and Port details for the proxy server.

3 If the proxy server is password protected, enter the Username and Password.

4 Click **Save Proxy Settings** to preserve these settings for future downloads.

To download updates when connected directly to the Internet, perform the following steps:

1 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* field. Otherwise, a message tells you no update is available.

2 In the *Key* field, enter the Update key provided by HP customer support.

3 Click **Update**. This downloads and installs the update. This can take some time, depending on your connection speed, since well over 100MB of data are transferred.

4 If the download includes an operating system update, a message appears stating that you must reboot RAMS to complete the download. Click **Reboot Now** and wait for the system to reboot. This should take approximately two or three minutes.

5 Click the **Home** link and log in again.

Note If at any time during the update process a 404 page error appears, click the **Back** button on the browser and then click **Refresh**.

Updating without Internet Access

If the RAMS appliance cannot access the Internet directly of through a proxy server, you can download an update to a local FTP server that the RAMS appliance can access, and install the update from there.

To download updates when RAMS is behind a firewall, perform the following steps:

1 Go to the HP OpenView Route Analytics Management System product web site (**http://www.openview.hp.com/products/ovrams/index.html**), and follow the **Software Patches** link. This will take you to the HP OpenView software patches web site.

2 Use the Browse By Product version list to navigate to patches for the Route Analytics Management System product. Use the information there to determine if an update is available for you.

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.

> **Note** 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 48.

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: `ftp://localhost/<dir>/<patch>`

5 On the Software Update page, click **Check for Updates**.

A message tells you if an update is available. If so, the **URL** field is automatically filled in for you.

6 Enter the Update key provided by HP customer support.

7 Click **Update**.

Downloading begins. If the download includes an operating system update, a message appears stating that you must reboot RAMS to complete the download.

8 Click **Reboot Now** and wait for the system to reboot. This should take approximately two or three minutes.

9 Click the **Home** link and log in again.

Returning to a Previous Version of RAMS

The previously installed version of the software is saved on the RAMS appliance. If you experience difficulty running a new version of RAMS, you can return to the previous software version. The *Software Update* page displays the previously installed version number of RAMS.

Caution Returning to the previous version of RAMS requires a reset to factory defaults, as described on page •93, because updates may not be completely reversible. This erases 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, do the following:

1. Click **`Install Alternate Software and OS`**.
2. Click **`Yes`** to install the previously installed version of RAMS.

   An informational window opens stating that an alternate version is installing and the system is rebooting.
3. After the system reboots, click the **`Home`** link.
4. Click **`Administration.`** The *Administrator Login* page opens.
5. Enter the user name and password.
6. Click **`Login`** or press **`Enter`**.

   The *Route Recorder Configuration* page or the *Select Recorder* page opens.
7. Click the **`System`** link to open the *System Configuration* page, and then click the **`Shutdown`** link to access the *Shutdown* page.
8. Click **`Reset to factory defaults and reboot`**, and then click **`Yes`** on the confirmation page that appears.
9. After the system reboots, log in from the *Home* page (if using DHCP network configuration) or use the serial console interface to reconfigure the network address and then connect to the *Home* page.
10. Log in as administrator (repeat steps 4 through 6).
11. Restore the system configuration from a backup file, or re-configure manually following the sequence of steps in this chapter.
12. If recording is enabled, verify on the *Route Recorder Configuration* page that Hellos and Events are being received from the areas or levels that are being monitored.

Configuring the Route Recorder

This section introduces the main functions of the Route Recorder and describes how to configure it and start recording. This section also introduces generic routing encapsulation (GRE) tunnels and describes how they are configured. The final part of this section deals with the configuration of a loopback interface for Cisco routers.

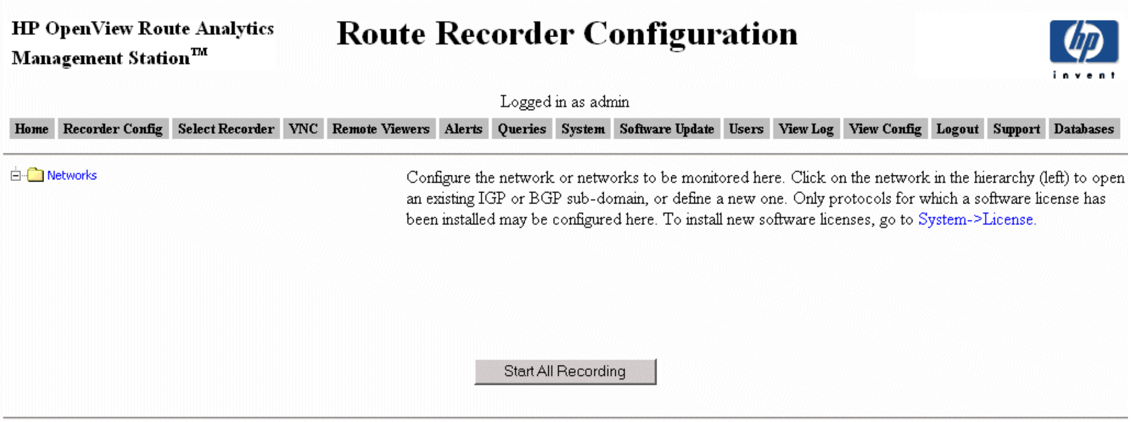
Caution Set the time and date on RAMS before configuring the recorder and recording data, according to the instructions in Setting the Time and Date on page 36. The date and time must be set before data recording begins because RAMS relies on accurate time stamps for generating report information.

The functions of the *Route Recorder Configuration* page include the following:

- Starting and stopping recording.
- Configuring and naming the databases used for recording data.
- Configuring interfaces and tunnels.
- Viewing the recording status.

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

Click **`Recorder Config`** to access the *Route Recorder Configuration* page, as shown in Figure 13.



Configure the network or networks to be monitored here. Click on the network in the hierarchy (left) to open an existing IGP or BGP sub-domain, 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 System->License.

Figure 13 Route Recorder Configuration Page

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

Configure Routing Databases and Start Recording

RAMS uses a hierarchical tree to represent the collection of IGP and BGP routing protocols to be recorded and the relationships among them. See the topology hierarchy examples in Figure 14.

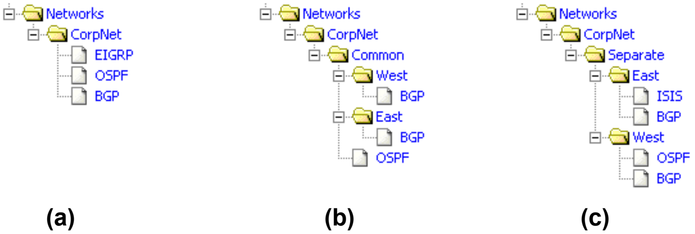


Figure 14 Topology Hierarchy Examples

Each instance of an IGP or BGP routing protocol is represented by a page icon at 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. Figure 14 (a) shows a simple multi-protocol topology that includes EIGRP, OSPF, and BGP protocol instances.

Folders represent *administrative domains*, which group related protocol instances together. You should first establish one top-level administrative domain, like *CorpNet* in the 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. 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 two administrative domains must be created to contain them. Also, a BGP instance cannot be configured in an administrative domain whose ancestor directly contains a BGP instance.

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 configuring 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 ASs 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 Create Domain Hierarchy and Protocol Instances.

The RAMS appliance supports up to 100 areas. This limitation applies to the total of OSPF areas, ISIS areas (levels), EIGRP ASs, and BGP ASs.

Interconnection of BGP and IGP Protocol Instances

A single physical router may 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 the network with two BGP and two IGP instances in Figure 14 (c). Here, the two BGP instances represent two BGP ASs 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 ASs 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 ASs but appears to outside ASs 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 ASs in the confederation may all be contained within one IGP domain, or each member BGP AS may be running a separate IGP instance. These two cases are illustrated in Figure 14 (b) and (c), respectively. 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 66 for guidelines on configuring BGP.

Configuring Multiple EIGRP ASs

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

- A single protocol instance can be configured with multiple network interfaces connected to the different EIGRP ASs, so long as no two ASs 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 ASs within the instance are merged so their relative timing can be easily viewed.

- Separate administrative domains can be created for each AS, each with its own protocol instance. However, a particular network interface can only be configured under a single protocol instance, so all of the ASs that may be heard on a single interface must be configured under the same domain and protocol instance.

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

Create Domain Hierarchy and Protocol Instances

To create a domain hierarchy and protocol instances, proceed as follows:

1. Log into the Administration Interface. The *Route Recorder Configuration* page appears.
2. Select **`Networks`** on the left side of the screen. See Figure 15.

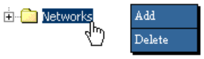
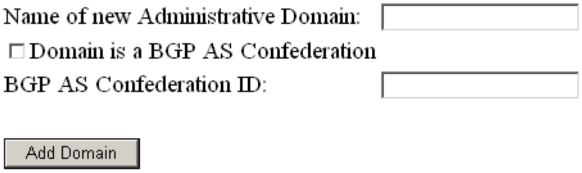


Figure 15 Networks

3 Move the cursor to **Add**, and then **Administrative Domain** appears.

4 Click **`Administrative Domain`**, and then type a domain name in the **`Name of new Administrative Domain`** box that appears on the right side of the screen, as shown in Figure 16. The name must consist solely of alphanumeric characters, with an alphabetic character first.



Name of new Administrative Domain:

□ Domain is a BGP AS Confederation

BGP AS Confederation ID:

Add Domain

Figure 16 Adding an Administrative Domain

5 If the administrative domain represents a BGP AS confederation, select **Domain is a BGP AS Confederation,** and then type the confederation ID number in the **BGP AS Confederation ID** box. See Configuring a BGP Confederation on page 59.

6 Click **`Add Domain`**.

7 Click on the "**+**" button to the left of **`Networks`** to open the folder and show the domain name just entered.

8 Click on the domain name, move the cursor to **Add**, and then you will have an option, as shown in Figure 17, to add another level of domain name hierarchy by repeating steps 4 through 7, or to add a protocol instance proceed to step 9.

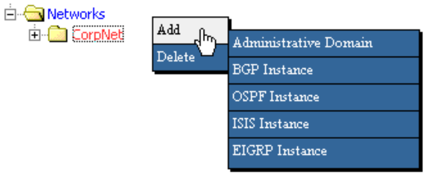


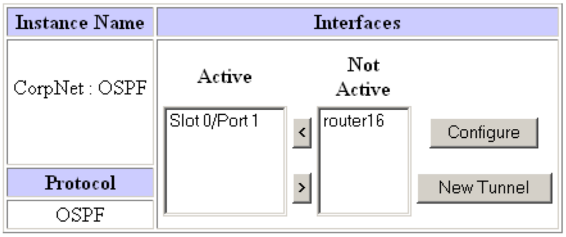
Figure 17 Adding a Protocol Instance

9 Click the desired type of protocol instance (BGP, OSPF, IS-IS, or EIGRP). The configuration section for the selected protocol appears on the right side of the *Route Recorder Configuration* page. For detailed instructions on configuring the protocol instance, see the next section, Configure an IGP Instance, or see Configure a BGP Instance on page 66. You can configure additional protocol instances by repeating steps 8 and 9.

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

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 *Route Recorder Configuration* page, as shown in Figure 18.



Instance Name	Interfaces	
	Active	Not Active
CorpNet : OSPF	Slot 0/Port 1	router16
Protocol		
OSPF		

Figure 18 Configuring an IGP Protocol Instance

To configure an IGP instance, proceed as follows:

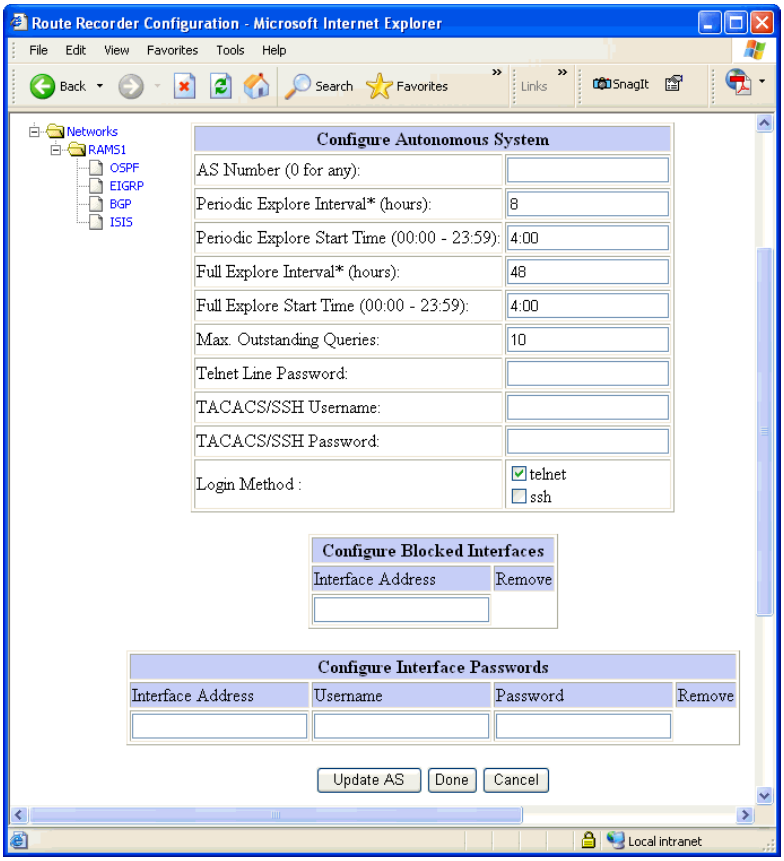
1 The configured network interfaces are shown in the Not Active column. Select the appropriate interfaces that are connected to network areas or autonomous systems for this protocol instance, and move them from the Not Active column to the Active column using the **<** button.

If a GRE tunnel is required to connect to a remote router, click **`New Tunnel`**, and then follow the instructions in GRE Tunnels on page 73 to create the tunnel interface. For EIGRP, there can be multiple interfaces connected to a single autonomous system in order to get complete coverage. A default route may need to be configured for each interface (see Configuring a Static Route on page 40).

2 If OSPF is selected, OSPF authentication can be enabled separately for each interface. Select the desired interface and click the **`Configure`** button. There are two types of OSPF authentication: simple and MD5. Simple authentication only requires a password (up to eight characters), while MD5 authentication requires a password (up to sixteen characters) and a Key-Id (a number between 1 and 255, inclusive).

Note To monitor two OSPF areas that are linked to a single router, it is necessary to configure a loopback interface on the Cisco router to monitor both areas with RAMS. See Configuration of a Loopback Interface for Cisco Routers on page 77.

3 For an EIGRP instance, one or more autonomous systems (AS) must also be configured. Click **`New AS`** to display the autonomous system configuration section, as shown in Figure 19. For a network with more than one EIGRP AS, there are two configuration choices as explained in Configuring Multiple EIGRP ASs on page 60. To configure OSPF or ISIS ASs, proceed to Step 8.


Route Recorder Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Links
SnagIt
Networks
RAMS1
OSPF
EIGRP
BGP
ISIS
Local intranet

Configure Autonomous System	
AS Number (0 for any):	
Periodic Explore Interval* (hours):	8
Periodic Explore Start Time (00:00 - 23:59):	4:00
Full Explore Interval* (hours):	48
Full Explore Start Time (00:00 - 23:59):	4:00
Max. Outstanding Queries:	10
Telnet Line Password:	
TACACS/SSH Username:	
TACACS/SSH Password:	
Login Method :	☑ telnet ☐ ssh

Configure Blocked Interfaces

Interface Address	Remove

Configure Interface Passwords

Interface Address	Username	Password	Remove

Update AS Done Cancel

Figure 19 Configuring an EIGRP Autonomous System

4 In the Configure Autonomous System table, fill in the following fields:

- AS Number: Enter 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 Username, and TACACS Password. If all routers use the same password or TACACS username and password combination, enter either the simple router login password or a TACACS username 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 username and password authentication configured through RADIUS or configured locally on the routers, although it must be the same for all routers in the AS.

Note See Step 6 if each router in the AS has a unique simple password or TACACS username 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.

5 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 when some routers exist that RAMS should not attempt to log into, or to limit the scope of RAMS’s topology exploration. Enter an interface address, then click **`Update AS`**.

6 Use the Configure Interface Passwords table to override the generic passwords specified in step 4 for any router that has a password different from those specified in the Configure AS table. Enter an interface address and its password or TACACS username and password combination, then click **`Update AS`**.

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

7 When you have configured all of the ASs, Blocked Interfaces, and Interface Passwords, click **`Done`** to complete the *Route Recorder Configuration* process.

8 Begin recording routing topology information for this protocol instance by clicking **Start Recording**.

or

Complete the configuration of all other protocol instances in the topology, if any, and then click **`Start All Recording`**.

Configure a BGP Instance

After you create a BGP protocol instance as described in Create Domain Hierarchy and Protocol Instances on page 60, the BGP configuration section appears on the right side of the *Route Recorder Configuration* page as shown in Figure 20. 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 autonomous system (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 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 ASs are monitored, an alias must be assigned to the RAMS appliance 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 ASs. 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 ASs.

If you use IP alias addresses, the addresses should all 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 interface's subnet. 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 RAMS appliance 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:

1. Ensure that the RAMS appliance 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.

2. 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 the 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.

3. 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, so it limits RAMS's ability to do some types of analysis, but route tracing should work correctly.

4. 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.

Note 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 router's other BGP neighbors, 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:

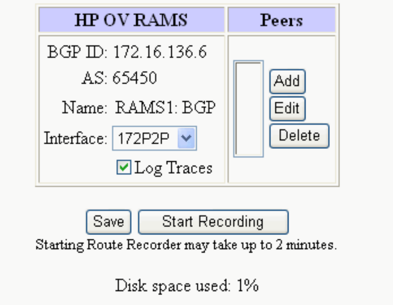
- EBGP routing information does not include certain BGP attributes such as the NextHop, Local-Pref, and MED attributes. These attributes are essential to determine the best BGP routes inside an AS. Without them, RAMS is unable to determine the correct exit routers or find correct paths for BGP prefixes.
- 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 ASs. 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. An different alias must be assigned to RAMS for each member AS.

If your RAMS unit 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 Chapter , "VPN Configuration and Reports," for more information about configuring customer/Route Target (RT) associations for VPN reports.

Once you have decided what BGP peerings you want to configure, you can enter the appropriate information in the BGP configuration section as shown in Figure 20.



BGP ID: 172.16.136.6

AS: 65450

Name: RAMS1: BGP

Interface: 172P2P

☑ Log Traces

Starting Route Recorder may take up to 2 minutes.

Disk space used: 1%

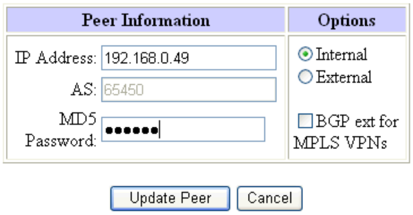
Figure 20 Configuring a BGP Instance

To configure a BGP instance, proceed as follows:

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, enter the AS number of the member (*not* the confederation ID) in the **Member AS** box.
3. Select the physical interface slot and port in the **Interface** drop-down list or select the logical interface alias.

4 The **Log Traces** function captures all raw BGP messages for diagnostic purposes. Select this box if requested by Technical Support.

5 In the Peers column, click `Add` to add peers as shown in Figure 21. The peer configuration table appears at the right side of the screen.



Peer Information

IP Address: 192.168.0.49

AS: 65450

MD5 Password: ••••••

Options

● Internal
○ External

□ BGP ext for MPLS VPNs

Figure 21 BGP Peer Configuration

6 In the Peer Information column, enter the IP address of the peer, and the peer's MD5 password if applicable. In the Options column, specify whether the peer is internal or external.

7 If this BGP topology is a BGP MPLS VPN, select **`BGP ext for MPLS VPNs`**. Otherwise, leave this check box cleared.

8 When you have entered all information for this peer, click **`Update Peer`** to return to the BGP instance configuration.

9 Repeat steps 5 through 8 for each additional peer.

10 Click **Save**.

11 Begin recording routing topology information for this protocol instance by clicking **Start Recording**.

or

Complete the configuration of all other protocol instances, if any, in the topology and then click **`Start All Recording.`**

Viewing and Modifying the Recorder Configuration

After a protocol instance is created and Route Recorder is started, RAMS is ready to receive routing announcements from the peer routers.

To view the status of an existing protocol instance, do the following:

1. From the *Route Recorder Configuration* page, select the protocol instance in the tree structure on the left side of the page.
2. Click the **`View`** menu option.

   A Status table is displayed at the bottom of the *Route Recorder Configuration* page.

   The Status table shows the status of the protocol adjacency, including the time of the last “hello” packet received as part of the routing protocol and the time of the last event written to the database by the Route Recorder. If this table is not empty, then a database is being created for RAMS. If the table is empty, verify that the connection to the router or the tunnel is properly configured.

Changing the Area ID Format

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. Open the Area ID Format drop-down menu and choose decimal or dotted decimal.
2. Click **`Submit`**.
3. Click the **`VNC`** link at the top of the *Route Recorder Configuration* page.
4. Click **`Stop`**. This stops the VNC server and closes any active VNC sessions.
5. Click **`Start`** to restart the VNC server.
6. Restart any VNC client sessions.

Deleting an Existing Domain or Protocol Instance

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

1. Click **`Stop Recording`**.
2. Select an existing instance from the tree structure on the left side of the screen.
3. Click **`Delete`**.
4. 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. Select the protocol instance name, and then click **`View`** to see the protocol configuration.
2. Click **`Stop Recording.`**
3. Choose an existing interface name. If the interface is in the Active column, move it to the Not Active column.
4. 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 *Route Recorder Configuration* page.
5. Click **`Delete`**. A confirmation message page opens.
6. Click **`Yes`**. The tunnel is deleted and the *Route Recorder Configuration* status page returns.

Changing an OSPF Authentication Password

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

1. Select the protocol instance name, and then click **`View`** to see the protocol configuration.
2. Click **`Stop Recording.`**

3 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.

4 Select the interface name, and then click **`Configure.`**

5 Highlight the password and type another password.

6 Click **`Update`**. This changes the password.

Deleting an OSPF Authentication Password

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

1 Select the protocol instance name, and then click **`View`** to see the protocol configuration.

2 Click **`Stop Recording.`**

3 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.

4 Select the interface name and click **`Configure.`**

5 Unselect **`Enable`**.

6 Delete the password.

7 Click **`Update`**. This deletes the OSPF authentication password.

GRE Tunnels

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 RAMS.
- Use a Generic Routing Encapsulation (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 RAMS 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 RAMS 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 RAMS end of the tunnel.
- 10.0.1.3/30 is the broadcast address.

The tunnel extends from the router to RAMS, and the tunnel must be configured both on the router and on RAMS.

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 RAMS.
- 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 RAMS, keep the following points in mind:

- From the RAMS's perspective, the tunnel *source* is the IP address for the physical interface on RAMS.
- The tunnel *destination* is the IP address of the physical interface of the remote router.

Configure a GRE Tunnel

To create a GRE tunnel on the destination router, the information in Table 3-2 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.)

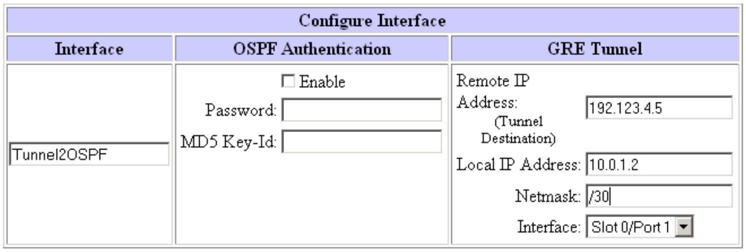
Table 4 **Required Tunnel Information on Remote Router**

Item	Example of Command
Tunnel Interface	`int tunnel <n>`
Tunnel IP	`ip address 10.0.1.1 netmask 255.255.255.252`
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 on RAMS, perform the following steps:

1. Click **`New Tunnel`** on the *Route Recorder Configuration* page.

   The *Configure Interface* section opens, as shown in Figure 22.



Configure Interface

Interface	OSPF Authentication	GRE Tunnel
Tunnel2OSPF	□ Enable Password: MD5 Key-Id:	Remote IP Address: (Tunnel Destination) 192.123.4.5 Local IP Address: 10.0.1.2 Netmask: /30 Interface: Slot 0/Port 1

Figure 22 **Configuring a GRE Tunnel Interface**

2. In the *Interface* text box, enter a descriptive name for the tunnel.
3. 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 **Enable**.

   For simple authentication, enter a password in the password field that matches the password in the remote area.

For MD5 authentication, enter 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.

4 In the *Remote IP Address* text box, enter the IP Address of the physical interface or loopback on the remote router. (This IP address should be the same as the **`Tunnel Source`** address you configured on the router.)

5 In the *Local IP address* text box, enter the IP Address assigned to the tunnel on RAMS. (Using the example addresses listed above, this would be 10.0.1.2).

6 In the *Netmask* text box, enter the network mask of the **`Tunnel IP`** address that you configured on the router. The format for the Netmask field can be one of the following:

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

Here is an example based on the addresses used in Figure 22:

- — 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)

7 Click **`Update`**.

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

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

9 Click **`Update`**.

Configuration of 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 to monitor both areas with RAMS. If you do not do this, only one adjacency will be formed with the remote router. Both areas will come up initially with full adjacency, but the first one to come up will fail soon after. Use the command line interface to the router to configure the loopback interface.

To configure a loopback, perform the following steps:

1 Open a session with the router.

2 Enter the following commands:

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

Configuring Multiple Recorders and View Servers

If you will be running multiple RAMS units in your network, with one or more acting as Recorders and one or more acting as View Servers, you must configure each unit according to the function it will perform. A unit's function depends upon the license assigned to it.

Note The procedures in this section do not apply if you run a single RAMS unit in your network that functions as both Recorder and View Server.

Configuring a Recorder

On each RAMS unit that will perform the Recorder function, you must configure information about all View Servers in the network. This information enables the remote View Servers to connect to the Recorder.

Note Each View Server must be running and configured with its own IP address before you configure the Recorder to enable that View Server.

To configure a Recorder, perform the following steps:

1. If you are not already logged in, navigate to the *Administration* page on the Recorder unit and enter your user name and password.

   The *Route Recorder Configuration* page appears.

2. Click **`Remote Viewers`** on the *Route Recorder Configuration* page.

   The *Manage Remote View Servers* page appears.

3. In the *Remote View Server Address* text box, enter the IP address of the remote View Server.
4. Click **`Update`**. The Recorder sends a special encrypted key to the specified remote View Server that enables that View Server to connect to this Recorder.
5. Repeat steps 3 and 4 for each additional remote View Server.

To remove a View Server from a Recorder's configuration, do the following:

1 If you are not already logged in, navigate to the *Administration* page on the Recorder unit and enter your user name and password.

The *Route Recorder Configuration* page appears.

2 Click **`Remote Viewers`** on the *Route Recorder Configuration* page.

The *Manage Remote View Servers* page appears.

3 Select **`Delete`** for the View Server you want to remove from the configuration, and then click **`Update`**.

The selected View Server is removed from the Recorder's list of enabled View Servers.

Configuring a View Server

On each RAMS unit that will perform the View Server function, you must configure information about the Recorder to which it will connect to obtain topology maps and history information.

To configure a View Server, perform the following steps:

1 If you are not already logged in, navigate to the *Administration* page on the View Server unit and enter your user name and password.

2 Click the **`Select Recorder`** link.

The *Select Remote Recorder* page appears. The first entry in the Remote Recorder table represents the local RAMS. The IP address field in this entry is *local* if this unit is licensed as both Recorder and View Server, or *none* if this unit is licensed as View Server only. In addition, the table contains an entry for each remote Recorder in the network that has enabled this View Server.

3 Select the remote Recorder that this View Server will connect to by clicking the **`Active Recorder`** radio button for that Recorder.

4 Click **`Update`**. This establishes a connection to the specified remote Recorder to view recorded data.

Note Each View Server is connected to one Recorder at a time. If you have multiple Recorders in your network and wish to connect your View Server to a different Recorder, you must reconfigure the View Server using the steps outlined above.

To remove a Recorder from a View Server's configuration, perform the following steps:

1 If you are not already logged in, navigate to the *Administration* page on the View Server unit and enter your user name and password.

2 Click the **`Select Recorder`** link.

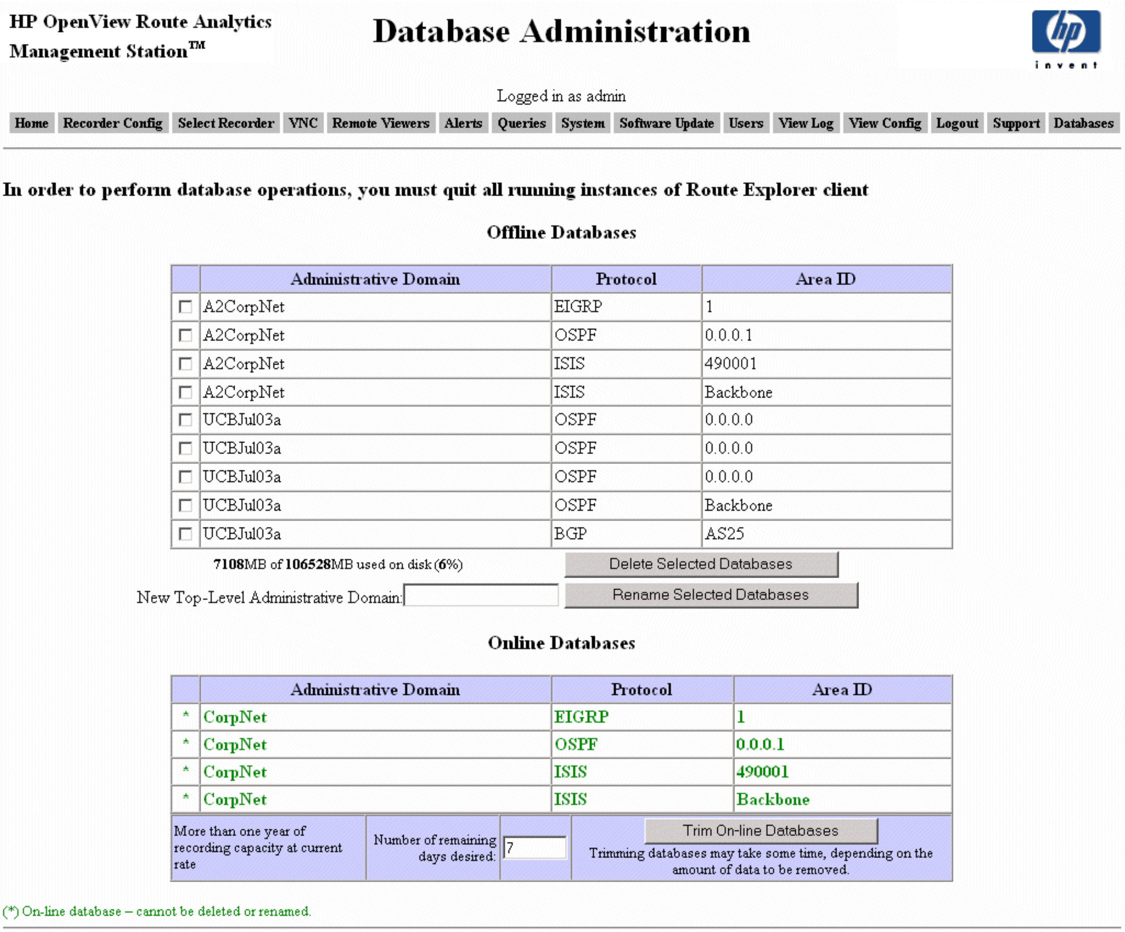
The *Select Remote Recorder* page appears.

3 Select **`Delete Recorder`** for the Recorder you want to remove from the configuration, and then click **`Update`**.

The selected Recorder is removed from the View Server's list of potential Recorders.

Database Administration

Use the *Database Administration* page to delete, rename, or trim an existing database. To access this page, click the **`Databases`** link, as shown in Figure 23.



In order to perform database operations, you must quit all running instances of Route Explorer client

Offline Databases

	Administrative Domain	Protocol	Area ID
□	A2CorpNet	EIGRP	1
□	A2CorpNet	OSPF	0.0.0.1
□	A2CorpNet	ISIS	490001
□	A2CorpNet	ISIS	Backbone
□	UCBJul03a	OSPF	0.0.0.0
□	UCBJul03a	OSPF	0.0.0.0
□	UCBJul03a	OSPF	0.0.0.0
□	UCBJul03a	OSPF	Backbone
□	UCBJul03a	BGP	AS25

7108MB of **106528**MB used on disk (**6%**)

New Top-Level Administrative Domain:

Online Databases

	Administrative Domain	Protocol	Area ID
*	CorpNet	EIGRP	1
*	CorpNet	OSPF	0.0.0.1
*	CorpNet	ISIS	490001
*	CorpNet	ISIS	Backbone

More than one year of recording capacity at current rate

Number of remaining days desired: 7

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

(*) On-line database – cannot be deleted or renamed.

Figure 23 Database Administration Page

Database administration is usually performed for housekeeping reasons, for example, when the RAMS disk is becoming full. Deleting unneeded databases and trimming active databases can help you to gain disk space. In this situation, you should also run your FTP application to connect to the RAMS's FTP file storage area and use the **FTP Delete** command to delete any unneeded files (see Configuring the FTP Server on page 48 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.

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

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. Near the bottom of the Offline Databases section is a field that indicates how much disk space is currently used, as well as the total amount of RAMS disk space.

Deleting a Database

To permanently delete a database, perform the following steps:

1. Stop all instances of the RAMS client.
2. Login to the *Administration Interface* and go to the *Route Recorder Configuration* page.
3. If the database you want to delete is currently recording, stop recording on that database
4. Delete the configuration corresponding to the database to be deleted.
5. Navigate to the *Database Administration* page.
6. Check the checkbox to the left of the databases to be deleted.
7. Click **`Delete Selected Databases`**.

   A confirmation page appears displaying the names of the selected databases.

8 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 RAMS client.

2 Login to the *Administration Interface* and go to the *Route Recorder Configuration* page.

3 If the database you want to delete is currently recording, stop recording on that database.

4 Navigate to the *Database Administration* page.

5 Check the checkbox to the left of the databases to be deleted.

6 Click the **`Delete Selected Databases`** button.

A confirmation page appears displaying the names of the selected databases.

7 Click **`Yes`** if you want to delete the selected databases.

The selected databases are deleted.

8 Navigate back to the *Route 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 RAMS client.

2 Login to the *Administration Interface* and go to the *Route Recorder Configuration* page.

3 If the databases you want to rename are currently recording, stop recording on these databases.

4 Navigate to the *Database Administration* page.

5 Select the checkbox to the left of the databases to be renamed to a single, new name (typically only databases that have a common first-level administrative domain name already).

6. Enter the new name in the **New Top-Level Administrative Domain** field. Only the first-level administrative domain name can be changed, meaning, no period is allowed in the new name. Names must begin with an alphabetic character and can contain only alphanumeric characters.
7. Click **`Rename Selected Databases`**.

   A confirmation page appears displaying the names of the selected databases.
8. Click **`Yes`** to confirm that you want to rename the selected databases. The top-level name of the selected databases is renamed to the new top-level administrative domain.

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 Remaining Days field is 7. You can specify a different interval.

When you trim the online databases, RAMS deletes data from the earliest point in the databases until the aggregate database size allows for a number of days' growth specified by the Remaining Days field. All databases are trimmed so that the data begins at approximately the same date.

To trim a database:

1. Login to the *Administration Interface* and navigate to the *Database Administration* page.
2. Click the **`Trim On-line Databases`** button.

   If the databases contain data older than the date implied by the Remaining Days field, the databases are trimmed, and a confirmation message is displayed on the *Database Administration* page.

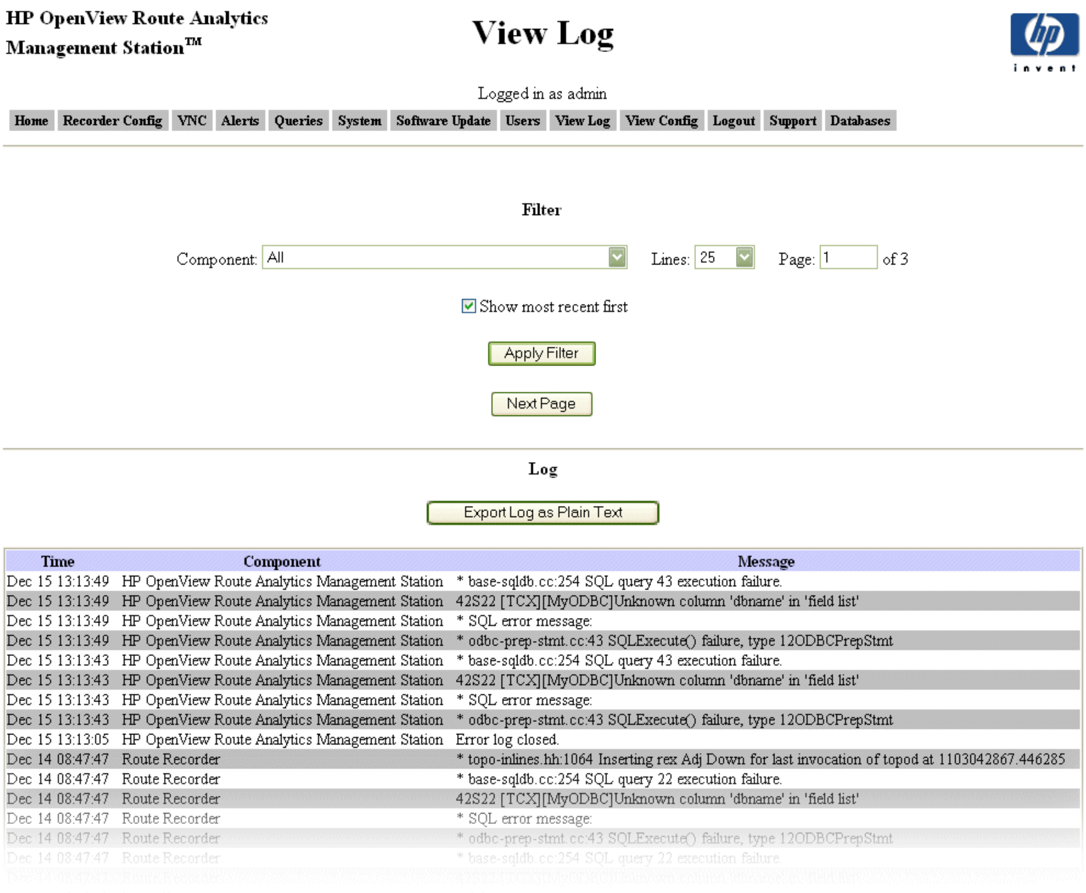
   If the databases do not contain data older than the date implied by the Remaining Days field, the message "No action required" is displayed.

Viewing the Log

Use the *View Log* page to view the RAMS logs. To view a log, click the **`View Log`** link. The *View Log* page opens, as shown in Figure 24.

To view a log page, perform the following steps:

1. On the *View Log* page, select Route Recorder, RAMS, or All from the Component drop-down list. (The number of pages in the log displays automatically.)
2. Select the number of lines to display from the Lines drop-down list.
3. Enter the desired page number in the *Page* text box.



HP OpenView Route Analytics Management Station™
View Log
invent
Logged in as admin
Home | Recorder Config | VNC | Alerts | Queries | System | Software Update | Users | View Log | View Config | Logout | Support | Databases
Filter
Component: All
Lines: 25
Page: 1 of 3
☑ Show most recent first
Apply Filter
Next Page
Log
Export Log as Plain Text

Time	Component	Message
Dec 15 13:13:49	HP OpenView Route Analytics Management Station	* base-sqldb.cc:254 SQL query 43 execution failure.
Dec 15 13:13:49	HP OpenView Route Analytics Management Station	42S22 [TCX][MyODBC]Unknown column 'dbname' in 'field list'
Dec 15 13:13:49	HP OpenView Route Analytics Management Station	* SQL error message:
Dec 15 13:13:49	HP OpenView Route Analytics Management Station	* odbc-prep-stmt.cc:43 SQLExecute() failure, type 12ODBCPrepStmt
Dec 15 13:13:43	HP OpenView Route Analytics Management Station	* base-sqldb.cc:254 SQL query 43 execution failure.
Dec 15 13:13:43	HP OpenView Route Analytics Management Station	42S22 [TCX][MyODBC]Unknown column 'dbname' in 'field list'
Dec 15 13:13:43	HP OpenView Route Analytics Management Station	* SQL error message:
Dec 15 13:13:43	HP OpenView Route Analytics Management Station	* odbc-prep-stmt.cc:43 SQLExecute() failure, type 12ODBCPrepStmt
Dec 15 13:13:05	HP OpenView Route Analytics Management Station	Error log closed.
Dec 14 08:47:47	Route Recorder	* topo-inlines.hh:1064 Inserting rex Adj Down for last invocation of topod at 1103042867.446285
Dec 14 08:47:47	Route Recorder	* base-sqldb.cc:254 SQL query 22 execution failure.
Dec 14 08:47:47	Route Recorder	42S22 [TCX][MyODBC]Unknown column 'dbname' in 'field list'
Dec 14 08:47:47	Route Recorder	* SQL error message:
Dec 14 08:47:47	Route Recorder	* odbc-prep-stmt.cc:43 SQLExecute() failure, type 12ODBCPrepStmt
Dec 14 08:47:47	Route Recorder	* base-sqldb.cc:254 SQL query 22 execution failure.
Dec 14 08:47:47	Route Recorder	42S22 [TCX][MyODBC]Unknown column 'dbname' in 'field list'

Figure 24 View Log Page

4 Select **`Show Most Recent First`** to see the last recorded log entries.

5 Click **`Apply Filter`**.

You can print a copy of this page using the web browser's print command or export the log entries as plain text.

To export the log as plain text, perform the following steps:

1 Choose which section of the log to export.

2 Click **`Export Log as Plain Text`**.

The log page is redisplayed in plain text form in the browser window.

3 Use the browser **`File`** menu or right-click in the window to open the pop-up menu.

4 Choose **`Save As`**.

5 Enter the directory where the log file will be stored and click **`Save`**.

6 Click the browser’s **`Back`** button to return to the *View Log* page.

License Keys

License keys control the number of routers and users that RAMS can support, as well as the protocols it participates in.

To view the license key information, click the **`System`** link to launch the System Configuration page. Then click the **`License`** link 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.

To install a new license key, proceed as follows:

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.

License Details

The following sections describe the various components of a license.

Temporary License

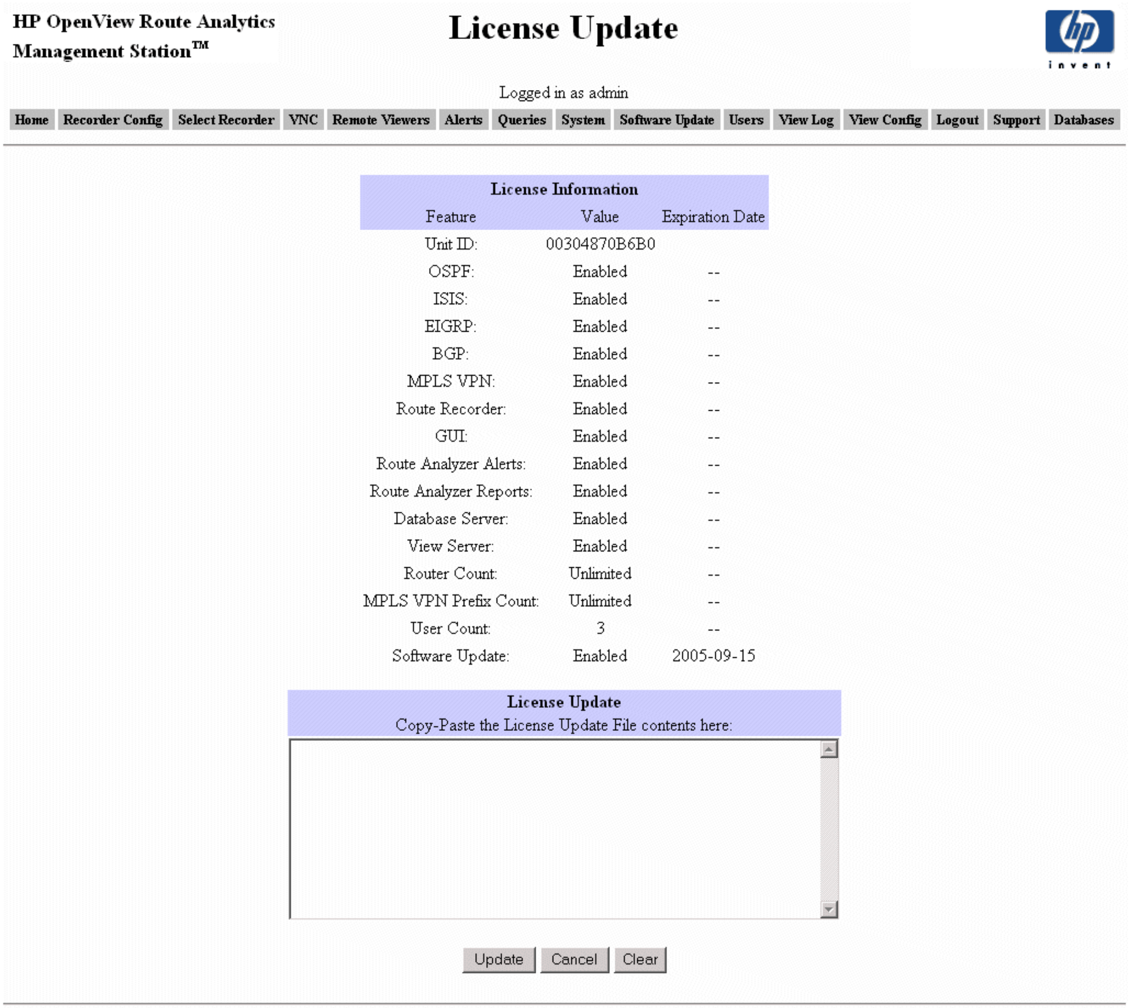
RAMS comes with a temporary license that unlocks all protocols for up to 3 users and 1000 routers. The temporary license key expires after 60 days.

To activate your temporary license, click **`Activate Temporary License`**. This will let you get started using RAMS, until you can install a permanent license key.

Warning **If the temporary license expires before you have installed a permanent license key, 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.**

Protocol Licenses

If a license for a given protocol (OSPF, IS-IS, EIGRP, BGP, or MPLS VPN) is not enabled, an instance of that protocol cannot be created on the *Route Recorder Configuration* 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.



HP OpenView Route Analytics Management Station™
License Update
invent
Logged in as admin
Home | Recorder Config | Select Recorder | VNC | Remote Viewers | Alerts | Queries | System | Software Update | Users | View Log | View Config | Logout | Support | Databases

License Information

Feature	Value	Expiration Date
Unit ID:	00304870B6B0	
OSPF:	Enabled	--
ISIS:	Enabled	--
EIGRP:	Enabled	--
BGP:	Enabled	--
MPLS VPN:	Enabled	--
Route Recorder:	Enabled	--
GUI:	Enabled	--
Route Analyzer Alerts:	Enabled	--
Route Analyzer Reports:	Enabled	--
Database Server:	Enabled	--
View Server:	Enabled	--
Router Count:	Unlimited	--
MPLS VPN Prefix Count:	Unlimited	--
User Count:	3	--
Software Update:	Enabled	2005-09-15

License Update

Copy-Paste the License Update File contents here:

Figure 25 License Page

Router Count

When the number of routers you are monitoring exceeds the number of routers supported by the license, a warning message is displayed on the RAMS user interface.

MPLS VPN Prefix Count

When the number of VPN prefixes you are monitoring exceeds the number supported by the license, a warning message is displayed on the RAMS user interface.

User Count

RAMS supports a specified number of concurrent users. Once this number is reached, RAMS rejects further user logins.

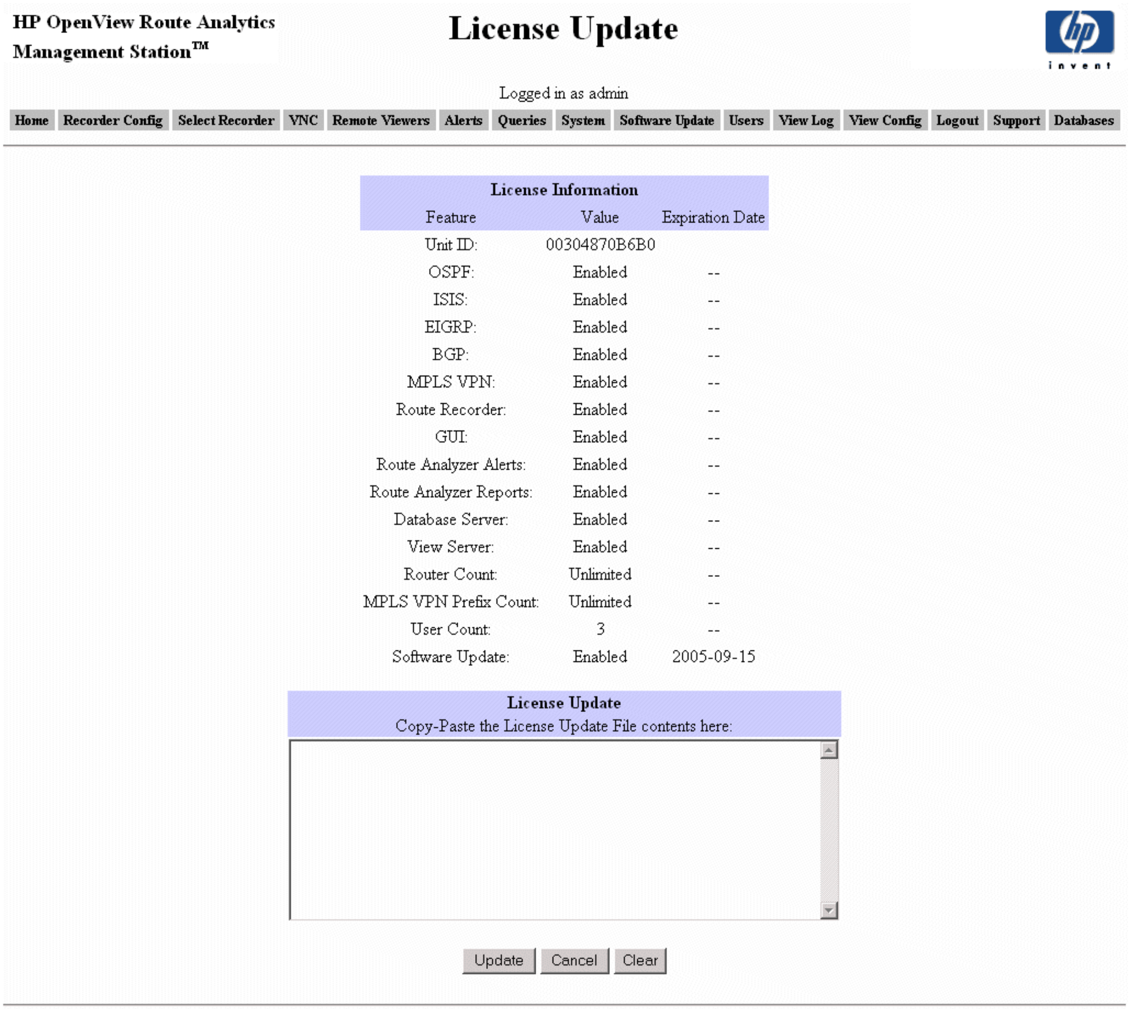
Shutdown

The RAMS appliance can be shut down at any time if needed. The system shutdown options are displayed on the *Shutdown* page, shown in Figure 26.

To access the *Shutdown* page, click the **`System`** link to open the *System Configuration* page, and then click the **`Shutdown`** link.

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

- **Reboot this system** – Click this button to reboot the system. A confirmation page appears. Click **`Yes`** to reboot the system. RAMS stops the VNC server and stops recording data, and reloads the operating system and recording software from the disk. Then, using the previous system settings, it automatically restarts the VNC server and the Route Recorder. 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 Route Recorder are operating correctly.



License Information		
Feature	Value	Expiration Date
Unit ID:	00304870B6B0	
OSPF:	Enabled	--
ISIS:	Enabled	--
EIGRP:	Enabled	--
BGP:	Enabled	--
MPLS VPN:	Enabled	--
Route Recorder:	Enabled	--
GUI:	Enabled	--
Route Analyzer Alerts:	Enabled	--
Route Analyzer Reports:	Enabled	--
Database Server:	Enabled	--
View Server:	Enabled	--
Router Count:	Unlimited	--
MPLS VPN Prefix Count:	Unlimited	--
User Count:	3	--
Software Update:	Enabled	2005-09-15

License Update

Copy-Paste the License Update File contents here:

Figure 26 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. RAMS stops the VNC server and stops recording data. To restart, press the power switch on the RAMS 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, log in from the *Home* page (if using DHCP network configuration) or use the serial console interface to reconfigure the network address and then connect to the *Home* page.

  Note If the factory settings are restored, the following information is lost:

  — All configuration information, including Network (reverts to DHCP), Route Recorder, usernames 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.

3

RAMS Clients

The X Window system or AT&T Lab's Virtual Network Computing (VNC) Viewer is required to run the RAMS client application.

- The X Window system lets you run an application on a remote computer anywhere in the Internet and display the application's windows on your local computer. Accessing RAMS using the X Window system works best with high-speed, low-delay Internet connections.
- VNC makes it possible to remotely display a desktop from anywhere in the Internet using a wide variety of operating systems. Accessing RAMS through VNC may give better performance than the X Window system over Internet connections with high delay and/or low bandwidth, such as DSL and dial-up connections.

This chapter explains how to download and configure the X Window system and VNC on Microsoft Windows, UNIX, and Linux operating systems. The downloads are available from the web server on the RAMS appliance.

The X Window Server

To use the X Window system, the user's computer must run an X server to receive and display the output of the remote RAMS application. In addition, RAMS requires that the X session be connected using the SSH (secure shell) protocol for privacy and security.

On Linux and UNIX platforms, an X server and SSH are already included since the X Window system is the native display method. On Microsoft Windows, an X server and SSH must be installed.

X Window Server for MS Windows™

Several X Window system products incorporating SSH are available for Microsoft Windows. The third-party X software included with RAMS comes with a 30-day evaluation license. To continue to use the software after this initial 30-day period, you must purchase a license from NetSarang Computer, Inc.

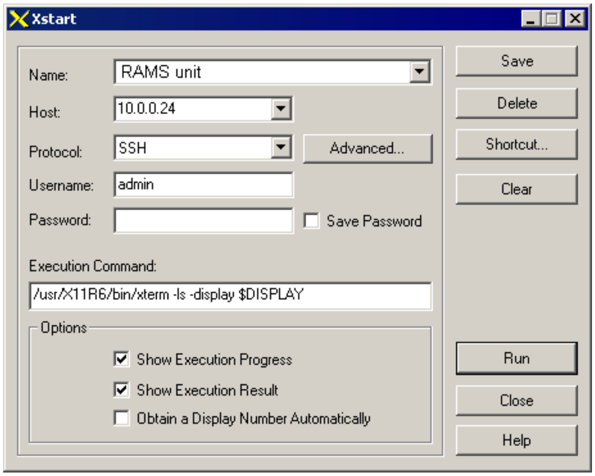
To download and install Xmanager™ for Windows, perform the following steps:

1. Using a web browser, connect to the RAMS *Home* page.
2. To view a demonstration of the XManager setup, click **`Xmanager Setup`**.
3. Click **`Xmanager 30 Day Evaluation`** to download an evaluation copy of Xmanager.

   The *File download* window opens.
4. Select **`Save this file to disk`**, and then click **`OK`** to save the Xmanager executable file to the specified local directory.
5. Open the `xmgr20.exe` file. The *Welcome* screen appears.
6. Follow the on-screen instructions to install Xmanager.

To start XManager, perform the following steps:

1. Double-click the Xmanager icon on the desktop.
2. Open **`Xstart`** from the Xmanager folder. The *Xstart* window is shown in Figure 27.



Name: RAMS unit

Host: 10.0.0.24

Protocol: SSH

Username: admin

Password:

☐ Save Password

Execution Command:

```
/usr/X11R6/bin/xterm -ls -display $DISPLAY
```

Options

☑ Show Execution Progress

☑ Show Execution Result

☐ Obtain a Display Number Automatically

Figure 27 Xstart Connection Details

3 Enter the connection details in the *Xstart* window that appears:

- Name: Enter a name for the session.
- Host: Enter either the hostname or IP address of the RAMS appliance.
- Protocol: Select SSH – to ensure privacy and security, RAMS accepts only SSH connections.
- User name and Password: Enter your RAMS user ID and password.

Note The Execution Command is not used

4 Click **`Save`** to save the connection details.

5 Click **`Shortcut`** to create a shortcut on the Windows desktop for easy repeat access.

6 Click **`Run`** to start an X session and open the application..

Note The first time the SSH connection is initiated, a *Security Warning* dialog may appear. Click **`Yes`** to save the host key and continue.

X Window Server for Unix Platforms

The X Window system is included with Linux and Solaris platforms.

Note SSH is required to run RAMS through the X Window system.

To run the X Window system on Red Hat Linux, perform the following steps:

1. Ensure a graphical user interface such as KDE or Gnome is running on the desktop.
2. From the shell in a terminal window, open an SSH connection to RAMS. Type the following command:

   ```
   ssh X userid@rex
   ```

   For example:

   ```
   ssh X op@10.0.0.24
   ```

3. Enter the RAMS user password when prompted.

   The RAMS application opens on the desktop.

To run the X Window system on Solaris, perform the following steps:

1. Ensure that a graphical user interface, such as OpenWindows or CDE, is running on the desktop.
2. Open an SSH connection to RAMS in a terminal window (CDE) or shelltool (OpenWindows). Type the following command at the shell prompt:

   ```
   ssh X userid@rex
   ```

   For example:

   ```
   ssh X op@10.0.0.24
   ```

3. Enter your RAMS password when prompted.

   The RAMS application opens on the desktop.

Note

RAMS is expected to work with the X Window system on other platforms, but they may not be tested or fully supported. For more information on these platforms, go to **www.openview.com**, and look up the Route Analytics Management System product.

VNC Client

To use VNC, a VNC viewer (client) must be installed on the user's system. The VNC viewer then connects to the VNC server running on the RAMS appliance. Before starting the VNC viewer on the desktop, configure and start the VNC server as described in VNC Server Configuration on page 31.

Downloading VNC

The RAMS *Home* page offers five versions of the VNC viewer:

- Windows 9x, NT, 2000, XP
- Linux (x86)
- Macintosh (os9)
- Macintosh (osX)
- Solaris (sparc)

RAMS supports the above viewers. It is possible to use another viewer but HP recommends that one of these be selected.

RAMS may also be used with VNC on other operating systems. To download a version of VNC for another operating system, please check the VNC home page at **http://www.realvnc.com** for the appropriate version of the viewer. Additional documentation for VNC is also available at that web site.

Downloading and Installing VNC on Windows

To download and install VNC, perform the following steps:

1. On the RAMS *Home* page, click the link for the appropriate version of the VNC viewer.

   The *File download* window opens.

2. Select **`Save this file to disk`**, and then click **`OK`**.

   This saves the VNC client to a local directory.

3 The downloaded VNC file is compressed. Before installing it, decompress it with a application such as WinZip.

4 Run the VNC `viewer.exe` file to install VNC.

After installing VNC, start it.

To start VNC, perform the following steps:

1 Double-click the VNC icon.

The *Connections Details* dialog appears.

2 If this is a first-time installation, adjust the optional settings as desired. Click **`Options`** to display the *Connection Options* dialog.

3 Check **`Tight Encoding`** to improve performance.

4 Check **`Full-screen mode`** to eliminate the VNC viewer's scroll bars and window frame. This prevents the taskbar and minimized icons on the RAMS desktop from being scrolled off-screen.

> **Note** When the VNC display is in full-screen mode, the Windows taskbar will not be visible. Type **`Ctrl-Esc Esc`** to make the Windows taskbar visible, then right-click on the VNC icon to see the menu.

5 Click **`OK`** to close the *Options* dialog.

6 Enter the RAMS IP Address or hostname in the *VNC Server* text box followed by ":1".

7 Click **`OK`** to start the VNC viewer.

> **Note** If a "`Failed to connect to server`" warning appears, either the VNC server is not running or RAMS is in single operator mode and another operator is already accessing it. Contact the RAMS administrator to resolve the problem.

8 In the *VNC Password* dialog, enter the VNC authentication password as set in the VNC Server Configuration on page 31.

9 Click **`OK`**.

This starts the VNC viewer.

10 To save the optional settings for VNC, right-click on the VNC icon in the Windows taskbar and select **`Save connection info as`** from the menu.

Downloading and Installing VNC on Linux

To download VNC, perform the following steps:

1 Click the link for the appropriate version of the VNC viewer.

The *File Download* window opens.

2 Select **`Save to disk`**.

The *Save As* dialog opens.

3 Choose the location for the file, and then click **`OK`**.

To decompress VNC, perform the following steps:

1 Open the console and log in as `root`.

2 Change to the directory where the TightVNC rpm was saved.

3 Enter the following command:

```
rpm -U vnc-3.3.3r2+tight1.2.4-1.i386.rpm
```

When the installation completes, the shell prompt reappears.

4 To verify the installation, enter the following command:

```
rpm -qa | grep vnc
```

To start VNC, perform the following steps:

1 Enter the following command at the command line, where `a.b.c.d` is the RAMS IP address or hostname:

```
vncviewer a.b.c.d:1
```

or

```
vncviewer -fullscreen a.b.c.d:1
```

Note The warning “`vncviewer: ConnectToTcpAddr: connect: Connection refused`” will appear if you omit the “`:1`” at the end of the IP address or if the VNC server is not running. In the latter case, contact the RAMS administrator and request that he or she start the VNC Server from the Administration page.

2 At the password prompt, enter the VNC authentication password as set in the VNC Server Configuration on page 31.

This starts the VNC viewer.

Note If RAMS is in Single Operator mode and another operator is already accessing it, the following message appears on the console: “`vncviewer: VNC server closed connection.`” Contact the RAMS administrator to resolve the problem. If shared access to the VNC desktop is appropriate, ask the RAMS administrator to change the setting to Multiple Operators and restart the VNC server.

3 To exit the VNC viewer when in full-screen mode, use the F8 key to bring up the menu and select **`Quit viewer`**.

Opening RAMS Application in VNC

When the VNC server is initially started, the RAMS application is automatically started on the VNC desktop so it appears as soon as the VNC viewer connects to the server.

If the RAMS application is subsequently closed using the **`Quit`** menu command or by closing the main window, then the next time VNC is opened the desktop will appear without the RAMS main window. In that case, proceed as follows:

1 Left click in the background of the VNC desktop or click **`Start`** from the taskbar at the bottom of the VNC desktop.

2 Click RAMS.

The RAMS main window opens.

4

RAMS Basics

This chapter describes the main RAMS windows that you use to display and monitor the network. These include:

- The *Routing Topology* window, which displays a graphical representation of the topology.
- The *History Navigator* window, which displays a graph indicating events that occur in the current topology.

In addition, this chapter provides a brief overview of the tasks that RAMS can perform for you. Chapter , “The Routing Topology Map,” provides a detailed description of the Routing Topology map, and Chapter , “The History Navigator,” provides a detailed description of the *History Navigator* window.

Selecting a Routing Topology

The routing topology is the overall view of the routing activity on the network that RAMS is monitoring. Each stored database has a corresponding routing topology. The routing topologies are displayed as a map in the main window of the RAMS application.

Chapter 3, "RAMS Clients" explained how to start the RAMS application in X-Windows or the VNC viewer. The next step is to select and open a routing topology.

To open a routing topology, perform the following steps:

1 Select **`Open Topology`** from the Topology menu on RAMS's main window.

The *Open Topology* dialog appears (see Figure 28). The names of databases that are currently recording data appear in green letters, while the names of inactive databases appear in black letters.

2 Select the desired databases from the list provided. Selected items are highlighted, as shown by *CorpNet* in the figure. Any combination of databases can be selected using the **`Shift`** key to extend the range of selected items or the **`Ctrl`** key to add or remove selected items. Selecting a higher-level folder implicitly selects all the folders contained within it.

3 Click **`Open`**.

After the database loads, the topology map appears in the main RAMS window, as shown in Figure 29. The larger the database the more time is required to load and lay out the nodes on the map. After the topology layout is saved, as explained in Chapter , "The Routing Topology Map," the database loads more quickly when it is reopened.

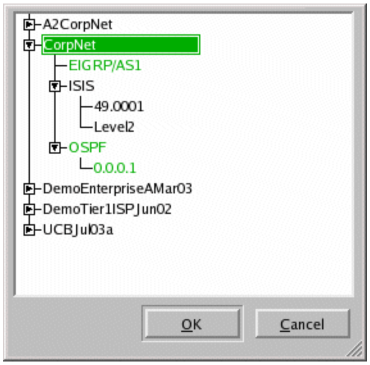


Figure 28 Open Topology Dialog

The Topology Map

The routing topology map displays the status of the routers and links in the entire network at a glance, which lets you quickly see any outages. The topology map provides a view of the network as it is currently running, including any tactical changes made during outage repairs that might not be reflected in the network design documents. The topology map is described in more detail in Chapter , “The Routing Topology Map.”

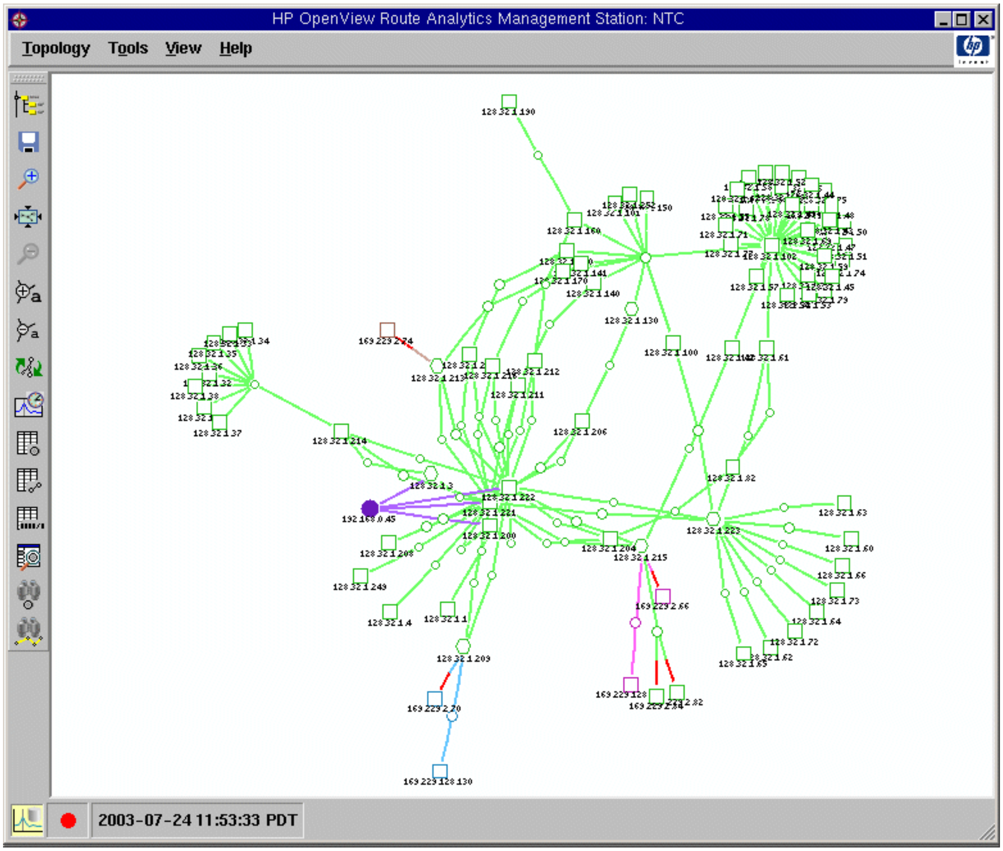
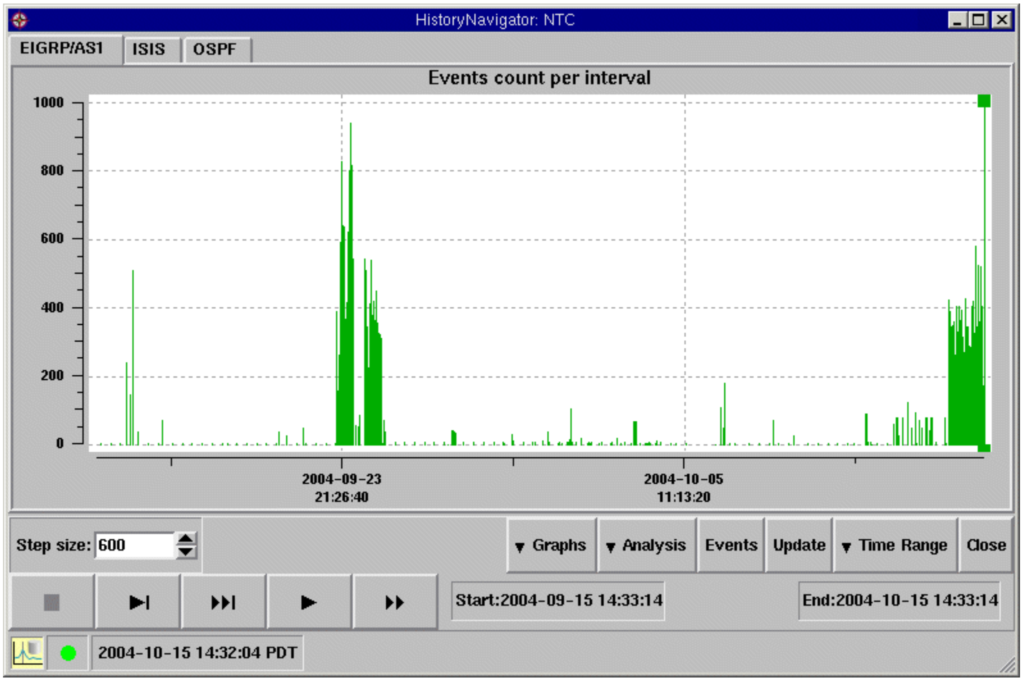


Figure 29 **Topology Map**

The History Navigator Window

The *History Navigator* window, in combination with the topology map, allows you to display information about your network in a wide variety of ways. You can choose to display detailed lists of events; move back in time to a specific event and see that event replayed in the topology map; distill large quantities of data related to an event down to the essentials, or view a real-time graph of events as they occur.

Initially, the *History Navigator* window contains a graph of recorded network routing events. An example of the window is shown in Figure 30. The controls and functions available in the *History Navigator* window are described in detail in Chapter , "The History Navigator."



Step size: 600

Start:2004-09-15 14:33:14

End:2004-10-15 14:33:14

2004-10-15 14:32:04 PDT

Figure 30 History Navigator Window in History Mode

If the topology map currently displayed by the RAMS is an actively recording database, you can switch between History mode and Online mode by clicking the mode icon located in the lower left-hand corner of the window. If the topology is not currently recording, the only mode available is *History* mode.

When in Online mode, the *History Navigator* window displays routing events as they occur. Online mode is available when an active database is selected from the *Open Topology* dialog. While RAMS is displaying an active database, it continuously updates the routing topology map and the *History Navigator* window from the network routing announcements it receives. Figure 31 shows an example of the *History Navigator* window in *Online* mode.

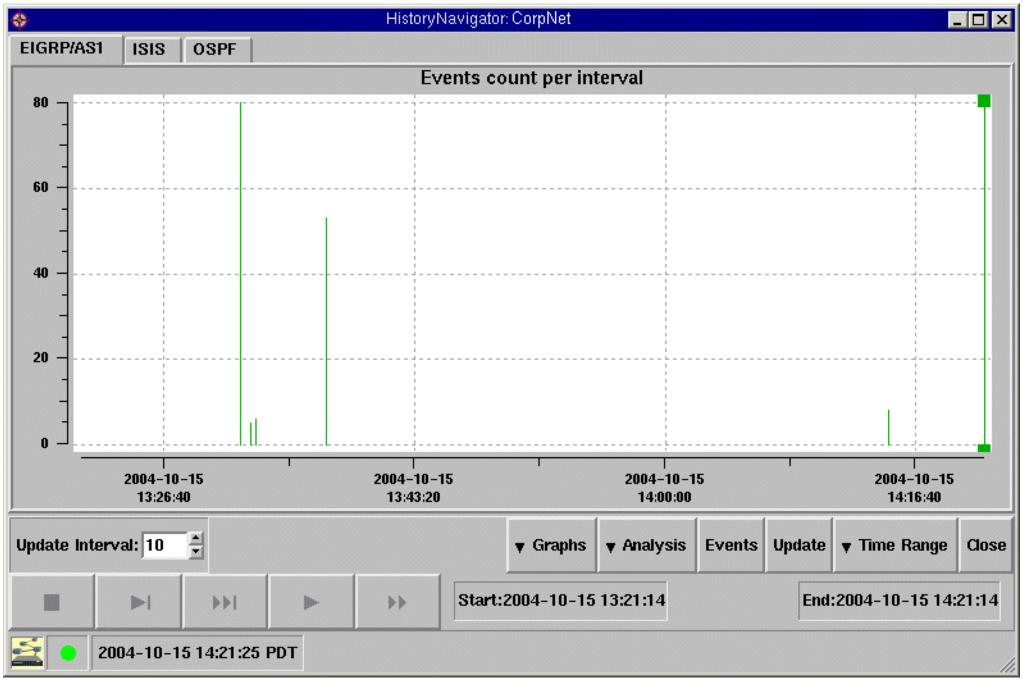


Figure 31 **History Navigator Window in Online mode**

The controls for the window in Online mode are the same as those present when the window is in History mode. However, options that do not apply in Online mode are disabled, such as playback controls and several of the Analysis options.

To switch between the Online mode and History mode, click the mode icon at the lower left-hand corner of the window.

Overview of RAMS Uses

RAMS lets you perform a variety of tasks that are not possible with traditional network management systems' displays. Some of these tasks are as follows:

- Viewing a comprehensive routing topology of a multiprotocol, multidomain network.

  RAMS monitors and displays the most complex multiprotocol, multi-AS routing networks. If a network consists of a single level IS-IS network with hundreds of routers, a multiarea OSPF network with many areas, or a global multi-AS network with EIGRP, OSPF, and BGP, RAMS can display the network in a unified topology map.

- Viewing complex routing hierarchies by abstracting and drilling down.

  RAMS lets you display and monitor the largest network topologies. You can display the whole network map and zoom in to specific areas to view the network in more detail.

- Finding routing and topology anomalies at a glance, for example, single points of failure or reduced redundancy.

  You can use the topology map to see possible points of failure, failed links and routers, and other routing anomalies. The Online Update Monitor displays routing changes as they occur. The history of events and summary statistics for the past 10 minutes (this time period is changeable) can alert you to potential route floods or cascade outages.

- Obtaining a complete up-to-the-minute inventory of the most vital network service parameters.

  A large enterprise of service provider networks may have hundreds of routers with thousands of prefixes attached. Summarization across boundaries helps reduce the amount of information carried across the network, but also makes it difficult to quickly determine the cause of a service outage. RAMS's prefix list lets you see which routers in a network are advertising default routes, see if a prefix is currently advertised and by which routers, see what metric is advertised with each prefix, verify that area border routers are properly re-advertising prefixes, and display the BGP prefixes advertised and the list of attributes associated with each prefix.

- Obtaining a summary view of the network’s current comprehensive Routing Information Base (RIB) or view the RIB at any point in the recorded topology history.

  RAMS’s RIB Browser helps you perform these tasks:

  - Determine which IGP prefixes and links are down and which routers are involved.
  - Determine if a customer or peer is flooding the network with unexpected routes.
  - Determine if a provider has withdrawn all their routes.
  - Determine which BGP hops there are from a network and how many routes each BGP is advertising to the network.
  - Obtain a list of all LOCAL-PREF values used in a network to make sure they conform to the routing policy and traffic engineering goals.
  - Determine what MED values are being advertised to the network and determine if they conform to network policy.
  - Display a list of all communities advertised and a distribution of routes with those communities.
  - Display all of the neighboring ASs or second hop neighboring ASs and the number of Internet routes through each.
  - Display all of the routes learned from a particular route reflector in the network.

- Viewing a visualization of a BGP network.

  RAMS lets you display the state of the BGP RIB (Routing Information Base) at any point in time as a still image.

- Performing a Root Cause Analysis of a BGP network.

  RAMS lets you distill the huge amounts of routing data generated by BGP nodes down to the essential information that reveals the root cause of a BGP event. The root cause event can be displayed as an animated visualization.

- Obtaining a high level summary of all routing events between two points in time.

  When diagnosing a network outage or performing forensic analysis after an outage, having complete historical data and analysis capability can prove invaluable. RAMS's Event Analysis lets you narrow down the event churn to the root cause.

- Displaying the history of the routing events and drill-down for diagnosis or forensics.

  Many routing instabilities are caused by interactions between multiple routers and are very difficult to isolate because routers do not keep an event history. You can use RAMS's Events List to display all of the events associated with a selected prefix during a selected time period.

- Displaying all the exit routers for any Internet destination from all points in the network.

  In a large network with multiple exit routers to the Internet, it is often useful to see the exits that routes take from various points in the network. RAMS can display all of the exit routers for all routers in a network or from a specific single router.

- Highlighting the IP route between two points in a network for scenario planning.

  Displaying the IP paths taken by traffic from a source router to a destination router in a multidomain network is very useful for network planning. RAMS can quickly display the current path between two points in the network or display the path at any time in the history of the network.

Chapter , "The Routing Topology Map," and Chapter , "The History Navigator," cover all of the above points in greater detail.

5

The Routing Topology Map

The routing topology map displays the status of the routers and links in the entire network at a glance, which lets you quickly spot outages. This chapter describes in detail the routing topology map and the various tools used to monitor the network.

The topology map provides a view of the network as it is currently running, including any tactical changes made during outage repairs that might not be reflected in the network design documents.

You can use the routing topology map to anticipate and head off user complaints by identifying any routing failures in the network. You can also identify potential configuration errors that might result in service outages following maintenance activities.

The routing topology map lets you view the routing events that led to failure, to aid forensic analysis. It also provides an accurate, vendor-independent view of the routing network that often points out potential implementation or interoperability issues that are not easily isolated using other tools.

Map Layout

The routing topology map consists of a variety of symbols, representing nodes, interconnected by lines that represent links. The symbols have different shapes depending upon the nodes' functions:

- Square nodes are routers internal to a protocol domain (Autonomous System) or on the border between domains.
- Hexagons denote Area Border Routers (ABR) located on the border of one or more OSPF areas and connecting those areas to the backbone OSPF area. In an EIGRP network, hexagons denote routers that are redistributing routes between EIGRP ASs.
- Open circles indicate the pseudonodes that represent multiaccess networks (LANs) in OSPF and ISIS.
- Filled circles represent BGP peers.

The nodes and links in each routing area of the network are drawn in a different color. You can turn the coloring off such that all nodes are black and all links are gray.

Links are divided into two halves representing the two directions of communication between a pair of nodes. The half adjacent to a node represents the direction outbound from that node. Each half can be separately up or down. Links that are down are bright red instead of the area color or gray. If a link represents multiple physical links between two nodes, and if only some but not all of the physical links are down, then the link will be dark red instead of bright red. Nodes that are down are also colored red.

Since RAMS cannot determine whether a node or link that goes down has temporarily failed or been decommissioned, an adjustable timeout interval determines when nodes and links that are down should be removed from the map (see Configuration Options Dialog on page 169).

A randomizing process creates the placement of the nodes in the routing topology map. The placement is not geographical. You can move nodes by dragging them with the mouse to create a preferred layout. Multiple different layouts can be named and saved, and each user can set a default named layout. You should save your layout periodically as the network topology changes. This helps RAMS to load the routing topology map more quickly.

Note User who are familiar with other HP OpenView products, such as Network Node Manager, should be aware that the RAMS product uses a different set of symbols and status colors to represent the routing topology.

Figure 32 shows an example of the RAMS window. The menus, tools, and other features of the window are described in detail below.

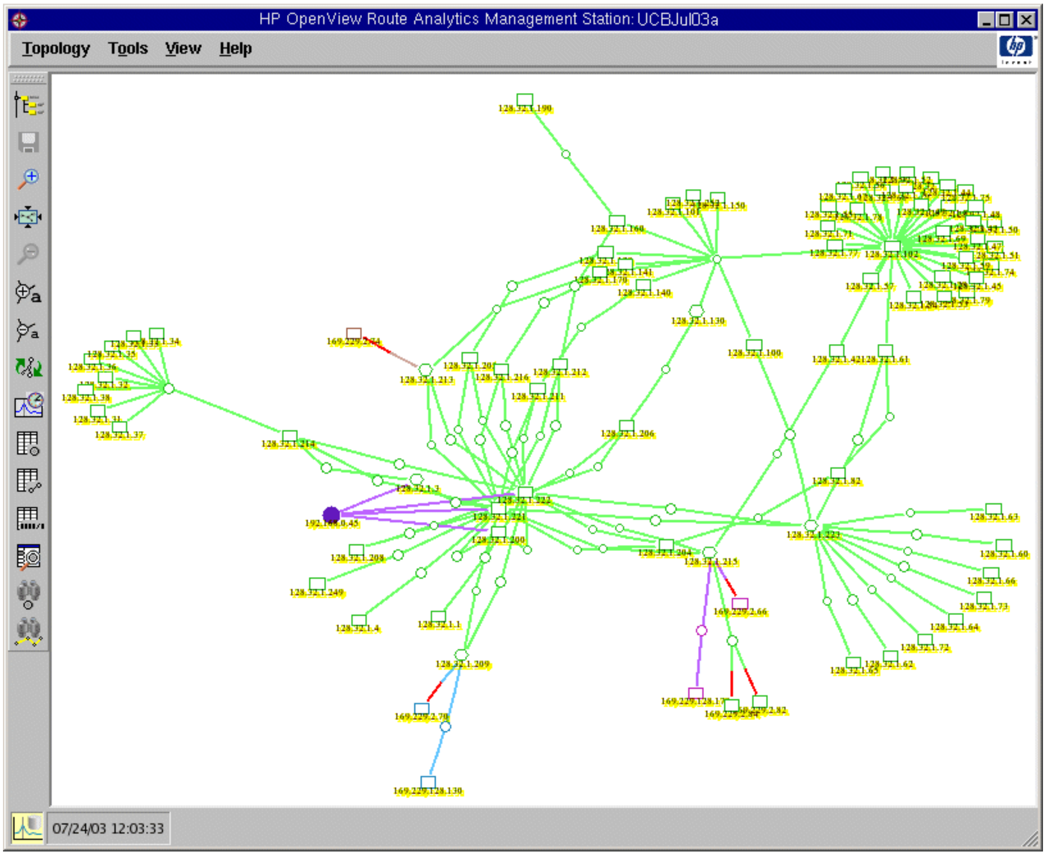


Figure 32 RAMS Window

Toolbar

The RAMS window has a toolbar along the left side with buttons that control the map display or provide shortcuts to menu options, as shown in Figure 32. You can move the toolbar to the right side or the top or bottom of the window by dragging the dimpled strip at the top of the toolbar.

The buttons on the toolbar are as follows:

Open Topology Explorer inserts a pane on the left side of the map window to display a hierarchical view (a tree structure) of the set of routing databases displayed in the map. See Topology Explorer on page 129 for a description of the available operations.

Save Layout saves the current map layout (disabled if no changes). If this is the first time you have saved the layout, a dialog allows you to name the layout and specify it as your default layout.

Zoom In and **Zoom Out** control the zoom level of the map display.

Reset View to 1:1 restores the zoom level to the default.

Node Size Up and **Node Size Down** increase or decrease the size of nodes and their accompanying text.

Relayout generates a new randomized layout of the nodes.

History Navigator opens the *History Navigator* window for the current topology. Shortcut to the corresponding option on the Tools menu.

VPN Navigator opens the *VPN Navigator* window for the current topology. Shortcut to the corresponding option on the Tools menu. This icon is only present if the RAMS unit has a license for the VPN protocol module.

List Routers generates a list of all routers in the current topology map. Shortcut to the corresponding option on the Tools menu (see Tools Menu on page 124).

List Links generates a table that lists all links in the current topology map. Shortcut to the corresponding option on the Tools menu (see Tools Menu on page 124).

List Prefixes generates a list of all prefixes in the current topology map. Shortcut to the corresponding option on the Tools menu (see Tools Menu on page 124).

RIB Browser opens the *RIB Browser* window. Shortcut to the corresponding option on the Tools menu (see Tools Menu on page 124).

Find Router opens the *Find Router* dialog. Shortcut to the corresponding option on the Tools menu (see Tools Menu on page 124).

List/Find Path opens the *List/Find Paths* dialog. Shortcut to the corresponding option on the Tools menu (see Tools Menu on page 124).

Status Bar

At the bottom of the RAMS window is a status bar. The icon at the left edge indicates the mode:

Online mode – A network icon indicates that the topology is currently being recorded and updates to the routing database are shown on the topology map as they occur.

History mode – A graph icon indicates that only previously recorded information in the routing database is shown on the topology map.

You can switch between modes by clicking the mode icon.

A colored dot to the right of the mode icon indicates Route Recorder status with different colors as listed in Table 5. If you position the mouse cursor over the colored dot, additional information on the recorder status is displayed.

Table 5 Status Indicator States

Color	Description
Green	Indicates Route Recorder is running and recording to the database, and adjacencies between Route Recorder and peer routers in all areas are up.
Blue	Indicates data is being recorded, but EIGRP topology exploration is in progress so changes in the topology will not be shown until completion.
Yellow	Indicates data is being recorded, but adjacencies to peer routers in some areas are down.
Red	Indicates no data is being recorded, either because Route Recorder is not running or all adjacencies with peer routers are down.

Next to the status indicator is the date and time of the network state currently being shown on the routing topology map. Status messages appear to the right of the date and time when applicable.

Menu Bar

The menu bar at the top of the RAMS window contains four pull-down menus:

- Topology menu
- Tools menu
- View menu
- Help menu

Use these menus to open routing topology maps and monitor and analyze routing data. The remainder of this section describes the options on these menus in more detail.

Topology Menu

The options available on the Topology menu are as follows:

- **Open Topology** – Opens a routing topology database, displaying the topology map in the RAMS window.
- **Close Topology** – Closes a routing topology database so that another can be opened.
- **History Mode** – Changes the RAMS window from Online mode to History mode.
- **Reload Layout** – Restores the node positions according to the previously loaded layout (disabled if no layout is loaded or no nodes have been moved).
- **Save Layout** – Saves the current node positions into the loaded layout (disabled if no changes). Same as **Save Layout As** if no layout is loaded.
- **Save Layout As** – Opens the *Save Layout* dialog to allow saving the current node positions as a new layout with a new name. You can also set the new layout as the default.
- **Load Layout** – Loads a saved layout to reposition the nodes. Multiple layouts can be saved under different names for different purposes.
- **Delete Layout** – Deletes a named layout.

- **Relayout** – Creates a new randomized placement of the nodes on the topology map, which can be helpful to find a preferred orientation that can then be named and saved.
- **Resolve DNS** – Resolves all of the node addresses on the topology map into DNS names. In a large network, this can take some time.
- **Quit** – Closes the RAMS client (RAMS itself continues to run).

Tools Menu

Use the Tools menu to view and analyze the routing layout. The options on the Tools menu are as follows:

- **History Navigator** – Opens the *History Navigator* window to allow “navigating in time” to analyze past routing data (see Chapter 6, “The History Navigator”).
- **RIB Browser** – Opens the *RIB Browser* window (see RIB Browser on page 196).
- **VPN Explorer** – Opens the *VPN Explorer* window to allow configuring and monitoring a VPN (see Chapter 8, “VPN Configuration and Reports”). This option is only present if the RAMS unit has a license for the VPN protocol module.
- **Correlate Time Series** – Opens the *Time Series File Selection* dialog to display a graph of external time series data in correlation with the routing history (see Correlating Time Series Data on page 224).
- **List Routers** – Opens the list of all routers on the routing topology map (described in Finding a Router on page 144).
- **List Links** – Opens the list of all links on the routing topology map (see Links List on page 149).
- **List Prefixes** – Opens the list of all prefixes announced by routers on the routing topology map (see Prefix List on page 150).
- **List VPN Prefixes** – Opens the list of all prefixes that are part of a VPN (see Chapter 8, “VPN Configuration and Reports”). This option is only present if the RAMS unit has a license for the VPN protocol module.

- **List Router/Link Edits** – Opens a list of routers and links on the routing topology map that have been edited (state changed or link metric changed) for *what-if* analysis (see the procedure for displaying Router/Link Edits on page 162). Disabled if no routers or links have been edited.
- **Find Router** – Opens the *Find Node* dialog box that enables you to search for routers by IP address or router name (described in Finding a Router on page 144).
- **List/Find Paths** – Opens the *List/Find Paths* dialog box that lets you highlight a path between a router and an Internet prefix or domain name (see Finding a Route By Prefix on page 158).
- **Highlight by Exit Router** – Finds the set of exit routers toward a specified prefix, IP address or domain name, then color-codes all routers to indicate which exit router each will use. The border routers that act as exit routers to the specified destination flash between the coded color and yellow. For more details, see Viewing the Exit Routers from the Network for any Internet Destination on page 153.

  Note To highlight exit routers, the displayed network must include a route to the desired destination.

- **Assign BGP ASs to Routers –** Allows you to assign routers manually to a BGP AS, primarily for a BGP confederation. See Verify and Manually Assign BGP AS Assignments to Routers on page 154.
- **Topology Diagnostics** – Presents a submenu to select display of several diagnostic tables (EIGRP topologies only). See Topology Diagnostics Submenu on page 125.
- **Options** – Opens the RAMS *Configuration Options* dialog box. Use this dialog box to configure the settings for the *Online Update Monitor* and *History Navigator* windows and set other preferences (see Configuration Options Dialog on page 169).

Topology Diagnostics Submenu

The topology diagnostics submenu is present only for EIGRP topologies. It provides several options to display any problems found in the network configuration or in RAMS's modeling of the topology. These options are described in detail in Diagnosing EIGRP Topology Errors on page 174.

- **List Topology Errors** – Opens a list of messages describing anomalies that were discovered during exploration of the EIGRP topology. Clicking on an entry in the list highlights the affected routers and links.
- **List Inaccessible Routers** – Opens a list of routers that were not accessible via telnet during exploration of the EIGRP topology, including a reason such as authentication failure. Clicking on an entry in the list highlights the last accessible router on the path toward the inaccessible router.

  Note Inaccessible routers are not shown on the topology map. They can cause incorrect routes to be displayed and can reduce RAMS's ability to track changes in the network topology.

- **List Mismatched Distances** – Opens a list of prefixes for which the distance to the prefix reported by a router that peers with RAMS does not match the distance that RAMS calculates across its model of the topology. This list also shows when the periodic topology explorations start and end, along with summary statistics.
- **Find Invisible Links** – Runs a simulation on the RAMS topology model to determine if there are any links where a failure will not be immediately detected because the routers that peer with RAMS will not report an EIGRP distance change.

  Note The simulation can take several hours to run on a large network topology. You can cancel it at any time.

View Menu

The view menu has the following options:

- **Show Topology Explorer** – Inserts a pane on the left side of the map window to display a hierarchical view (a tree structure) of the set of routing databases displayed in the map (see Topology Explorer on page 129). Toggles to **Hide Topology Explorer** when the pane is shown.
- **Hide Toolbar** – Turns off the toolbar on the left edge of the main RAMS window, and toggles to **Show Toolbar**.

- **Node Label Modes** – Opens the Node Label Modes submenu. See Node Label Modes on page 127.
- **Color** – Colors each area of the topology map with a distinct color.
- **Uncolor** – Removes colors from the topology map, so that failed links and nodes can be more easily seen.
- **Trim Nodes** – Opens the *Trim Nodes* dialog where you can specify that nodes matching a pattern be hidden from view on the routing topology map (see Trimming the Displayed Nodes on page 141).
- **Unhide All Nodes** – Displays any hidden (trimmed) nodes.
- **Trim Leaf Nodes** – Removes nodes that are on the edges of the map with a single link to simplify the map display (see Trimming Leaves on page 142).
- **Hide Failed Nodes** – Removes failed nodes from the display.
- **Zoom In** – Enlarges the center portion of the topology map to fill the window, reducing the amount of the map that is visible.
- **Zoom Out** – After **Zoom In** has been done, **Zoom Out** shrinks back the routing topology map to increase the amount of the map that fits within the window.
- **Node Size Up** – Increases the size of node symbols and their accompanying text on the routing topology map. Does not affect zoom level.
- **Node Size Down** – Decreases the size of node symbols and their accompanying text on the routing topology map. Does not affect zoom level.
- **Node Size Reset** – Resets the size of nodes and their accompanying text to the default size. Does not affect zoom level.
- **Reset View to 1:1** – Resets the *Routing Topology* window to the original zoom level.

Node Label Modes

Use the options on the Node Label Modes submenu to specify the node identification displayed with each node on the routing topology map.

- **Label Routers Only** – Does not label the pseudonodes representing LANs.
- **IP Address** – Displays the router IP address.
- **DNS Names** – Displays the router DNS name. If no DNS name resolution has been performed yet, selecting this mode will initiate DNS name resolution for all routers. In a large network, this can take some time.
- **Router Names** – Displays the name of the router obtained from the protocol (if available).
- **System ID** – Displays the IS-IS System ID (for IS-IS networks).
- **ID Number** – Displays RAMS's internal ID number for the router, which may be useful as a shorthand reference.

Note The menu options displayed depend on the network protocol. For example, all of the above options appear for an IS-IS network, while Router Names and System ID do not appear for an OSPF network.

Help Menu

The Help Menu contains two options. The **Contents** option displays the PDF version of this guide in a new window. The **About** RAMS option displays RAMS version information.

Topology Explorer

The *Topology Explorer* presents a hierarchical view (a tree structure) of the set of routing databases shown in the routing topology map. It lets you to work with a subset of the topologies displayed in the RAMS window. This is particularly useful for large networks that contain a number of different IGP areas and BGP ASs.

When requested, the Topology Explorer appears on the left side of the map window, as shown in Figure 33. You can display the Topology Explorer from the **View** menu or by clicking the button on the toolbar. To close the Topology Explorer, click the **X** button in the upper right-hand corner of the Topology Explorer pane or click the button again.

The **Tools** and **View** menus within the Topology Explorer pane contain a subset of the items on the similarly named menus on the main window menu bar, but they operate only on the areas selected from the tree structure. So, for example, by using the Topology Explorer **Tools** menu, it is possible to list the routers in just one area.

Alternatively, RAMS lets you display each individual area or AS in a separate window. Click **`New View`** to open a new topology map window containing only the selected areas.

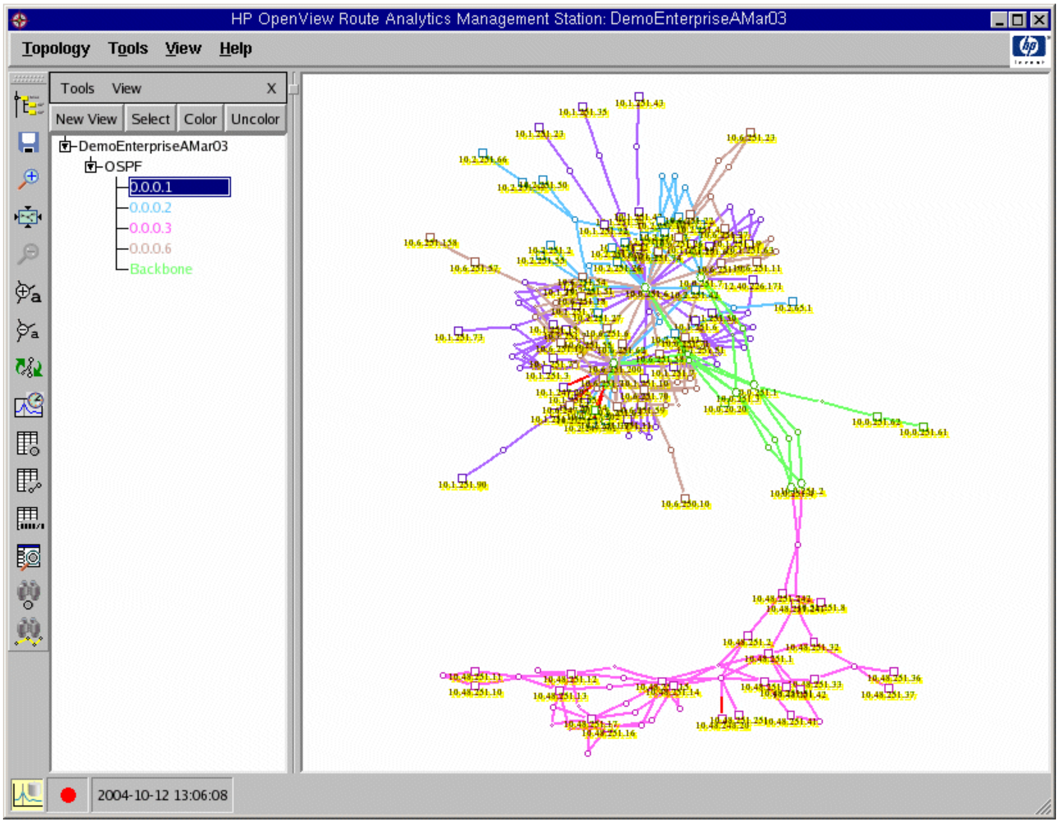


Figure 33 RAMS Window with Topology Explorer Pane

To display an individual IGP area or BGP AS, perform the following steps:

1 Click on the toolbar or select **`Show Topology Explorer`** from the **`View`** menu.

A tree structure appears displaying the names of all the administrative domains in the network.

2 For the network shown in Figure 33, click area 0.0.0.1 in the tree structure.

3 Click **Select** in the Topology Explorer pane, and then click **Zoom In** on the toolbar to expand the selected area of the topology map to fill the window. Alternatively, click **New View** in the Topology Explorer pane to open a new window containing just the selected area, as shown in Figure 34.

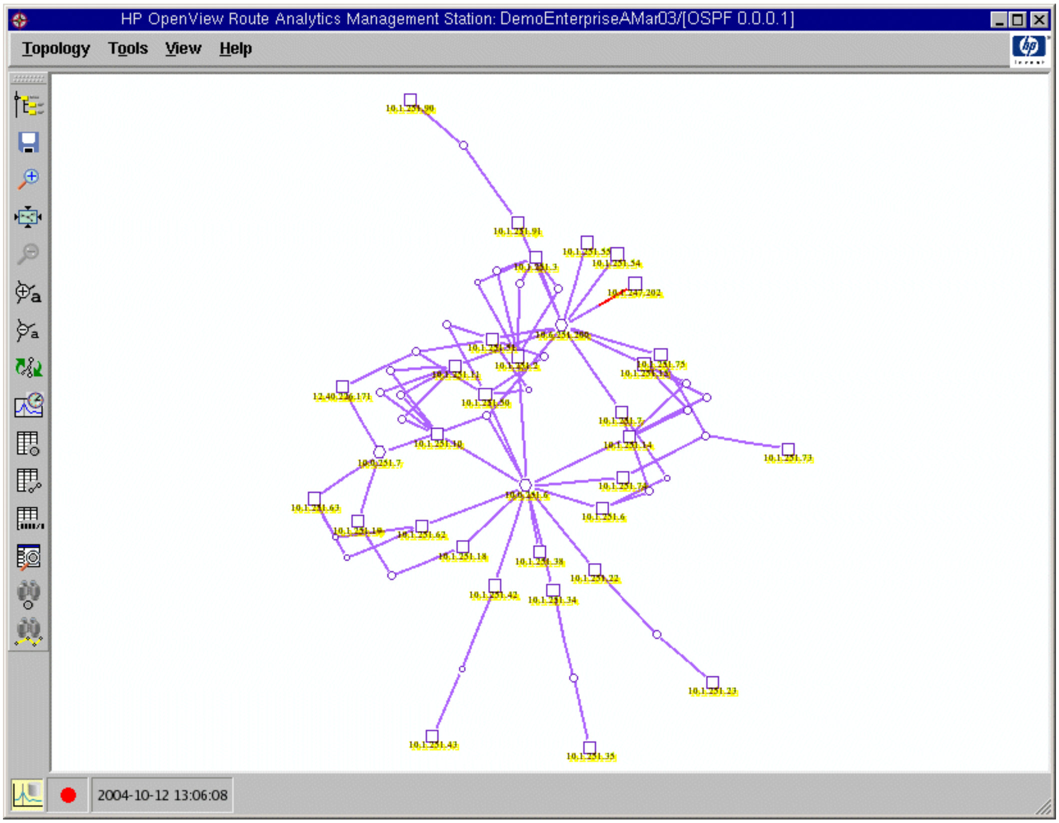


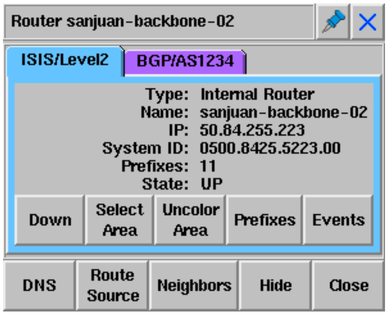
Figure 34 New View of Single Area

Viewing Node and Link Details

RAMS stores many details about the nodes and links on the routing topology map besides the IP address and name labels that can be displayed next to the nodes. Since there is not enough space to display those details all at once, additional details about a particular node or link can be viewed by right-clicking on the object to open an information panel overlaid on the map.

Node Information Panel

Right-click on a node in the routing topology map to access the node's information panel, as shown in Figure 35. If the node is a pseudonode, the corresponding Designated Router (DR) is highlighted in orange on the topology map at the same time.



Router sanjuan-backbone-02

Type: Internal Router
Name: sanjuan-backbone-02
IP: 50.84.255.223
System ID: 0500.8425.5223.00
Prefixes: 11
State: UP

Figure 35 Node Information Panel

The title bar of the node information panel displays the name of the node and contains a tack button and a close button. Click the tack button to keep the panel open while opening the information panel for another object on the topology map. If you do not use the tack button, the current information panel disappears when you click anywhere outside the panel or on any of the panel's buttons.

The center pane of the node information panel contains one or more tabs. Each displays the details for an instance of the node in a particular topology area (for example, OSPF area or IS-IS level). The color of the tab is the same as the color of the nodes and links in that area on the map, and the label identifies the protocol and area identifier.

The details available for a router depend upon the protocol, but typically include the type of the node and one or more identifiers. In addition, the number of prefixes the router announces and the Up or Down state of the router are shown. The tab label text is red if the router state is Down.

A row of buttons on each tab provides access to functions specific to the particular instance (routing process) on the node:

- **Down** – Simulates what would happen to highlighted paths if the selected router should fail. This button is enabled when in History mode and disabled when in Online mode.
- **Uncolor/Color Area** – Colors or removes colors from the area of the topology map that contains this node.
- **Select Area** – Selects all of the nodes within the routing area that contains this node. A bounding box is drawn around those nodes on the topology map, and then other operations can be performed on those nodes as described in the later sections of this chapter.
- **Prefixes** – Displays a list of the network prefixes announced by this router. The button is disabled when number of prefixes (shown on the information panel tab) is zero.
- **Events** – Displays a list of the routing events originated by this router. If a time range has been selected in the *History Navigator*, the same time range is used for this list; otherwise, events occurring in the last 10 minutes are listed.

A second row of buttons at the bottom of the node information panel selects functions that apply to all instances of the node:

- **DNS** – Resolves the address of this router into a DNS name. If the resolution succeeds, the DNS name for the router appears on an additional line in the node information panel. This button is not present for pseudonodes.
- **Route Source** – Sets this node as the starting point for path highlighting. After a node is set as the route source, the text on this button changes to **Route Destination** when the node information panel is displayed for another node, and the path between the two nodes is highlighted if you click the button. For an illustration, see Highlighting the IP Route Between Two Points in the Network on page 156. This button is not present for pseudonodes.

Note Paths are generally highlighted in yellow; an orange highlight indicates that the route is not complete.

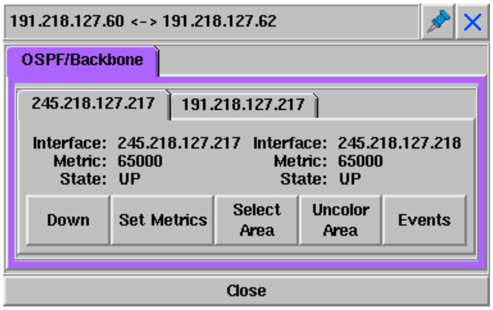
- **Neighbors** – Displays a list of neighboring routers and the interface addresses and metrics of the links connecting them.
- **Hide** – Hides the selected node. To redisplay the node, select **`Unhide All Nodes`** from the *View* menu.
- **Close** – Closes the node information panel. The panel will also close if you click on the map.

Link Information Panel

Right-click on a link in the routing topology map to open a link information panel similar to the example shown in Figure 36.

The title bar of the link information panel displays the name of the link and also contains a tack button and a close button. Click the tack button to keep the panel open while opening the information panel for another object on the topology map. If you do not use the tack button, the current information panel disappears when you click anywhere outside the panel or on any of the panel's buttons.

Each link has two halves representing the two directions of communication. The router interface corresponding to the half that was clicked will appear on the left side of the link information panel, except for links to pseudonodes, in which case the interface for the real router appears on the left and the pseudonode on the right. The direction is indicated by the node names in the title bar of the panel.



191.218.127.60 <-> 191.218.127.62

```
Interface: 245.218.127.217  Interface: 245.218.127.218
   Metric: 65000               Metric: 65000
    State: UP                   State: UP
```

Figure 36 **Link Information Panel**

The link information panel can have one or two levels of tabs:

- The outer level of tabs indicates the instance of the link in a particular topology area (for example, OSPF area or IS-IS level). There is more than one tab on the outer level if the routers at the two ends of the link participate in more than one routing protocol (or multiple instances of the same protocol). You can select a tab to display the link details corresponding to the tab's protocol instance. The color of each tab is the same as the color of the nodes and links in that area on the map, and the label tells the protocol and area identifier. The label text will be red if the link is down, or dark red if it is partially down.
- There is an inner level of tabs if the link on the map represents multiple, parallel, physical links between the two routers. The inner tabs are labeled with the interface of the router on the left side of the arrow in the title bar. The center of the tab shows two columns of details for the interfaces on the routers at the two ends of the link, including address, metric, and state. For EIGRP, the bandwidth and delay are shown individually as configured on the interface, and in addition, the EIGRP metric is shown as two components calculated from inverse bandwidth and delay that are added. The details for each end correspond to the link direction outbound from that router. The text on the inner tab label will be red if the interface is down.

A row of buttons on the tab provides access to functions specific to the particular instance (routing process) on the node:

- **Down** – Simulates what would happen to highlighted paths if the selected physical link (interface) should fail. For OSPF and IS-IS, both halves of the duplex link are taken down. For EIGRP, only one half (a simplex link) is taken down in order to accurately represent the state of LAN interfaces. This button is enabled when in History mode and disabled when in Online mode.
- **Set Metrics** – Opens a *Set Metric* dialog to simulate a change to the metric for the physical link in one or both directions. The routing table for the topology is recalculated using the simulated metric and any highlighted paths affected by the metric change are redrawn. This button is enabled when in History mode and disabled when in Online mode.
- **Uncolor/Color Area** – Colors or removes color from the area of the routing topology map that contains this link.

- **Select Area** – Selects all of the nodes within the routing area that contains this link. A bounding box is drawn around those nodes, and then other operations can be performed on those nodes as described in the later sections of this chapter.
- **Events** – Displays a list of the routing events related to adjacency changes on this link. If a time range has been selected in the *History Navigator*, the same time range will be used for this list; otherwise, events occurring in the last 10 minutes will be listed.

The **Close** button at the bottom of the link information panel closes the panel. The panel will also close if you click on the topology map.

Viewing Complex Routing Hierarchies

In a complex network, such as the one illustrated in Figure 37, it can be very difficult to see exactly what is happening. RAMS provides tools that let you tailor your view of the network so that the display contains just what you need to see.

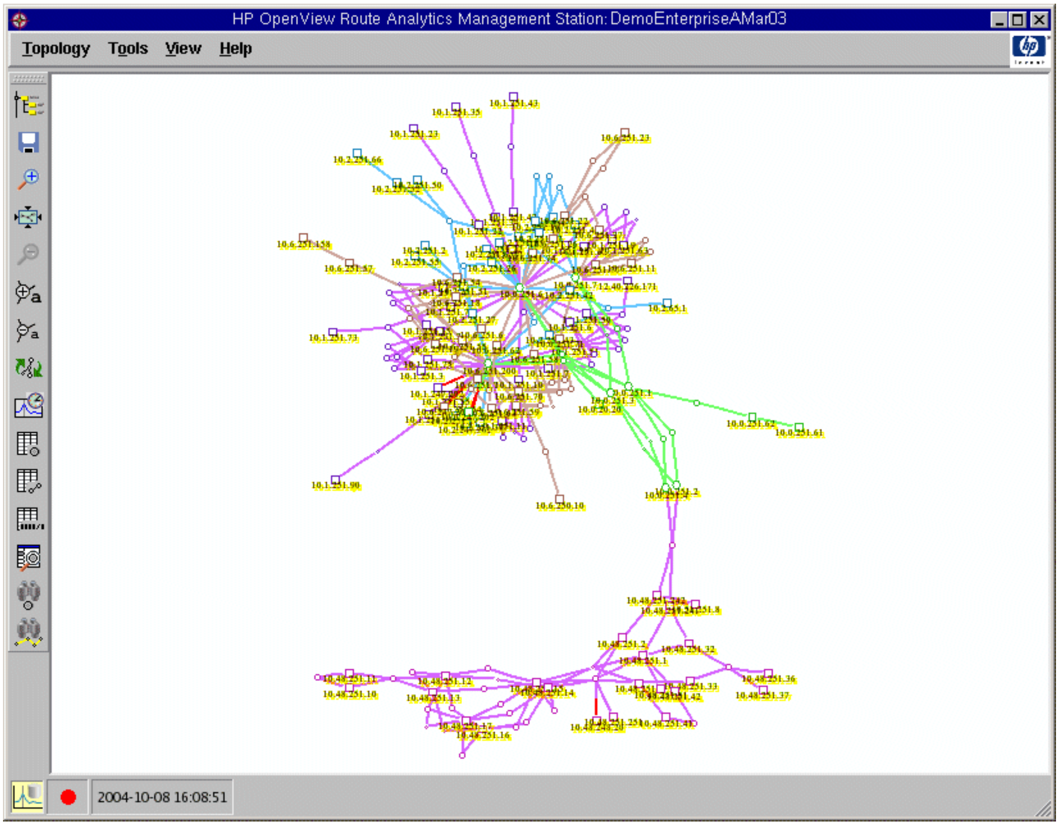

HP OpenView Route Analytics Management Station: DemoEnterpriseAMar03
Topology
Tools
View
Help
2004-10-08 16:08:51

Figure 37 Complex Network Routing Topology

Selecting Nodes in a Specific Area

In some situations, your investigations might focus on a specific area of routers in the network. RAMS lets you select specific nodes on the routing topology map and analyze the details of the selected nodes.

It is a good idea to save the routing layout (see page 120) before making any changes to the layout.

To select multiple nodes individually, proceed as follows:

1. Left-click on any node on the map. A selection box is drawn around the node.
2. Add nodes to the selection by holding down the **`Ctrl`** key and left-clicking on the desired nodes. The selection box expands to contain the additional node.

To select multiple nodes by dragging a selection box, proceed as follows:

1. Position the mouse cursor at one corner of the rectangular area bounding the nodes to be selected. The cursor must not be on a node.
2. Hold the left button and drag the cursor to the diagonally opposite corner of the rectangular area so that all desired nodes are included within the bounding box you have drawn.
3. Release the left button.

After you select the desired nodes by either method, you can perform various operations on those nodes:

- You can move the selected nodes to a different position on the map. With the mouse cursor inside the bounding box, hold the left button and drag the bounding box to the new position.
- You can zoom in on the selected nodes by clicking **`Zoom In`** 🔍 on the toolbar or selecting **`Zoom In`** from the *View* menu. Figure 38 shows the result of zooming in on the lower portion of the network illustrated in Figure 37.
- You can access additional operations by right-clicking in an open space inside the bounding box area to display the Selection menu, as shown in Figure 39.

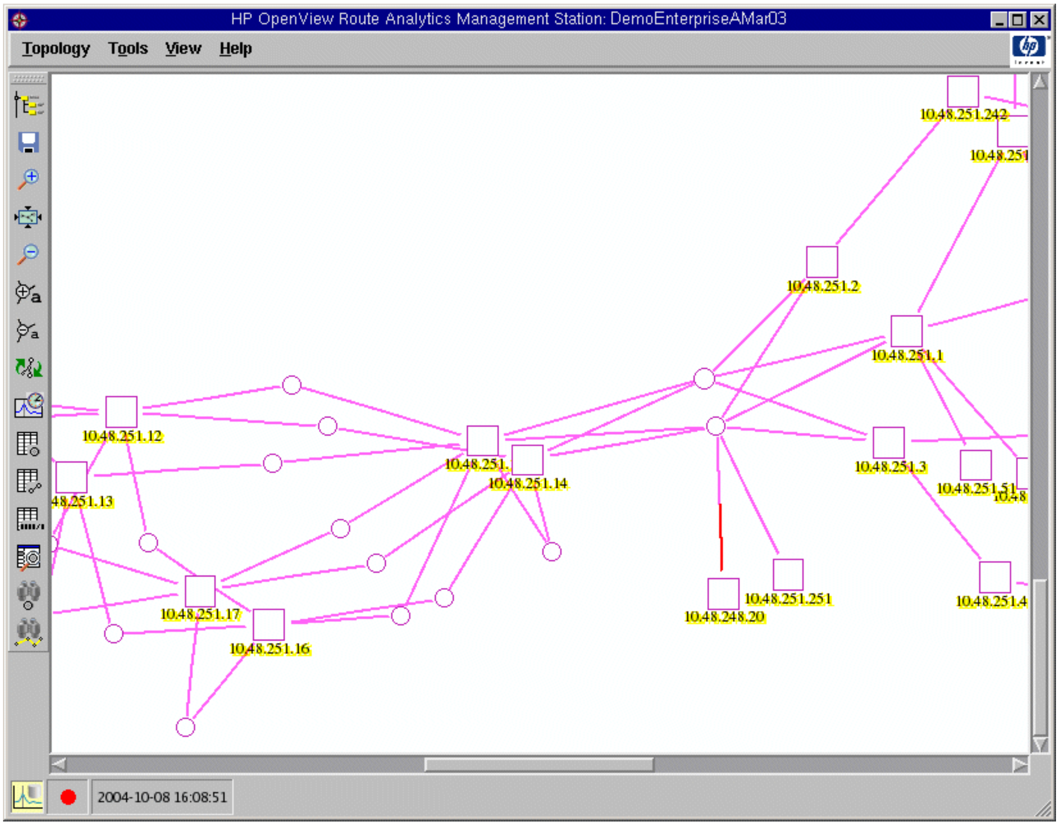
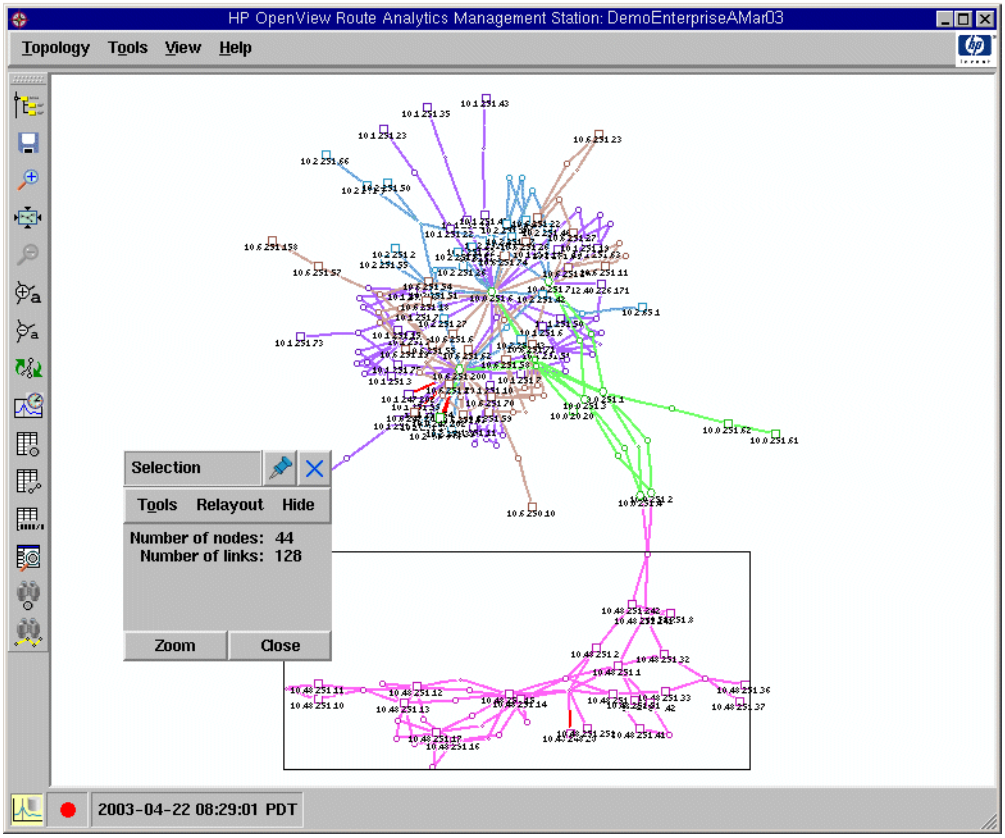


Figure 38 **Zooming in on a Portion of the Network**


HP OpenView Route Analytics Management Station: DemoEnterpriseAMar03
Topology
Tools
View
Help
Selection
Tools
Relayout
Hide
Zoom
Close

Number of nodes: 44
Number of links: 128

2003-04-22 08:29:01 PDT

Figure 39 Selection Menu and Bounding Box

Note Only the elements completely within the bounding box are included in the counts shown in the Selection menu. Each direction of a link is counted separately, since one or both halves may be inside the bounding box.

The following options are available from the Selection menu:

- **Tools** – Use this option to open a pull-down menu of commands used to list routers, links, or prefixes that are within the bounding box.
- **Relayout** – Use this option to relayout the selected nodes, or relayout the unselected nodes.

- **Hide** – Use this option to hide the nodes in the selected area, hide the nodes outside the selected area, or unhide all nodes.
- **Zoom** – Use this option to zoom in on the selected nodes.
- **Close** – Use this option to close the Selection menu.

Note If nodes were selected explicitly, only those nodes are affected by the specified action even if other nodes appear within the area of the bounding box.

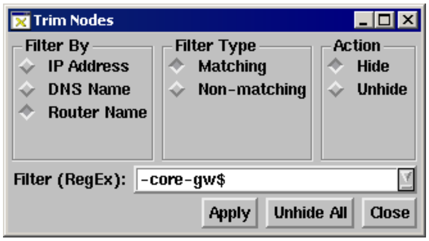
In addition, the Selection menu contains a tack button. Click the tack button to keep the menu open while you perform other operations in the Topology Map. If you do not use the tack button, the Selection menu closes as soon as you click anywhere outside the menu.

Trimming the Displayed Nodes

You can instruct RAMS to display a particular class of router on the routing topology map, based on the naming conventions established when the routers were named. If the core router names have a common text string in their name, for example the letters *core-gw*, you can use the Trim Nodes menu option to display only these routers.

To trim the displayed nodes, proceed as follows:

1 Select **`Trim Nodes`** from the View menu to open the *Trim Nodes* dialog box, as shown in Figure 40.



Filter (RegEx): -core-gw$

Figure 40 **Trim Nodes Dialog**

2 Choose among filtering by IP address, DNS name, or router name.

3 Click **`Matching`** to select routers that match the criteria of the filter or **`Non-matching`** to select routers that do not match the criteria of the filter.

4 Click **`Hide`** in the `Action` section to remove nodes from the display, or click **`Unhide`** to restore them.

5 In the **`Filter (RegEx)`** box, type in a regular expression to select the class of routers to be matched. In the example shown in Figure 40, "`-core-gw$`" matches routers whose names end with *-core-gw*. The string "`^10\.251\.`" matches addresses that begin with *10.251*. Matching is case sensitive.

6 Click **`Trim`**.

Trimming Leaves

Another useful trimming operation is leaf trimming. All routers on the edge of the network with a single link to the network are hidden from view. This operation can be repeated multiple times. Each time **Trim Leaf Nodes** is selected, edge nodes with only one link are removed.

Select **`Trim Leaf Nodes`** from the *View* menu to trim the nodes on the edge of the network. Figure 41 illustrates the result of the Trim Leaf Nodes operation performed twice in succession.

To restore hidden nodes, select **`Unhide All Nodes`** in the *View* menu.

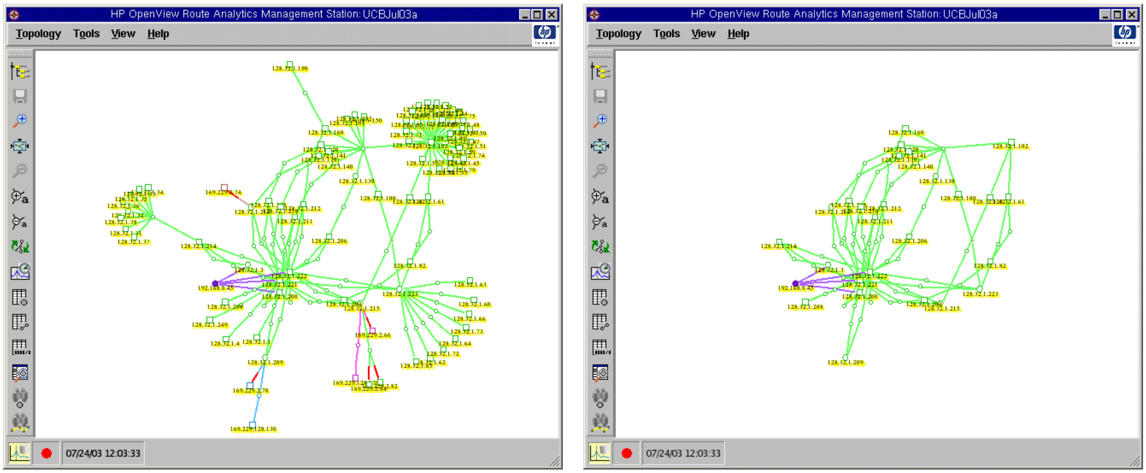

HP OpenView Route Analytics Management Station: UCBJul03a
Topology
Tools
View
Help
07/24/03 12:03:33
HP OpenView Route Analytics Management Station: UCBJul03a
Topology
Tools
View
Help
07/24/03 12:03:33

Figure 41 Trimming Leaves – Before and After

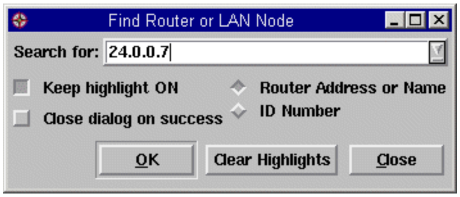
Note This operation does not trim all edge routers, since edge routers often have multiple redundant connections to the network core.

Finding a Router

When you know the name or address of a router and want to find where it is on the map, use the method described here. If you would prefer to scan the list of router names and addresses to find a router, see Router List on page 147.

To find a router using the Find Router method, proceed as follows:

1 Select **`Find Router`** from the Tools menu to open the *Find Router or LAN Node* dialog box, as shown in Figure 42.



Search for: 24.0.0.7

Figure 42 Find Router Dialog

2 In the *Search For* text box, enter the IP address, name or System ID of a router, or the prefix of a LAN pseudonode. If the name entered is the initial portion of multiple router names, then all those routers will be matched.

3 Click **`OK`**. The router flashes yellow on the routing topology map.

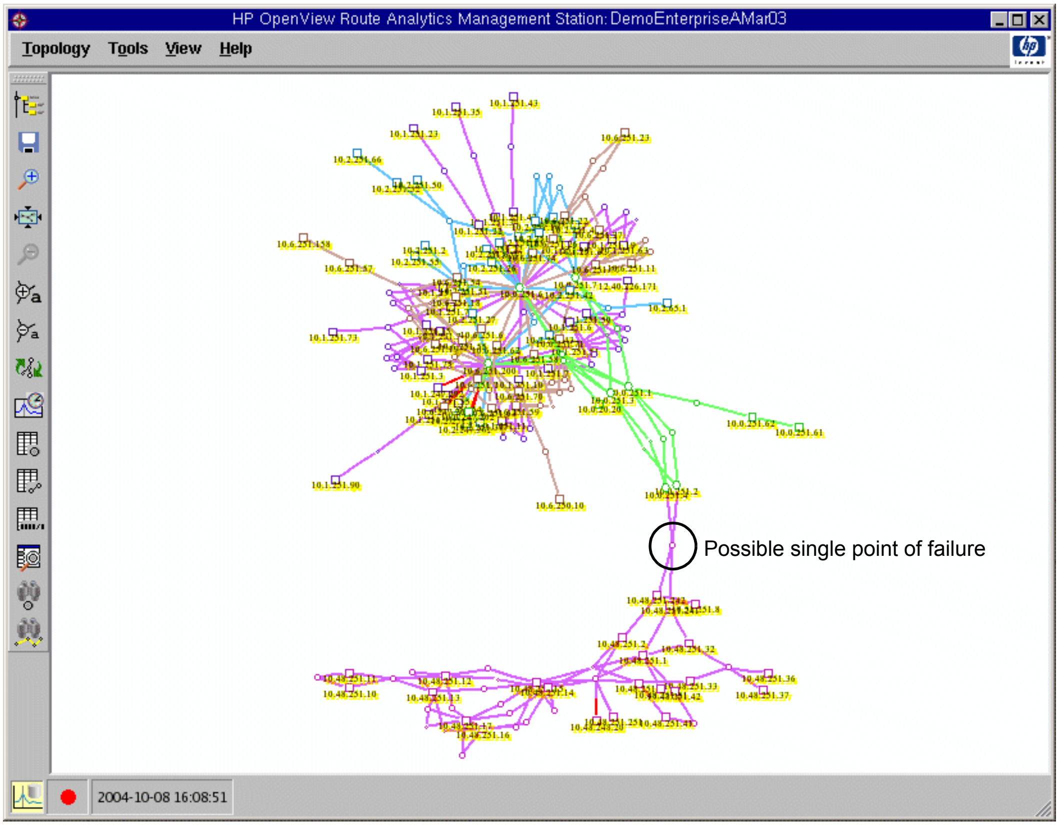
4 To highlight multiple routers at the same time, select **`Keep highlight ON`** and deselect **`Close dialog on success`**, and then repeat steps 2 and 3.

Viewing Network Anomalies At-A-Glance

RAMS's topology map enables you to quickly see possible points of failure, failed links and routers, and other anomalies. For example, when a link goes down, that link turns red on the routing topology map.

To identify network anomalies at a glance, perform the following steps:

1. Open the desired routing topology in RAMS.
2. Look for links that are shown in red. If a link is bright red, it means that the link has gone down. If it is dark red, then the link represents multiple parallel physical links only some of which are down.
3. Look for parts of the network that route through a single router (square or hexagon) or LAN (circle). Figure 43 illustrates a LAN that could be a single point of failure.



Possible single point of failure

Figure 43 Possible Single Point of Failure

Viewing a Complete Up-To-The Minute Network Inventory

RAMS can display a complete, up-to-date list of routers, links, and prefixes in each IGP area and AS of a network. You can sort these lists by prefix, AS, attributes, status, and so on, and each entry in any list can be traced back to the associated router in the topology map with a single click.

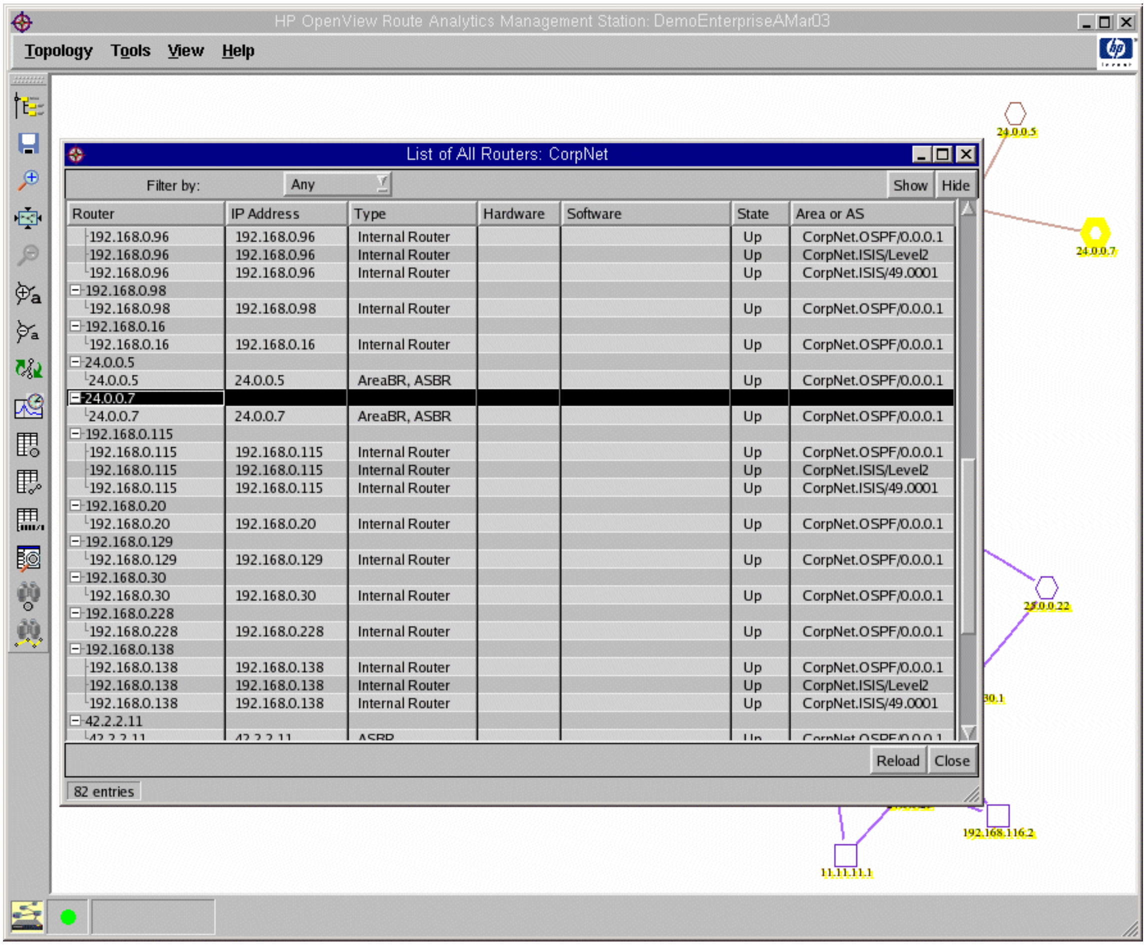
Router List

Use the Router List to do the following:

- Verify if a particular router is currently up and running.
- Verify that a router appears in the correct IGP area or AS.
- Verify that a router is configured as expected, including that the correct IP address is associated with it and that it has the correct name (for IS-IS or EIGRP).
- Display the hardware type and software version of each router (EIGRP only).
- View the total number of routers currently in the network.
- Verify the health of the network visually without sifting through hundreds of *syslog* entries.

To find a router using the List Routers method, proceed as follows:

1. Click the **`List Routers`** button ▦ on the toolbar or select **`List Routers`** on the *Tools* menu to open the *List of All Routers* window, as shown in Figure 44.


HP OpenView Route Analytics Management Station: DemoEnterpriseAMar03
Topology
Tools
View
Help
List of All Routers: CorpNet
Show
Hide
Reload
Close
24.0.0.5
24.0.0.7
25.0.0.22
30.1
192.168.116.2
11.11.11.1

Filter by: Any

Router	IP Address	Type	Hardware	Software	State	Area or AS
192.168.0.96	192.168.0.96	Internal Router			Up	CorpNet.OSPF/0.0.0.1
192.168.0.96	192.168.0.96	Internal Router			Up	CorpNet.ISIS/Level2
192.168.0.96	192.168.0.96	Internal Router			Up	CorpNet.ISIS/49.0001
192.168.0.98						
192.168.0.98	192.168.0.98	Internal Router			Up	CorpNet.OSPF/0.0.0.1
192.168.0.16						
192.168.0.16	192.168.0.16	Internal Router			Up	CorpNet.OSPF/0.0.0.1
24.0.0.5						
24.0.0.5	24.0.0.5	AreaBR, ASBR			Up	CorpNet.OSPF/0.0.0.1
24.0.0.7						
24.0.0.7	24.0.0.7	AreaBR, ASBR			Up	CorpNet.OSPF/0.0.0.1
192.168.0.115						
192.168.0.115	192.168.0.115	Internal Router			Up	CorpNet.OSPF/0.0.0.1
192.168.0.115	192.168.0.115	Internal Router			Up	CorpNet.ISIS/Level2
192.168.0.115	192.168.0.115	Internal Router			Up	CorpNet.ISIS/49.0001
192.168.0.20						
192.168.0.20	192.168.0.20	Internal Router			Up	CorpNet.OSPF/0.0.0.1
192.168.0.129						
192.168.0.129	192.168.0.129	Internal Router			Up	CorpNet.OSPF/0.0.0.1
192.168.0.30						
192.168.0.30	192.168.0.30	Internal Router			Up	CorpNet.OSPF/0.0.0.1
192.168.0.228						
192.168.0.228	192.168.0.228	Internal Router			Up	CorpNet.OSPF/0.0.0.1
192.168.0.138						
192.168.0.138	192.168.0.138	Internal Router			Up	CorpNet.OSPF/0.0.0.1
192.168.0.138	192.168.0.138	Internal Router			Up	CorpNet.ISIS/Level2
192.168.0.138	192.168.0.138	Internal Router			Up	CorpNet.ISIS/49.0001
42.2.2.11						
42.2.2.11	42.2.2.11	ASBR			Up	CorpNet.OSPF/0.0.0.1

82 entries

Figure 44 Locating a Router using the List of Routers

2. Use the **Filter by** drop-down list at the top of the window to filter the routers displayed in the window (see Using Filters on page 226).

3. Scroll down the list to find the desired router.

4. To identify where a particular router is on the map, click anywhere on that router's row. The row is highlighted in the *List of All Routers* window and the router flashes yellow on the routing topology map, as shown in Figure 44.

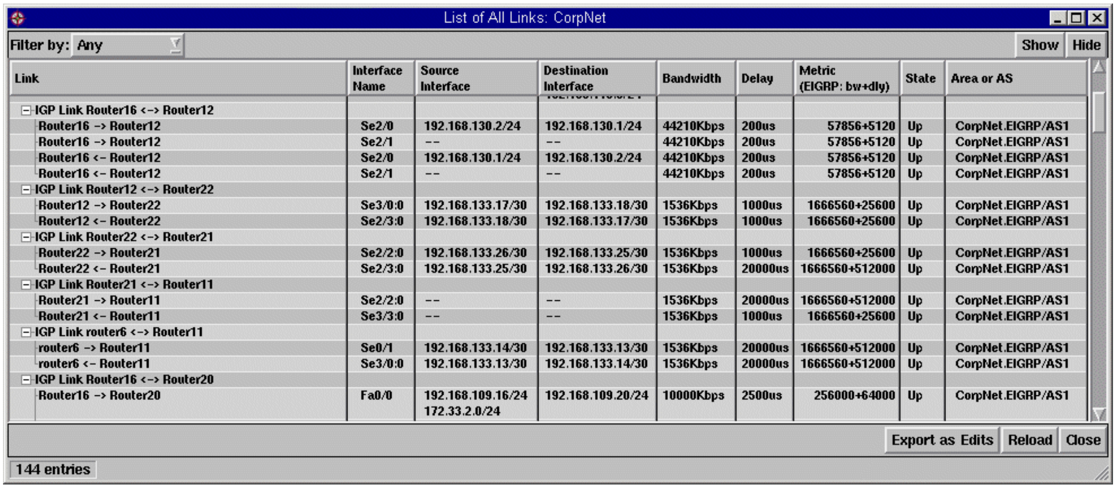
Links List

The Links List displays the number and current state (Up or Down) of all routing adjacencies in the network, along with their link metrics and the router interface addresses.

To view the Links List, perform the following steps:

1 Click the **`List Links`** button on the toolbar or select **`List Links`** from the *Tools* menu.

The *List of All Links* window opens, as shown in Figure 45.



List of All Links: CorpNet

Filter by: Any

Link	Interface Name	Source Interface	Destination Interface	Bandwidth	Delay	Metric (EIGRP: bw+dly)	State	Area or AS
⊟ IGP Link Router16 <-> Router12								
Router16 -> Router12	Se2/0	192.168.130.2/24	192.168.130.1/24	44210Kbps	200us	57856+5120	Up	CorpNet.EIGRP/AS1
Router16 -> Router12	Se2/1	--	--	44210Kbps	200us	57856+5120	Up	CorpNet.EIGRP/AS1
Router16 <- Router12	Se2/0	192.168.130.1/24	192.168.130.2/24	44210Kbps	200us	57856+5120	Up	CorpNet.EIGRP/AS1
Router16 <- Router12	Se2/1	--	--	44210Kbps	200us	57856+5120	Up	CorpNet.EIGRP/AS1
⊟ IGP Link Router12 <-> Router22								
Router12 -> Router22	Se3/0:0	192.168.133.17/30	192.168.133.18/30	1536Kbps	1000us	1666560+25600	Up	CorpNet.EIGRP/AS1
Router12 <- Router22	Se2/3:0	192.168.133.18/30	192.168.133.17/30	1536Kbps	1000us	1666560+25600	Up	CorpNet.EIGRP/AS1
⊟ IGP Link Router22 <-> Router21								
Router22 -> Router21	Se2/2:0	192.168.133.26/30	192.168.133.25/30	1536Kbps	1000us	1666560+25600	Up	CorpNet.EIGRP/AS1
Router22 <- Router21	Se2/3:0	192.168.133.25/30	192.168.133.26/30	1536Kbps	20000us	1666560+512000	Up	CorpNet.EIGRP/AS1
⊟ IGP Link Router21 <-> Router11								
Router21 -> Router11	Se2/2:0	--	--	1536Kbps	20000us	1666560+512000	Up	CorpNet.EIGRP/AS1
Router21 <- Router11	Se3/3:0	--	--	1536Kbps	1000us	1666560+25600	Up	CorpNet.EIGRP/AS1
⊟ IGP Link router6 <-> Router11								
router6 -> Router11	Se0/1	192.168.133.14/30	192.168.133.13/30	1536Kbps	20000us	1666560+512000	Up	CorpNet.EIGRP/AS1
router6 <- Router11	Se3/0:0	192.168.133.13/30	192.168.133.14/30	1536Kbps	20000us	1666560+512000	Up	CorpNet.EIGRP/AS1
⊟ IGP Link Router16 <-> Router20								
Router16 -> Router20	Fa0/0	192.168.109.16/24 172.33.2.0/24	192.168.109.20/24	10000Kbps	2500us	256000+64000	Up	CorpNet.EIGRP/AS1

144 entries

Figure 45 List of All Links Window

2 Use the **`Filter by`** drop-down list at the top of the window to filter the links displayed in the window (see Using Filters on page 226).

3 The following additional operations can be performed in this dialog:

- Select a link in the list, which causes the link to flash yellow on the map.
- Copy a single row of the table using **`Ctrl-C`** or the entire table using **`Ctrl-A`**. The data is copied to the clipboard, from which you can paste it into a text file. This operation captures all of the data from one or more rows.

- Export the table by clicking the **`Export as Edits`** button. This operation copies to the clipboard a subset of the data in each row, and does so in the format required for import in the *Router/Link Edits* dialog. See Exporting and Importing Router/Link Edits on page 164 for more information on exported edits.
- If the routing topology has changed since the dialog was opened, refresh the contents of the dialog by clicking **`Reload`**.
- Close the dialog by clicking **`Close`**.

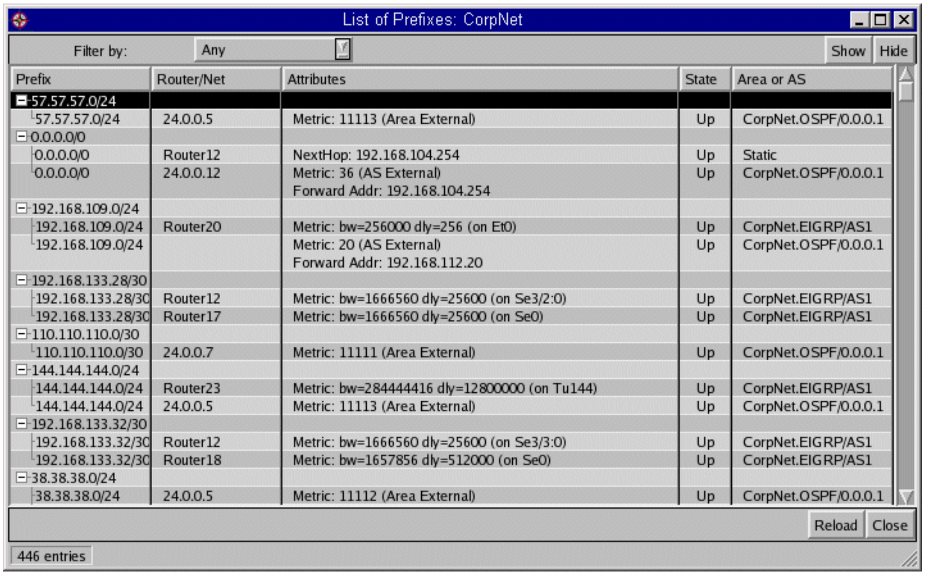
Prefix List

Use the Prefix List to do the following:

- View the routers in a network that are advertising default routes.
- Determine if a prefix is currently advertised or not, and by which routers.
- See what metric is advertised with each prefix.
- Verify that area border routers are properly advertising prefixes.
- Display the advertised BGP prefixes and the list of attributes associated with each BGP prefix.

To view the Prefix List, perform the following steps:

1 Click the **`List Prefixes`** button ▦ on the toolbar or select **`List Prefixes`** from the *Tools* menu to open the *List of Prefixes* window (shown in Figure 46).



Filter by: Any

Prefix	Router/Net	Attributes	State	Area or AS
⊟57.57.57.0/24				
57.57.57.0/24	24.0.0.5	Metric: 11113 (Area External)	Up	CorpNet.OSPF/0.0.0.1
⊟0.0.0.0/0				
0.0.0.0/0	Router12	NextHop: 192.168.104.254	Up	Static
0.0.0.0/0	24.0.0.12	Metric: 36 (AS External) Forward Addr: 192.168.104.254	Up	CorpNet.OSPF/0.0.0.1
⊟192.168.109.0/24				
192.168.109.0/24	Router20	Metric: bw=256000 dly=256 (on Et0)	Up	CorpNet.EIGRP/AS1
192.168.109.0/24		Metric: 20 (AS External) Forward Addr: 192.168.112.20	Up	CorpNet.OSPF/0.0.0.1
⊟192.168.133.28/30				
192.168.133.28/30	Router12	Metric: bw=1666560 dly=25600 (on Se3/2:0)	Up	CorpNet.EIGRP/AS1
192.168.133.28/30	Router17	Metric: bw=1666560 dly=25600 (on Se0)	Up	CorpNet.EIGRP/AS1
⊟110.110.110.0/30				
110.110.110.0/30	24.0.0.7	Metric: 11111 (Area External)	Up	CorpNet.OSPF/0.0.0.1
⊟144.144.144.0/24				
144.144.144.0/24	Router23	Metric: bw=284444416 dly=12800000 (on Tu144)	Up	CorpNet.EIGRP/AS1
144.144.144.0/24	24.0.0.5	Metric: 11113 (Area External)	Up	CorpNet.OSPF/0.0.0.1
⊟192.168.133.32/30				
192.168.133.32/30	Router12	Metric: bw=1666560 dly=25600 (on Se3/3:0)	Up	CorpNet.EIGRP/AS1
192.168.133.32/30	Router18	Metric: bw=1657856 dly=512000 (on Se0)	Up	CorpNet.EIGRP/AS1
⊟38.38.38.0/24				
38.38.38.0/24	24.0.0.5	Metric: 11112 (Area External)	Up	CorpNet.OSPF/0.0.0.1

446 entries

Figure 46 **List of Prefixes Window**

2 Use the **`Filter by`** drop-down list at the top of the window to filter the prefixes displayed in the window (see Using Filters on page 226).

3 The following additional operations can be performed in this dialog:

- Select a router in the list, and the node will flash yellow on the map.
- If the routing topology has changed since the dialog was opened, refresh the contents of the dialog by clicking **`Reload`**.
- Close the dialog by clicking **`Close`**.

To list prefixes for a node, perform the following steps:

1 Locate the router on the map.

2 Right-click on the node to open the node information panel.

3 Click **`Prefixes`**.

The *Prefix List* opens showing all prefixes advertised by the node you selected. For each prefix, all nodes that advertise the prefix are listed.

Note

The names and addresses in the *Router/Net* column are the routers that are advertising the prefix. The way that the routers are displayed depends on which protocol is in use. In OSPF, the pseudonode advertises the prefix of a LAN. In IS-IS, the designated router advertises the prefix of a LAN. For a point-to-point link there is no pseudonode, so both routers advertise the prefix. An EIGRP network does not have pseudonodes, so all prefixes are advertised by routers.

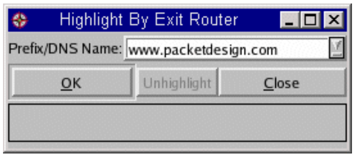
Viewing the Exit Routers from the Network for any Internet Destination

In a large network with multiple exit routers to the Internet, it is often useful to see which exits are being taken from various points in the network. This information can help you to infer the flow of traffic to service providers or peers, helping you to balance those flows to achieve optimum performance or minimize monthly cost in transit fees and bandwidth costs.

RAMS can calculate the IGP path from each router to its nearest exit router if there is a default route or if external routes are redistributed from BGP. Each router is then color-coded by exit router and exit routers are highlighted in flashing yellow. Alternatively, to highlight the path from a single router to its exit router, see Finding a Route By Prefix on page 158.

To view the exit routers from all routers in the network, perform the following steps:

1. Select **`Highlight by Exit Router`** from the *Tools* menu.
2. Enter the desired Internet prefix or domain name in the *Highlight By Exit Router* dialog (shown in Figure 47).
3. Click **`OK`**.



Prefix/DNS Name: www.packetdesign.com

Figure 47 Highlight by Exit Router Dialog

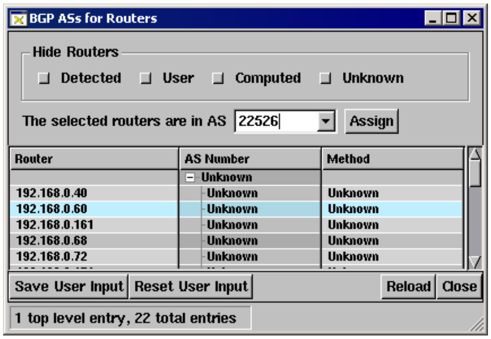
Verify and Manually Assign BGP AS Assignments to Routers

RAMS can display the path resolved between two points in a network, as described in the next section. For network configurations that include BGP, RAMS requires correct BGP AS assignments to routers to accurately resolve the path. For a BGP confederation topology, it is not always possible to automatically determine the correct assignment for all routers. For network configurations that include BGP without confederations, RAMS can create BGP AS assignments for all routers automatically, but some routers may not be running BGP. For these cases, you can change the BGP AS assignment manually in the *BGP ASs for Routers* dialog.

If one or more routers do not belong in a BGP AS, you can select *No BGP* in **`The selected routers are in AS`** drop-down list. By specifying routers as not belonging to a BGP AS, RAMS can calculate IP routes across the topology more accurately. This may be needed in topologies without BGP confederations when only some routers run BGP and others follow a static default route.

To verify and manually assign AS assignments to routers, perform the following steps:

1. On the **Tools** menu, click **Assign BGP ASs to Routers** to open the *BGP ASs for Routers* dialog as shown in Figure 48. Some routers may have AS numbers already assigned to them as detected by BGP peering or computed from network topology.



□ Detected □ User □ Computed □ Unknown

The selected routers are in AS 22526

Router	AS Number	Method
	⊟ Unknown	
192.168.0.40	Unknown	Unknown
192.168.0.60	Unknown	Unknown
192.168.0.161	Unknown	Unknown
192.168.0.68	Unknown	Unknown
192.168.0.72	Unknown	Unknown

1 top level entry, 22 total entries

Figure 48 **BGP ASs to Routers dialog box**

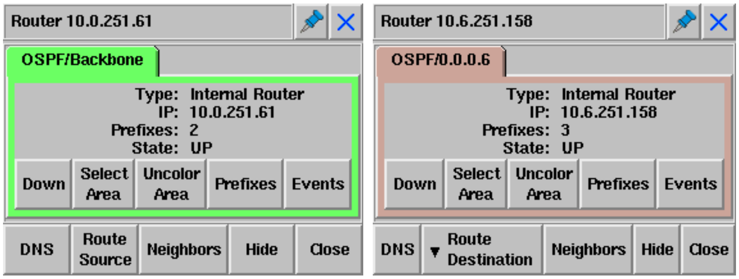
2. Click a router in the Router list. You can also select multiple routers or a range of routers by holding down the Ctrl or Shift key when you click another router in the list. Routers for which an assignment was *Detected* cannot be reassigned.
3. Select the appropriate AS or *No BGP* in the **`The selected routers are in AS`** drop-down list. Select *No BGP* if, for example, the router is not running BGP and is following a default route.
4. Click **Assign**.
5. Repeat Steps 2-4 to manually assign other routers.
6. Click **Save User Input**.
7. Click **Close**.

Highlighting the IP Route Between Two Points in the Network

Seeing the IP paths taken by traffic from a source router to a destination router in a multidomain network is very useful for network planning. There can be paths of high importance in a network such as a VoIP service path between an IP PBX and a PSTN media gateway that would not tolerate significantly increased delay resulting from a possible rerouting due to link or router failures.

RAMS can quickly display the path resolved between two nodes in a network at the current time or at any point in recorded topology history. The path is highlighted in yellow (or orange if the path is not complete). Each segment of the path can be listed, along with the link metric and the prefix by which each next hop was resolved, using the *List/Find Paths* dialog described in Finding a Route By Prefix on page 158.

The path is selected using the information panels for the source and destination nodes on the routing topology map. Figure 49 shows the node information panels for the source and destination of a route.



Router 10.0.251.61

OSPF/Backbone

Type: Internal Router
IP: 10.0.251.61
Prefixes: 2
State: UP

Router 10.6.251.158

OSPF/0.0.0.6

Type: Internal Router
IP: 10.6.251.158
Prefixes: 3
State: UP

Figure 49 Source and Destination Node Information Panels

To view the path between two routers, perform the following steps:

1 Right-click on the source node on the routing topology map.

The node information panel appears.

2 Click **`Route Source`**.

3 Right-click on the destination node on the routing topology map.

4 Click **`Route Destination`** in the node information panel that appears, and then select an interface from the drop-down list.

The route between the selected routers is highlighted in yellow on the routing topology map, as shown in Figure 51.

5 To see the path details, select from the toolbar or **`List/Find Paths`** from the *Tools* menu.

The *List/Find Paths* dialog displays the segments of the path as shown in Figure 50.

Note The route may not be complete between the two points if the destination address falls within a prefix that is not routable in the topology known to the RAMS, or if the address resolves to a summary prefix such as the default route. Consequently, the route from point B to point A might be incomplete even if the route from point A to point B is complete.

Finding a Route By Prefix

In addition to finding paths between pairs of nodes on the routing topology map, RAMS can also find the route from a router to any prefix internal or external to the network for which a route exists.

To find a route using a prefix, proceed as follows:

1 Open the *Tools* menu and select **`List/Find Paths`**.

The *List/Find Paths* dialog opens, as shown in Figure 50.

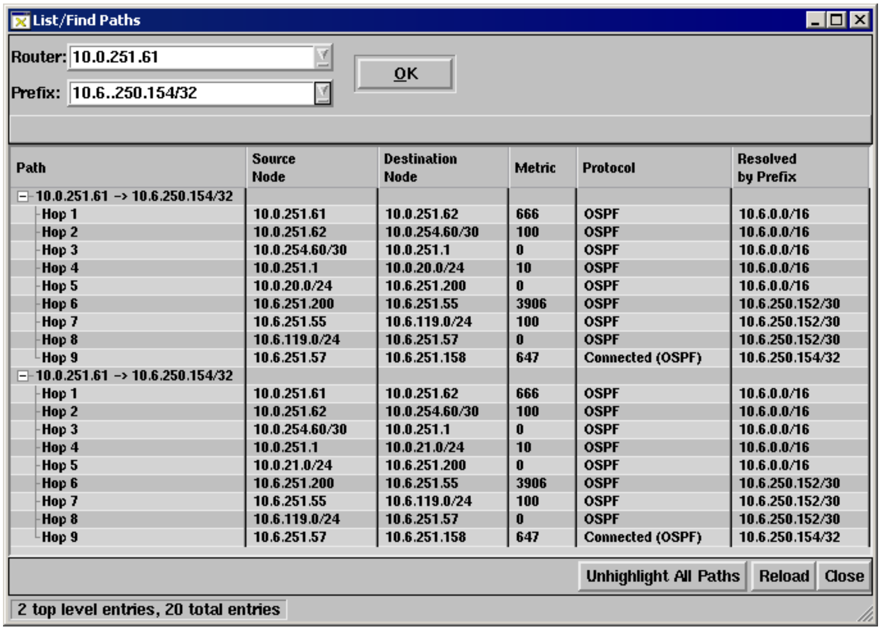
2 Enter the source router's IP address or name in the *Router* field.

3 Enter the destination IP address, Internet prefix or domain name in the *Prefix* field.

4 Click **`OK`**.

The route is calculated to the destination prefix if internal or to the nearest exit router if external. The segments of the path are displayed in the lower section of the *List/Find Paths* dialog, including the link metric and the prefix by which each next hop was resolved. The path is highlighted on the routing topology map in yellow if the route is complete, as shown in Figure 51, or orange if the route is incomplete. Multiple paths are shown for equal-cost multi-path routes.

Note If you enter a destination prefix that does not exist in the network, the route might go to the default router and the default router might forward the route to a router outside the topology. In that case, the path might end at a LAN pseudonode.



Router: 10.0.251.61

Prefix: 10.6..250.154/32

Path	Source Node	Destination Node	Metric	Protocol	Resolved by Prefix
⊟ 10.0.251.61 -> 10.6.250.154/32					
Hop 1	10.0.251.61	10.0.251.62	666	OSPF	10.6.0.0/16
Hop 2	10.0.251.62	10.0.254.60/30	100	OSPF	10.6.0.0/16
Hop 3	10.0.254.60/30	10.0.251.1	0	OSPF	10.6.0.0/16
Hop 4	10.0.251.1	10.0.20.0/24	10	OSPF	10.6.0.0/16
Hop 5	10.0.20.0/24	10.6.251.200	0	OSPF	10.6.0.0/16
Hop 6	10.6.251.200	10.6.251.55	3906	OSPF	10.6.250.152/30
Hop 7	10.6.251.55	10.6.119.0/24	100	OSPF	10.6.250.152/30
Hop 8	10.6.119.0/24	10.6.251.57	0	OSPF	10.6.250.152/30
Hop 9	10.6.251.57	10.6.251.158	647	Connected (OSPF)	10.6.250.154/32
⊟ 10.0.251.61 -> 10.6.250.154/32					
Hop 1	10.0.251.61	10.0.251.62	666	OSPF	10.6.0.0/16
Hop 2	10.0.251.62	10.0.254.60/30	100	OSPF	10.6.0.0/16
Hop 3	10.0.254.60/30	10.0.251.1	0	OSPF	10.6.0.0/16
Hop 4	10.0.251.1	10.0.21.0/24	10	OSPF	10.6.0.0/16
Hop 5	10.0.21.0/24	10.6.251.200	0	OSPF	10.6.0.0/16
Hop 6	10.6.251.200	10.6.251.55	3906	OSPF	10.6.250.152/30
Hop 7	10.6.251.55	10.6.119.0/24	100	OSPF	10.6.250.152/30
Hop 8	10.6.119.0/24	10.6.251.57	0	OSPF	10.6.250.152/30
Hop 9	10.6.251.57	10.6.251.158	647	Connected (OSPF)	10.6.250.154/32

2 top level entries, 20 total entries

Figure 50 List/Find Path Dialog

Simulating Router/Link Failures and Metric Changes

After highlighting a route, you can simulate the effects that link failures or metric changes would have on the highlighted route.

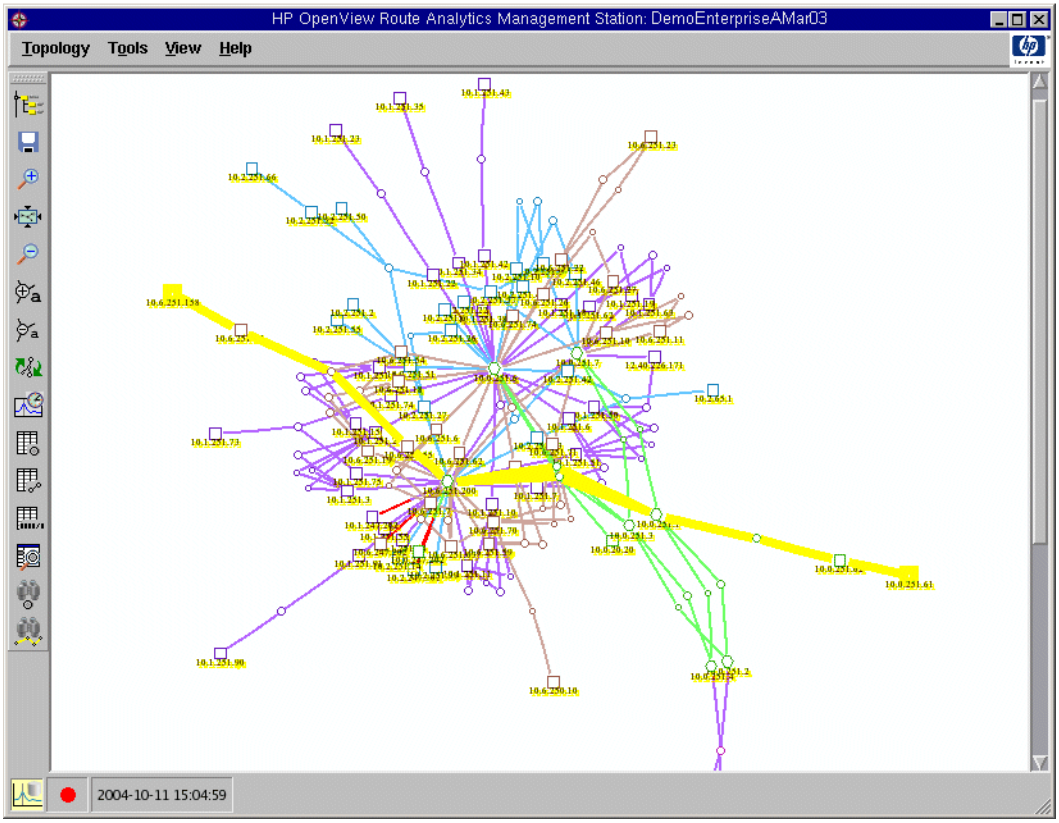


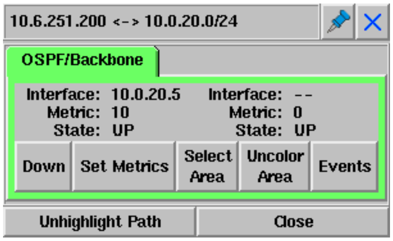
Figure 51 Highlighted Route

To simulate a down link, perform the following steps:

1 Right-click on a link in the path.

The link information panel appears (see Figure 52).

2 Click **Down**. The link goes down and turns red. The highlighted path is rerouted around the down link if another route is available.



10.6.251.200 <-> 10.0.20.0/24

OSPF/Backbone

Interface: 10.0.20.5 Interface: --
Metric: 10 Metric: 0
State: UP State: UP

Figure 52 Link Information Panel

3 To bring the link back up, right-click on the link and click **Up** in the link information panel.

> **Note** The **Down** button is only enabled in History mode. If the database is currently recording data and the *Online Update Monitor* is open, the **Down** button is disabled.

To simulate a metric change, perform the following steps:

1 Right-click on a link.

2 Click **Set Metric** in the link information panel to open the *Set Metric* dialog

3 Enter a metric in the *Set Metric* dialog.

4 Click **Set**.

> **Note** The **Set Metric** button is only enabled in History mode. If the database is currently recording data and the *Online Update Monitor* is open, the **Set Metric** button is disabled.

To simulate a down router, perform the following steps:

1 Right-click on a router.

2 Click **Down** in the *Router* dialog that appears.

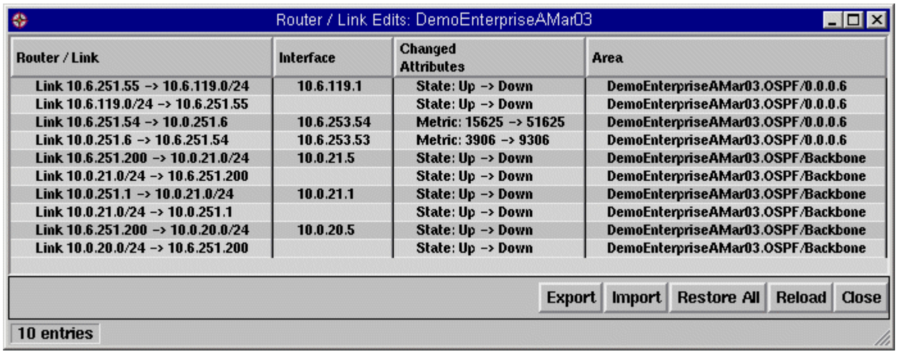
3 To bring the router back up, right-click on the router and click **Up** in the *Router* dialog.

Note The **Down** button is only enabled in History mode. If the database is currently recording data and the *Online Update Monitor* is open, the **Down** button is disabled.

To view all link and router changes, perform the following steps:

1. From the Tools menu, select **`List Router/Link Edits`** to open the *Router/Link Edits* window, which displays all of the changes made, as shown in Figure 53.
2. Click **`Restore All`** in the *Router/Link Edits* window to restore all the edits at once.

Note In the attributes column of the *Router/Link Edits* window, the state of an object may be listed as *Up -> Up*. This occurs because the table keeps track of all objects that have been edited until those edits are restored, either singly by right-clicking on the edit, or globally by clicking the **`Restore All`** button, or by moving to a different time. Thus, if you edit an object from *Up* to *Down*, then back again, it is listed as *Up -> Up* until you restore the edits or move to a different time.



Router / Link Edits: DemoEnterpriseAMar03

Router / Link	Interface	Changed Attributes	Area
Link 10.6.251.55 -> 10.6.119.0/24	10.6.119.1	State: Up -> Down	DemoEnterpriseAMar03.OSPF/0.0.0.6
Link 10.6.119.0/24 -> 10.6.251.55		State: Up -> Down	DemoEnterpriseAMar03.OSPF/0.0.0.6
Link 10.6.251.54 -> 10.0.251.6	10.6.253.54	Metric: 15625 -> 51625	DemoEnterpriseAMar03.OSPF/0.0.0.6
Link 10.0.251.6 -> 10.6.251.54	10.6.253.53	Metric: 3906 -> 9306	DemoEnterpriseAMar03.OSPF/0.0.0.6
Link 10.6.251.200 -> 10.0.21.0/24	10.0.21.5	State: Up -> Down	DemoEnterpriseAMar03.OSPF/Backbone
Link 10.0.21.0/24 -> 10.6.251.200		State: Up -> Down	DemoEnterpriseAMar03.OSPF/Backbone
Link 10.0.251.1 -> 10.0.21.0/24	10.0.21.1	State: Up -> Down	DemoEnterpriseAMar03.OSPF/Backbone
Link 10.0.21.0/24 -> 10.0.251.1		State: Up -> Down	DemoEnterpriseAMar03.OSPF/Backbone
Link 10.6.251.200 -> 10.0.20.0/24	10.0.20.5	State: Up -> Down	DemoEnterpriseAMar03.OSPF/Backbone
Link 10.0.20.0/24 -> 10.6.251.200		State: Up -> Down	DemoEnterpriseAMar03.OSPF/Backbone

10 entries

Figure 53 Route/Link Edits Window

With the edits shown in Figure 53 applied to the network shown in Figure 51, the highlighted path changes as shown in Figure 54.

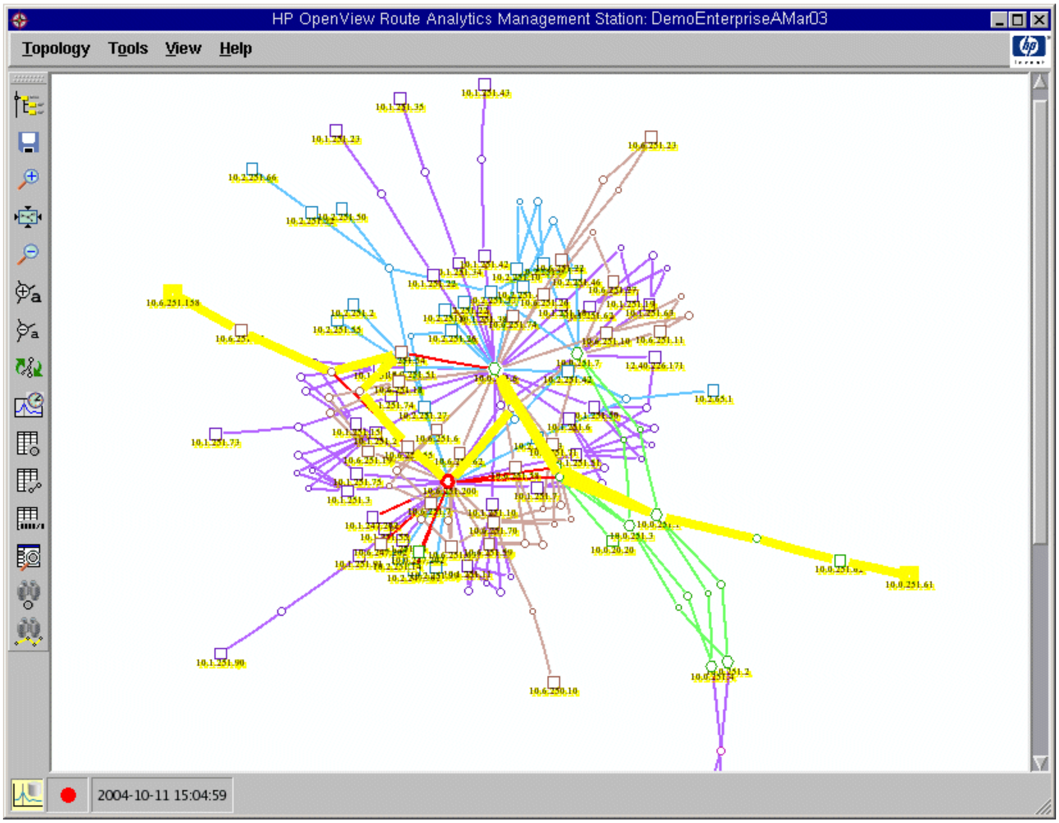


Figure 54 Highlighted Route After Edits

When a simulated change is made to the state or metric of a link in one area, that change is propagated across area boundaries within one protocol domain.

However, RAMS does not support simulation of route redistribution for *what-if* edits, so the change is not propagated across AS boundaries from one protocol to another, such as between OSPF and EIGRP. As a result, a simulated route starting in an AS other the one where the edit is made and ending at a prefix affected by the edit may not be routed correctly.

Exporting and Importing Router/Link Edits

The procedures described above let you perform simple what-if simulations. For more comprehensive simulations, the *Router/Link Edits* window provides tools to export the table in plain text format so that you can make changes to the table, import it, and then view the results of the simulation.

What-if edits are exported and imported using copy and paste operations on the *Router/Link Edits* window. The whole table can be exported with the **Export** button or by typing **Ctrl-A**. A single edit can be exported with **Ctrl-C**. As for the copy operation on other tables, the output is prepared for three selection mechanisms:

- CUTBUFFER 0, which is stored by the X server and which the VNC server passes to the VNC viewer for forwarding to the host window system's selection mechanism.
- The CLIPBOARD selection, which X running on Windows will pass to the Windows clipboard, or to **Ctrl-V** paste in Mozilla on Unix or Linux systems.
- The PRIMARY selection, which will be fetched by traditional X applications on a Button-2 paste or **Ctrl-Y** in emacs.

Unlike other tables, the copy function does not show the information literally as it appears in the table. Instead, it is formatted into an external table format suitable for a person to interpret and manipulate in a spreadsheet. Each row in the table is a separate edit, where the columns specify the parameters of the edit. The table format includes a header line in one of the following forms to give meaning to the columns:

```
Source      Destination     Interface         BW        Delay     Area or AS
Router16    Router20        92.168.109.17     10000     500       Lab58.Left.EIGRP/AS1
```

```
Source            Destination          Interface         Metric    Area
192.168.107.7     192.168.103.0/24     192.168.103.7     555       CorpNet.OSPF/0.0.0.1
```

The *Area or AS* column may not be present if there is only one area. The columns are separated by tabs (but in these examples the tabs have been converted to spaces for display). New edits can be created manually following this format using a spreadsheet or other tools if desired. In addition, the **Export as Edits** button on the *List Links* dialog will prepare and copy a table in the format described above to represent the current state of all links. This output can be modified in a spreadsheet and then imported for what-if analysis.

The **Import** button on the *Router/Link Edits* dialog imports a table of edits from one of the three selection sources, trying in order a PRIMARY selection, then CLIPBOARD, then CUTBUFFER 0. The input is assumed to be in CSV (comma-separated value) format. This is the format produced by a copy operation from a spreadsheet program, for example.

The input may include one or more header lines as described above, which may be interspersed with data lines. The order and presence of columns (except for *Source* and *Destination*) in the input is controlled by the header keywords (which are case insensitive). If the number of columns present in the data lines following one of these header lines is the same as the number of columns in the header line, then the order and presence of the columns will be assumed to be the same. The order or presence of columns may be changed part way through the input by including another header line.

If there are no header lines, then the order of the columns is assumed as shown, but the format of the data is used to determine if the *Interface*, *BW*, and *Area or AS* columns are present. Note that the interface must be specified for a link that has more than one interface (i.e., parallel physical links), and the area or AS must be specified if the loaded topology includes more than one. *BW* is specified only for EIGRP, but all protocols must include a *Delay* or *Metric* column to specify metric value for metric edits, or the keywords *DOWN* or *UP* (case insensitive) for state changes. For EIGRP, the *BW* value is in Kbps and the delay value is in microseconds. For other protocols, the metric value is dimensionless.

The *Interface* field may be an interface name or an interface address. At this time, interface names are only known for EIGRP. The first character of the interface name will be folded to uppercase, so et0 is acceptable in place of Et0, but at0 is not acceptable if the router uses AT0.

The label portion of the *Area or AS* name (i.e., the Administrative Domain name) must have character case matching what is in the database. The protocol name can be in any case. For EIGRP, the AS number after the slash is acceptable either with or without the prefix *AS*. For OSPF, the area ID is acceptable in either dotted decimal or 8-character uppercase hexadecimal forms.

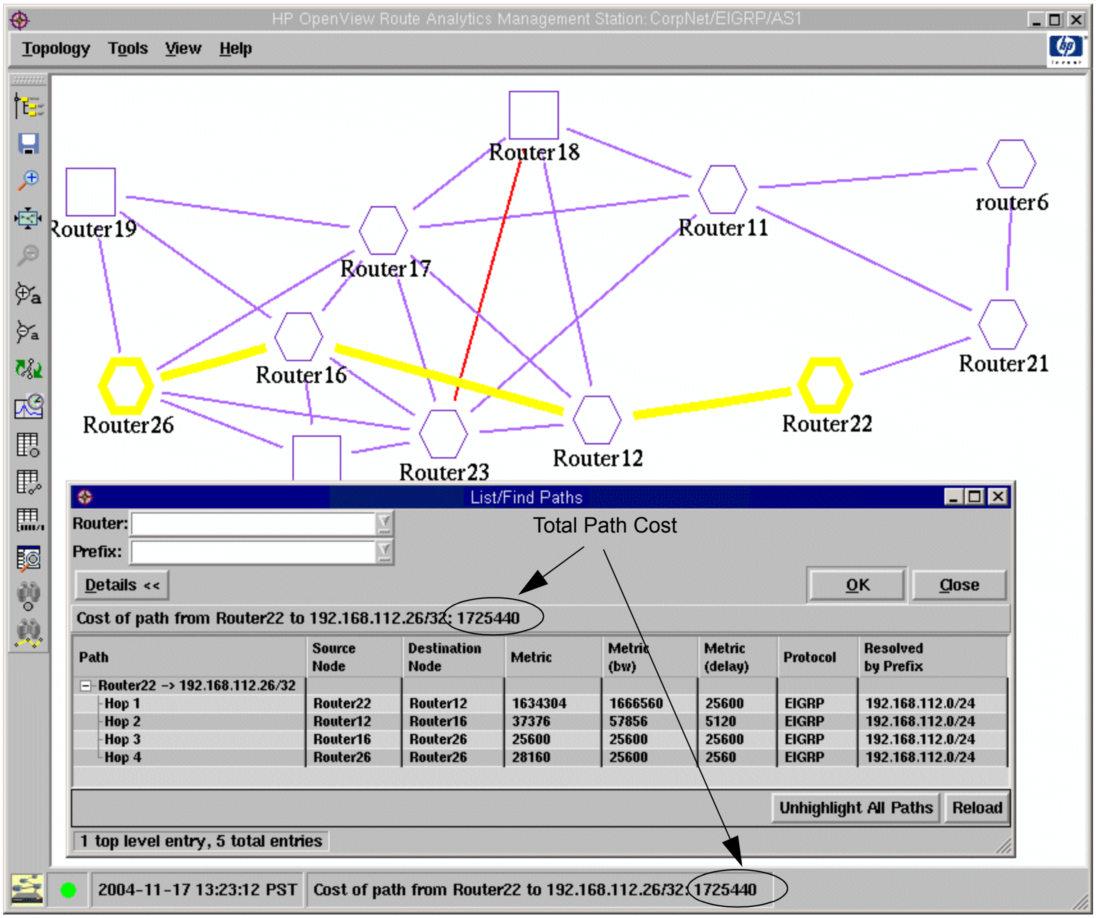
Columns with no value for a particular row may be empty or contain "--". For example, the *Destination* column has no value for a router *DOWN* edit.

Highlighted Path Cost for EIGRP

To view the details of a highlighted path, select **`List/Find Paths`** from the *Tools* menu. An example for the EIGRP protocol is shown in Figure 55.

The resulting *List/Find Paths* dialog displays, for each link along the path, the source and destination nodes of the link, the metric cost of the link, the protocol used by multiprotocol routing to select that link, and the prefix used to resolve that hop.

The *Metric (bw)* and *Metric (delay)* columns for EIGRP show the cost in EIGRP metric units associated with the bandwidth and delay values that are configured for the link. The *Metric* column is not as obvious; it lists the amount that each link contributes to the overall path distance, or cost. The path cost for EIGRP is the sum of the *delay* values for each hop plus the maximum of the *bw* values (which would be the lowest bandwidth link since the bw values correspond to the inverse of the link bandwidth).



Total Path Cost

Cost of path from Router22 to 192.168.112.26/32: 1725440

Path	Source Node	Destination Node	Metric	Metric (bw)	Metric (delay)	Protocol	Resolved by Prefix
⊟ Router22 -> 192.168.112.26/32							
Hop 1	Router22	Router12	1634304	1666560	25600	EIGRP	192.168.112.0/24
Hop 2	Router12	Router16	37376	57856	5120	EIGRP	192.168.112.0/24
Hop 3	Router16	Router26	25600	25600	25600	EIGRP	192.168.112.0/24
Hop 4	Router26	Router26	28160	25600	2560	EIGRP	192.168.112.0/24

1 top level entry, 5 total entries

2004-11-17 13:23:12 PST

Cost of path from Router22 to 192.168.112.26/32: 1725440

Figure 55 Highlighted Path Details for EIGRP

Since the EIGRP protocol calculates routes from the destination back towards the source, the *Metric* column needs to be read from bottom to top. In Figure 55, hop 4 contributes both the *bw* and *delay* values to the total cost of 28160. At hop 3 the maximum *bw* value is unchanged, so hop 3 increases the total cost only by its *delay* value 25600. Hop 2 adds the amount by which its *bw* value is larger than the current maximum of the *bw* values (57856-25600) plus its *delay* value 5120, for a total of 37376. At hop 1, the maximum *bw* value increases again (1666560–57856) and a *delay* of 25600 is added. If all the values in the *Metric* column are added, the total path cost is the same as is reported in the *List/Find Paths* dialog and in the status bar of the *Routing Topology* window.

In a multiprotocol network, it is not always possible to calculate the total path cost because the metrics of different protocols are of different magnitudes and are therefore meaningless to add. In such cases, the status line indicates that the path cost cannot be calculated.

Configuration Options Dialog

Selecting **`Options`** on the *Tools* menu opens the RAMS *Configuration Options* dialog, where you can set preferences for various parameters of RAMS operation. The dialog contains a hierarchical list of option categories. Select a category to display the options in that category in the right pane of the dialog.

To close the dialog and save any changes you have made, click the **`Close`** button at the bottom of the dialog. To restore all options to their factory default values, click the **`Factory Settings`** button at the bottom of the dialog.

Analysis Options

There are two subcategories of analysis options. The first lets you customize the level of detail that is displayed in visualizations and animations of the BGP RIB, and the second lets you set the thresholds used in Root Cause Analysis. In each case, a higher value decreases the level of detail, and a lower value increases it.

- Visualization options control whether a network entity appears in a *RIB Visualization* window or a root cause analysis *Animation* window. For each type of entity, you can choose to always include it, include it if it announces more than a specified percentage of prefixes to any of its peers, or to never include it. The Always option is disabled if choosing it could create a visualization too big or crowded to read. The entities are as follows:
    - — Peer. The default is to include it if it announces 5% or more of the total number of prefixes.
    - — Nexthop. The default is to include it if it announces 5% or more of the total number of prefixes.
    - — Neighbor AS. The default is to include it if it announces 5% or more of the total number of prefixes.
    - — Non-Neighbor AS. The default is to include it if it announces 5% or more of the total number of prefixes.
- Algorithmic options control thresholds used by the Root Cause Analysis function:

- Percentage of prefixes on an edge that is flapping. The default is 10 percent.
- Percentage of prefixes that have shifted from one edge to another. The default is one percent.

Node Labels Options

The Node Labels options determine which node details to display on the routing topology map when it is first opened.

- DNS Names. Display the router DNS name.
- ID Number. Display RAMS's internal ID number for the router.
- IP Address. Display the router IP address (checked by default).
- Router Names. Display the name of the router obtained from the protocol (if available).
- Label routers only. Don't label the pseudonodes representing LANs (enabled by default).
- System ID. Display the IS-IS System ID (for IS-IS networks).

Miscellaneous Options

- The *Color Areas on Open Topology* option determines whether areas of the topology map are displayed in color. If checked (default), each area's nodes and links are displayed in a distinct color. If unchecked, all areas are displayed with black nodes and gray links.
- The *Default layout on Open Topology* option specifies the name of the saved layout that is used when loading a topology. This field is empty by default. You can enter a name manually, or set one automatically by saving a topology layout in the *Save Layout* dialog invoked from the Topology menu and clicking the **`Set as default`** checkbox in that dialog.
- The *Event panel default time interval* option sets the time period (default 600 seconds) that is included when you open a list of routing events using the **`Events`** button on a *Node Info* panel or *Link Info* panel when there is

no other time-range-based window opened. For example, if this value is set to 300 seconds, the list includes events that occurred in the past 300 seconds.

- The *Hide DNS Suffix* option determines how DNS names are displayed on the routing topology map. When DNS names of nodes are displayed, this suffix (if present) is trimmed from the names to reduce crowding of the layout. The default string is “mycompany.com”.
- The *Path Highlight: ECMP degree* option limits the number of ECMP (Equal Cost Multi-Path) routes to compute and display when you highlight a path between two routers or use the **`List/Find Path`** option from the Tools menu. The default is 4096; set to 1 to disable ECMP routes.

History Navigator Options

These options set default parameters for the History Navigator:

- The initial collection of graphs to be displayed in the *History Navigator* window (see Figure 59) may be selected by checking the desired options. Only the *Events* graph is enabled by default.
  - The *Events* graph displays the number of routing protocol changes that occurred in the network between recorded snapshots. Example routing events are a neighbor adjacency going down or a new prefix being announced.
  - The *Routers* graph displays the number of physical entities in the network. For OSPF, this includes AS Border Routers in other areas that are visible within the viewed area.
  - The *Links* graph displays the sum of router-to-router links plus the number of router-to-prefix links. Does not apply to BGP protocols.
  - The *Prefixes* graph displays the cumulative number of prefixes available in the network.
  - The *Routes* graph displays the number of routes advertised in the network. Does not apply to IGP protocols.
- The *Value of playback step in seconds* option sets the default value for a single step forward or backward in time during *History Navigator* playback. The factory setting is 600 seconds.

- The *Max number of data points in event graph* option limits the event graph to the specified number of data points. The factory default is 25,000 data points.
- The *Online Mode Update interval* option sets the number of seconds between updates. The factory default is 10 seconds.

Auto-Hide Options

These options determine when down or failed nodes or links are removed from the topology map.

- *Seconds to auto-hide failed links* (default 43200 seconds = 12 hours). A failed link is indicated by changing its color to red. However, when a link is decommissioned from service permanently, as far as routing is concerned there is no difference from the link going down. Set this value to the number of seconds after which a failed link should be considered decommissioned and no longer displayed. Set the option to -1 to disable this feature and continue to display down links. In any case, the link will again be displayed if the *History Navigator* is used to move the time cursor to a time when the link was up.
- *Seconds to auto-hide failed nodes* (default 43200 seconds = 12 hours). This option is analogous to the *Seconds to auto-hide failed links* option. Set this value to the number of seconds after which a failed node should be considered decommissioned and no longer displayed. Set the option to -1 to disable this feature.
- *Seconds to auto-hide failed links to pseudo nodes* (default, 0 seconds). This option is analogous to the *Seconds to auto-hide failed links* option but applies where one end of the failed link is a pseudonode. This option defaults to zero (hide immediately) since the pseudonode for a broadcast network will change whenever a new Designated Router is elected.
- *Seconds to auto-hide failed pseudo nodes* (default, 0 seconds). This option is analogous to *Seconds to auto-hide failed node* where the failed node is a pseudonode. This option defaults to zero (hide immediately) since the pseudonode for a broadcast network will change whenever a new Designated Router is elected.

- *Seconds to auto-hide detached nodes* (default, -1, meaning, disabled). A node can become detached from the rest of the network when all of its links are auto-hidden due to one of the conditions above. This option specifies the number of seconds after which the detached node will be hidden.
- *Seconds to auto-hide pseudo nodes with one attachment* (default -1, meaning, disabled).This option is similar to *Seconds to auto-hide detached nodes*, except that this option applies when the node is a pseudonode and one of its links is still visible. This condition can happen due to a bug in the router's implementation of IS-IS. When the pseudonode for a network changes, the Designated Router of the old pseudonode does not flush its attachment to the old pseudonode. Set this value to the number of seconds after which to auto-hide the pseudonode when the number of attached links is reduced to one.

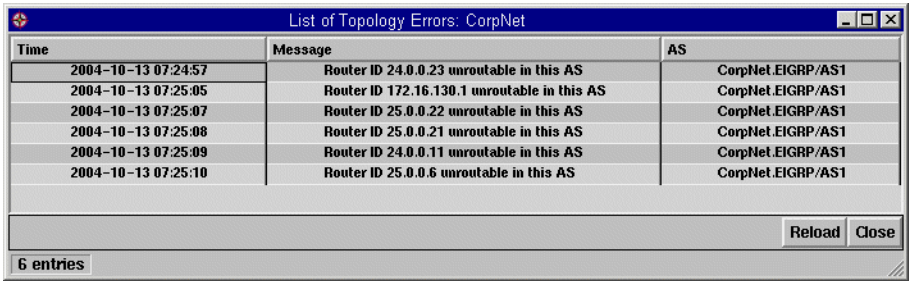
Diagnosing EIGRP Topology Errors

For EIGRP topologies, RAMS includes a Topology Diagnostics submenu in the Tools menu. You can select four different tables from this submenu to diagnose both anomalies in the network topology and problems with RAMS's modeling of the topology: **List Topology Errors, List Inaccessible Routers**, **List Mismatched Distances**, and **Find Invisible Links**. These tables are described in the following sections.

List Topology Errors

The Route Recorder can detect configuration anomalies as it collects information from the routers during its initial exploration of the topology and subsequent periodic re-explorations. These anomalies are stored in the database for presentation in the *List of Topology Errors* table. Only those anomalies detected since the start of the last full exploration are shown. These anomalies can indicate router configuration errors that should be corrected. Each row of the table includes the time at which the anomaly was detected, a description of the problem, and for topologies with multiple AS's, the AS where the anomaly was detected. Clicking on the table row for an error message will highlight the associated router(s) and/or link(s), assuming that those objects are present in the topology at the time currently being displayed. The History Navigator can be used to change the current time back to the time of the error message so that other tables can be used to diagnose the problem.

Figure 56 shows an example of the *List of Topology Errors* table.



List of Topology Errors: CorpNet

Time	Message	AS
2004-10-13 07:24:57	Router ID 24.0.0.23 unroutable in this AS	CorpNet.EIGRP/AS1
2004-10-13 07:25:05	Router ID 172.16.130.1 unroutable in this AS	CorpNet.EIGRP/AS1
2004-10-13 07:25:07	Router ID 25.0.0.22 unroutable in this AS	CorpNet.EIGRP/AS1
2004-10-13 07:25:08	Router ID 25.0.0.21 unroutable in this AS	CorpNet.EIGRP/AS1
2004-10-13 07:25:09	Router ID 24.0.0.11 unroutable in this AS	CorpNet.EIGRP/AS1
2004-10-13 07:25:10	Router ID 25.0.0.6 unroutable in this AS	CorpNet.EIGRP/AS1

6 entries

Figure 56 List of Topology Errors Table

The following anomalies are included in the table:

- Interface mask length mismatch – The address mask length is not the same for the interfaces on the two ends of a link.
- Duplicate router ID – Two routers are using the same router ID for the EIGRP routing process. The router ID is usually taken from the IP address of a loopback interface or other interface on the router, and should be unique for each router.
- Router ID is an interface address on another router – Since the router ID is normally derived from an interface address on the router, and interface addresses are normally unique to one router, it is an anomaly for the router ID on one router to be the same as an interface address on another router.
- Duplicate interface address – One or more interfaces on one router have the same IP addresses as interfaces on another router. The two routers are highlighted.
- Potential redistribution error – If an external prefix is advertised by a router but is unreachable from that router, this can indicate that the prefix is configured for redistribution but the metric has not been configured.
- Variance not supported by RAMS – Indicates that the router is configured for equal-cost multi-path routing with a variance value other than one. RAMS will only include the paths with the lowest metric.
- Router ID unroutable in this AS – The router ID of the indicated router is not an address within any routable prefix in the AS. If RAMS's router-to-router path highlighting function is used with this router as the destination, the path will be incomplete.
- Prefix with delay of 0 – The delay component of a prefix metric is zero. This condition can be caused by connected or static routes being redistributed without explicitly specifying the delay. This can result in a routing loop.
- Routing loop – The Route Recorder can discover a routing loop either during topology exploration or while investigating routing changes. Occasionally a routing loop can persist until manual intervention is taken. The *Time* column indicates when the loop was detected. Use the cursor in the *History Navigator* window to display the routing topology at that time,

and then click **Events** to look in the *All Events* list for events related to the prefix that is looping. Also try highlighting the path from one of RAMS's peer routers to that prefix.

List Inaccessible Routers

During the EIGRP topology exploration, RAMS attempts to establish a telnet/CLI connection to each router to collect information about neighbors, interface metrics, and external prefix attachments. If the connection to a router fails, RAMS cannot include that router in the topology, nor can it learn about other routers connected beyond that router. This might not matter if the routers are, for example, lab routers connected as a stub network. However, if there is a path between two accessible routers that passes through an inaccessible router, RAMS will not be able to find that path. Therefore, it is important to fix router accessibility problems so that RAMS's topology is correct. An example of the *List of Inaccessible Routers* table is shown in Figure 57. The table lists the routers that were inaccessible since the start of the most recent full topology exploration. For each inaccessible router, there is a column indicating the address of the last router on the path to the inaccessible one, and clicking on the entry in this column highlights that router on the topology map. Another column indicates the gateway (first-hop router) that RAMS used in attempting the connection, in case the solution would be to specify a different default gateway. The next column indicates a possible reason for failure to access the router:

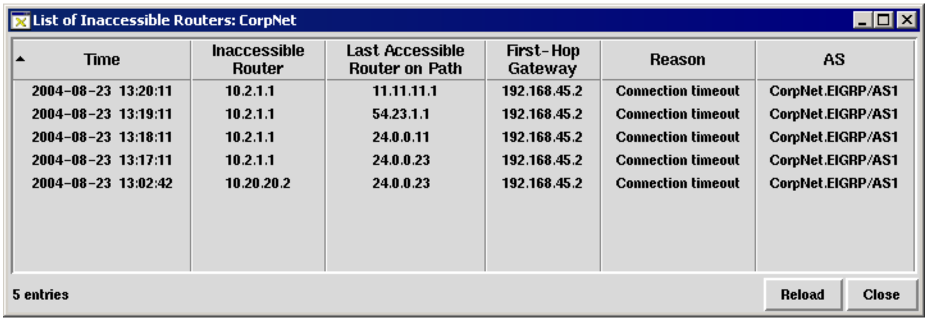
- Authentication failure – This occurs if the router does not accept the login password or user name/password configured in RAMS for the AS.
- Invalid input (unauthorized command?) – This error occurs if the TACACS account used by RAMS is not authorized to use one of the commands needed for topology exploration. This error could also occur due to garbled communication.
- Connection refused (no vty?) – If too many other telnet sessions are open at the time Route Explore attempts its connection such that no free virtual terminal is available on the router, the connection is refused.

RAMS attempts several connections with exponentially increasing delay. This error can also occur if the connection is blocked by a firewall or other device between RAMS and the intended destination router.

- Connection timeout – If the router is unreachable, for example, if the path to the router hits a black hole, then the connection will time out.
- Telnet open failed – Additional details are listed if provided by telnet.
- CLI parsing error – The output of the commands issued to the router in a query was not formatted as expected by RAMS. Please report this problem to technical support.
- Problem in recorder – RAMS was unable to issue the query for some reason. Please contact technical support to report this problem.

The final column indicates the AS in which the router resides.

By default, the table is sorted in descending order by time. To sort the table on any other field of information, click the column heading. To change the sort order (descending versus ascending order), click the column heading a second time.



List of Inaccessible Routers: CorpNet

Time	Inaccessible Router	Last Accessible Router on Path	First-Hop Gateway	Reason	AS
2004-08-23 13:20:11	10.2.1.1	11.11.11.1	192.168.45.2	Connection timeout	CorpNet.EIGRP/AS1
2004-08-23 13:19:11	10.2.1.1	54.23.1.1	192.168.45.2	Connection timeout	CorpNet.EIGRP/AS1
2004-08-23 13:18:11	10.2.1.1	24.0.0.11	192.168.45.2	Connection timeout	CorpNet.EIGRP/AS1
2004-08-23 13:17:11	10.2.1.1	24.0.0.23	192.168.45.2	Connection timeout	CorpNet.EIGRP/AS1
2004-08-23 13:02:42	10.20.20.2	24.0.0.23	192.168.45.2	Connection timeout	CorpNet.EIGRP/AS1

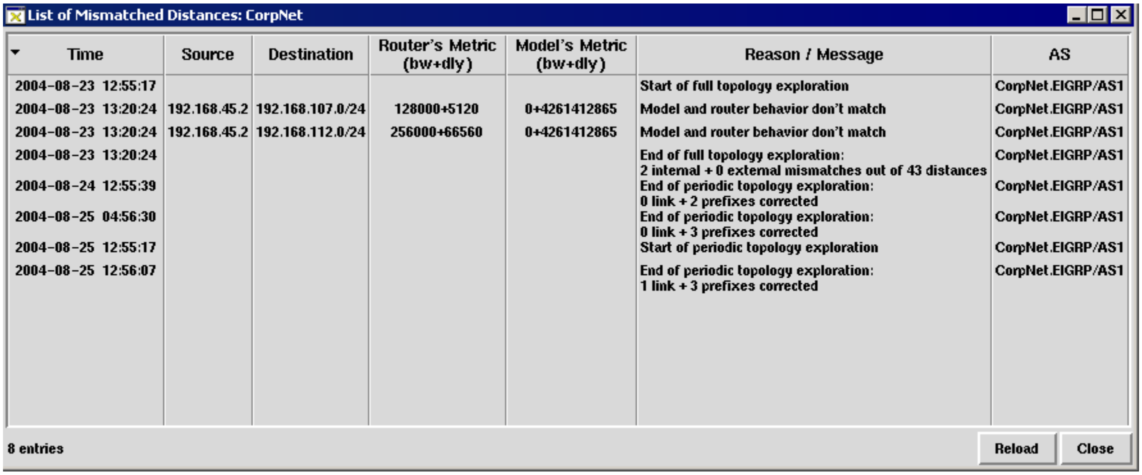
5 entries

Figure 57 List Inaccessible Routers Table

List Mismatched Distances

The *List of Mismatched Distances* table presents a list of prefixes for which the distance (metric) to the prefix reported by a router that peers with RAMS does not match the distance that RAMS calculates across its model of the topology. The Route Recorder compares these distances at the end of each full topology exploration to provide a measure of the accuracy of RAMS's topology model. Ideally, this table should be empty except for the messages telling when the last full topology exploration and subsequent periodic topology explorations began and ended.

An example of the *List of Mismatched Distances* table is shown in Figure 58.



List of Mismatched Distances: CorpNet

Time	Source	Destination	Router's Metric (bw+dly)	Model's Metric (bw+dly)	Reason / Message	AS
2004-08-23 12:55:17					Start of full topology exploration	CorpNet.EIGRP/AS1
2004-08-23 13:20:24	192.168.45.2	192.168.107.0/24	128000+5120	0+4261412865	Model and router behavior don't match	CorpNet.EIGRP/AS1
2004-08-23 13:20:24	192.168.45.2	192.168.112.0/24	256000+66560	0+4261412865	Model and router behavior don't match	CorpNet.EIGRP/AS1
2004-08-23 13:20:24					End of full topology exploration: 2 internal + 0 external mismatches out of 43 distances	CorpNet.EIGRP/AS1
2004-08-24 12:55:39					End of periodic topology exploration: 0 link + 2 prefixes corrected	CorpNet.EIGRP/AS1
2004-08-25 04:56:30					End of periodic topology exploration: 0 link + 3 prefixes corrected	CorpNet.EIGRP/AS1
2004-08-25 12:55:17					Start of periodic topology exploration	CorpNet.EIGRP/AS1
2004-08-25 12:56:07					End of periodic topology exploration: 1 link + 3 prefixes corrected	CorpNet.EIGRP/AS1

8 entries

Figure 58 List Mismatched Distances Table

There are several reasons why a mismatch occurs:

- Unreachable router hides actual path – Some mismatches are caused when the actual path goes through a router that RAMS cannot access and therefore the actual links traversed and their metrics are not known.
- Different equal-cost path chosen by model – If there are multiple paths with equal total cost but different bandwidth and delay components of the metric, then RAMS might choose a different path than the routers actually use because the router's algorithm is not always deterministic.
- Prefix not converged – When RAMS traces the actual path taken by the routers but finds that one of the routers has no route to the prefix in question, this usually indicates that EIGRP routing to the prefix has not converged, so the peer router's distance is not valid.

- Network has routing loop – This message indicates that RAMS encountered a routing loop when attempting to trace the actual path taken by the routers, which means EIGRP routing to the prefix has not converged and the peer router's distance is not valid.
- Model and router behavior don't match – A mismatch can occur if RAMS's modeling of the routers' behavior is not exact. However, a mismatch can also occur when a router becomes "confused" and reports inconsistent metric information (perhaps due to a bug in the router software). Some router configuration changes, such as changing an access-list (ACL) used in a route filter, don't take effect until the routing process is restarted.

  RAMS will see the new value but the router won't be using it, causing a distance mismatch. Please report this message to technical support if it persists across multiple full explorations.
- RAMS failed to query – This message indicates a possible bug in RAMS. Please report this problem to technical support.

The message inserted at the end of the full exploration tells how many internal and external prefix distances did not match along with the total number of distances known from peer routers that were compared.

RAMS periodically re-explores the topology to make sure no changes have been missed due to transitions that do not result in an EIGRP update being sent to RAMS or due to limitations in tracking network dynamics. The period is set as part of Route Recorder configuration and defaults to 8 hours. At the end of each periodic topology exploration, a message is added to the *List of Mismatched Distances* table telling the number of links and prefix attachments that were corrected during the last periodic topology exploration. Ideally, these numbers should also be zero.

By default, the table is sorted by time in descending order. To sort the table by any other field, click the column heading. To change the sort order (descending versus ascending order), click the column heading a second time.

Find Invisible Links

The first time this option is selected, RAMS runs a simulation on its topology model to determine if there are any links where a failure will not be immediately detected because the routers that peer with RAMS will not report an EIGRP distance change. During the simulation, RAMS fails each router interface in the topology model one at a time and then checks for a change in the routing distance to any prefix from any of the routers that peer with it. If there is any change, then RAMS will be able to detect a failure of the real interface. If not, then RAMS can only detect the interface failure during the next periodic topology exploration (by default every 8 hours). The most common cause of invisible links is route summarization. Using GRE tunnels to peer with additional routers behind summarization boundaries can increase RAMS's coverage.

The simulation can take several hours to run on a large network topology, but it can be canceled at any time. When completed, the results are stored in the database so that they can be viewed again later without waiting for the simulation to run again. If the topology has changed or additional peer routers have been added, click the **`Reload`** button on the *Invisible EIGRP Interfaces* table to re-run the simulation.

6

The History Navigator

One of the most powerful features of RAMS is its ability to display the detailed routing history of a network. The routing history is recorded by the recording component of the appliance, Route Recorder, which listens to the routing protocols and records all protocol events in a database.

Every ten minutes the Route Recorder saves a complete, time-stamped snapshot of the routing topology in the database. In between the snapshots, all routing announcements are recorded with timestamps. With this data, RAMS is able to display a precise routing map of the network at any point in time.

The *History Navigator* window displays statistical summaries of the recorded data in graphical format.The graphs show many vital network statistics versus time, including the number of events between snapshots and, at each snapshot, the number of routers, routing adjacencies, and prefixes.

The *History Navigator* window provides powerful data analysis functions. You can perform root cause analysis on event data, display the contents of the Routing Information Base (RIB) or visual representations of the RIB at any point in time, and perform a before-and-after comparison of the state of the network at two different points in time.

The *History Navigator* window can also display a list of the routing events that occurred during a specified time period. This is useful when diagnosing a network outage or performing forensic analysis after an outage.

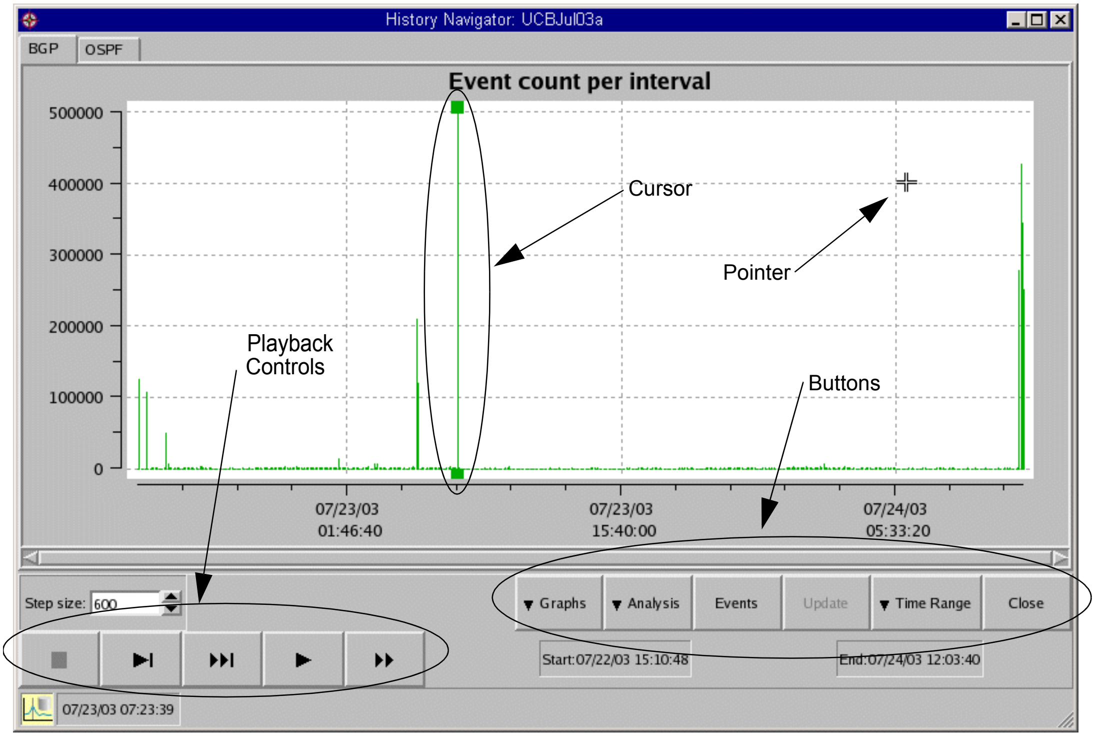
The History Navigator Window

Selecting **History Navigator** from the *Tools* menu, or clicking on the toolbar, displays the *History Navigator* window, as shown in Figure 59.

Note If a database contains multiple protocols, the *History Navigator* window displays multiple tabs, one for each protocol. As in the example shown in Figure 59, a database containing BGP and OSPF protocols has tabs for BGP and OSPF.

History Navigator Controls

The *History Navigator* controls, shown in Figure 59, allow you to navigate through the routing database and customize the presentation of data being displayed.



History Navigator: UCBJul03a

Step size: 600

Start:07/22/03 15:10:48

End:07/24/03 12:03:40

07/23/03 07:23:39

Figure 59 History Navigator Window

The elements on the window vary depending upon the current topology map mode:

Online mode – Indicates that the topology is currently being recorded and updates to the routing database are shown in the graphs as they occur. In this mode, the playback controls are disabled. Just above the playback controls is a text box that specifies the interval in minutes between updates. In addition, the **Graphs** button is disabled in this mode if the Time Range option is set to Online.

History mode – Indicates that only previously recorded information in the routing database is shown on the topology map. In this mode, the playback buttons are enabled and just above them is a text box that specifies the step size in seconds that is used during playback.

You can switch between modes by clicking the mode icon. This has the effect of changing the Time Range shown on the graph from *Online* to *One Week* (see Buttons on page 184 for information about the values that can be set with the **Time Range** button).

Status Bar

The status bar at the bottom of the *History Navigator* window is the same as the status bar on the *Topology Map* window. See Status Bar on page 122 for information about the icons and indicators on the status bar.

Cursor

The cursor is the green vertical hairline with green squares at the top and the bottom. The cursor indicates the currently displayed point in time within the routing topology history. There are several ways to move the cursor:

- You can use the mouse to drag the cursor to a different point on the time line. The topology map immediately displays the routing topology as it existed at that time.
- You can right-click on a point in the time line. A pop-up appears asking if you want to move time to that point. Select **`Yes`**. The topology map immediately displays the routing topology as it existed at that time.

- You can move the cursor through time by stepping or animating (automated stepping) using the playback controls as described in Playback Controls on page 185. Any paths highlighted on the routing topology map will be recomputed and redisplayed at each step of the replay.

Note Because the routing topology database does not store nodes and links that are down, any objects that are down when the topology is first opened will not be shown. If the cursor is moved back to a time when a down node or link was up, and then the cursor is moved to the current time again, the down node or link may remain on the map, but colored red to indicate that it is down, if the time traversed by the cursor movement is less than the failed node or link timeout interval (see Auto-Hide Options on page 172 for information about node/link timeout intervals).

Buttons

The panel of buttons in the lower right-hand corner of the window access graphs, data analysis tools, and events lists, and allow you to specify the time range that the *History Navigator* window displays. From left to right, the buttons are:

- The **Graphs** button lets you select which graphs are displayed. See Selecting History Graphs on page 186 for a description of the graphs. The **Graphs** button is disabled if you are working with an actively recording database and the Time Range option is set to Online.
- The **Analysis** button offers a list of five data analysis tools. See Analyzing Historical Data on page 188 for information about these tools.
- The **Events** button displays a detailed list of routing events. See Events List on page 206 for information about the Events list.
- The **Update** button is only enabled if the current window represents an actively recording database. If you display the window for more than 15 minutes, you can add newly recorded data to the current graph by clicking the `Update` button.
- The **Time Range** button determines how much data is included in the *History Navigator* window. By default, the time range is set to *Online* when in Online mode and to *One Week* when in History mode. You can set the time range to one hour, day, week, or month.

- The **Close** button closes the *History Navigator* window.

Playback Controls

The panel of buttons in the lower left-hand corner of the window control playback. From left to right, the buttons are:

■ The **Stop** button stops animated playback. The **Stop** button is enabled only in animated playback mode.

▶| The **Step** button advances the cursor by the number of seconds specified in the **Step size** text box. The topology map is updated with the recorded data from the new point in time.

▶▶| The **Fast Step** button advances the cursor by 10 times the number of seconds specified in the **Step size** text box. The topology map is updated with data from the new point in time.

▶ The **Animate** button automatically steps through routing history by executing a continuous sequence of cursor advances, with the network map being updated at each step. If any paths are highlighted, the routes will also be recomputed and redisplayed at each step. Click the **`Stop`** button to stop the animated playback.

▶▶ The **Fast Animate** button starts animated playback in fast mode, that is, automatically advancing the cursor by 10 times the number of seconds specified in the **Step size** text box. Click the **`Stop`** button to stop the animated playback.

Note Because stepping and animation advance time in steps of the specified interval, a routing change will not be shown if it occurs and then changes back within one time interval. The *Events List* window, described on page 206, includes all routing changes.

Zooming the Time Line

RAMS lets you zoom into a subsection of the recorded history shown on the *History Navigator* graph. Zooming in the time dimension may help you to see more detail within a cluster of event spikes when the graph covers a long period of time. Zooming in the Y dimension may help you to see small changes in the number of objects in the Routers or Links graphs when the total number is large.

To zoom the time line, perform the following steps:

1. While holding the **CTRL** key down, click and drag a rectangle with the mouse to select the area to be expanded to fill the graph.
2. While holding the **CTRL** key down, release the left mouse button to set the zoom area.
3. Repeat steps 1 and 2 to increase the level of zoom.
4. To broaden (unzoom) the view one level, hold the **CTRL** key down, and then click the right mouse button. Repeat until the graph returns to the original zoom level.

Selecting History Graphs

The primary feature of the *History Navigator* window is the Events graph that is shown in the default window. RAMS provides four additional graphs that may be used to display data. Together, these graphs offer a wide range of statistics about the state of the network.

- **Routers** – The Routers graph displays the number of physical entities in the network. For OSPF, this includes AS Border Routers in other areas that are visible from the viewed area.
- **Routes** – The Routes graph displays the number of routes advertised in the network. This graph does not appear if the topology currently selected in the History Navigator is an IGP area or AS.
- **Prefixes** – The Prefixes graph displays the number of prefixes available in the entire network.
- **Events** – The Events graph displays the number of routing protocol changes that occurred in the network between recorded snapshots. Example routing events include a neighbor adjacency going down or a new prefix being announced. For EIGRP, both distance-vector events and derived link-state events are included.
- **Links** – The Links graph displays the sum of router-to-router links plus the number of router-to-prefix links. This graph does not appear if the topology currently selected in the History Navigator is a BGP AS.

To display any of these graphs, click **`Graphs`**, and then select the boxes beside the desired graphs.

Note The **`Graphs`** button is disabled when you are working with an actively recording database and the **`Time Range`** option is set to Online.

You can configure RAMS to include any or all of the graphs in the default window. See Configuration Options Dialog on page 169 for more information.

Analyzing Historical Data

RAMS provides five powerful analysis tools via the **Analysis** button in the *History Navigator* window. These tools include the following:

- Root Cause Analysis
- RIB Visualization
- RIB Browser
- RIB Before-and-After Comparison
- Event Analysis

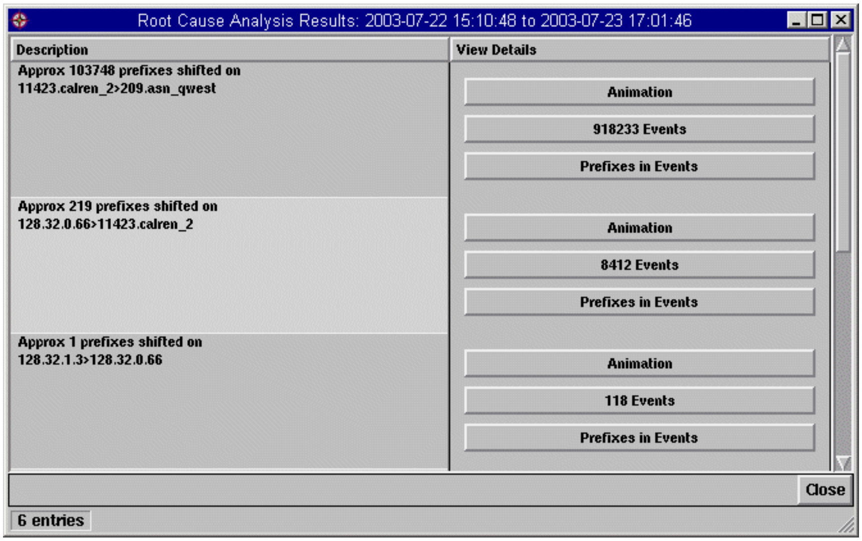
Root Cause Analysis

The Root Cause Analysis function analyzes the huge amounts of data generated by BGP-related routing events and distills the data down to the essential information that helps you to pinpoint the cause and location of the event.

To perform a root cause analysis, perform the following steps:

1. Click the **`Analysis`** button.
2. Select **`Root Cause Analysis`**.
3. Left-click in the graph just before the events occurred.
4. Left-click in the graph just after the events occurred.

   The *Root Cause Analysis Results* dialog opens. Figure 60 shows an example of the dialog.



Root Cause Analysis Results: 2003-07-22 15:10:48 to 2003-07-23 17:01:46

Description	View Details
Approx 103748 prefixes shifted on 11423.calren_2>209.asn_qwest	Animation 918233 Events Prefixes in Events
Approx 219 prefixes shifted on 128.32.0.66>11423.calren_2	Animation 8412 Events Prefixes in Events
Approx 1 prefixes shifted on 128.32.1.3>128.32.0.66	Animation 118 Events Prefixes in Events

Figure 60 Root Cause Analysis Results Dialog

The events that occurred during the time period you specified in steps 3 and 4 are analyzed and correlated into groups. All of the BGP routing messages that apply to related events are summarized in the dialog. In the example shown in Figure 60, three groups of events are listed. To the right of each group are three buttons:

- The **Animation** button generates an animated visualization of the routing topology during the related events. The *Animation* window is described below.
- The **Events** button displays a detailed list of the events that constitute the group.
- The **Prefixes** button displays a list of all prefixes affected by the group of events.

Animation Window

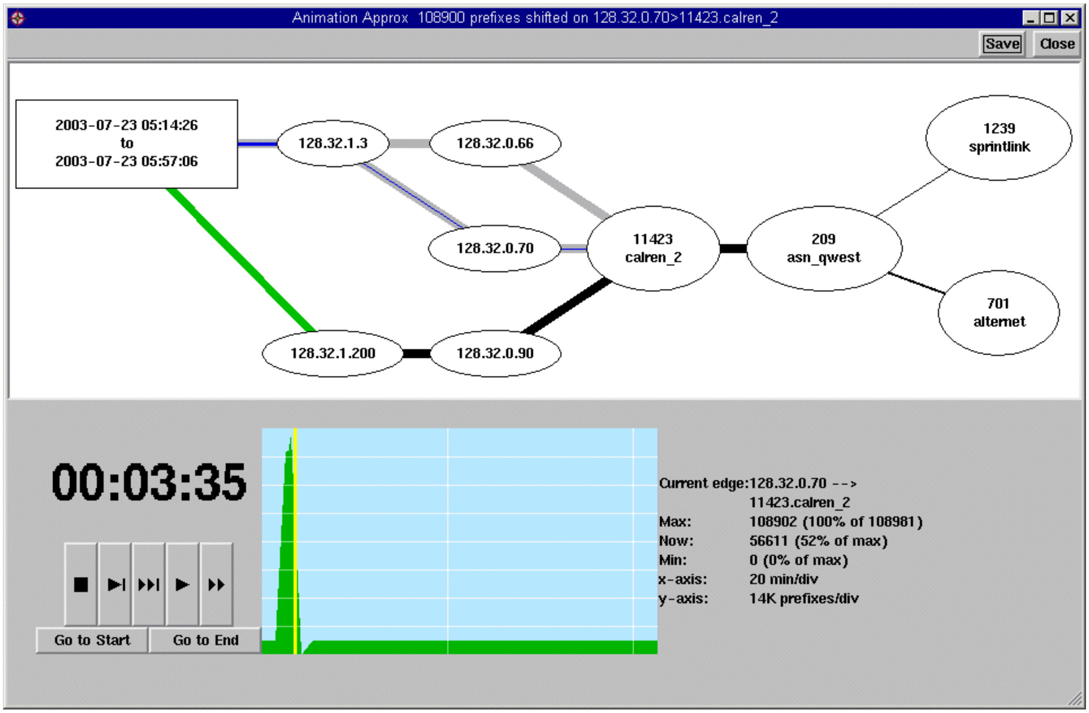
A BGP router's routes form a virtual tree rooted at the router. The visualization function creates a graphical representation of this tree from the viewpoint of each BGP edge router (or core route reflector) and merges them into a single tree. The RAMS appears at the left side of the tree. The time range of the animation is indicated in the RAMS rectangle. To the right of the

RAMS are its BGP peers; to their right are its BGP NextHops; to their right are the ASs the NextHops serve; to the right of the ASs are any downstream ASs; to the right of the downstream ASs are the prefixes they advertise.

The visualization function assigns a weight to each edge (that is, each trunk or branch or twig) of the tree that is equivalent to the number of unique prefixes carried by the edge, and uses this weight to determine the thickness of the line representing that edge. The thickness of an edge displayed on the *Animation* window is based solely on the number of prefixes that are routed over that edge, not how much traffic is flowing over the edge. (The visualization function is a routing diagnostic tool, not a traffic diagnostic tool.)

Figure 61 shows an example of the *Animation* window.

Animations can help you to identify, isolate, and resolve problems that are difficult to diagnose, for example, continuous customer route flaps, persistent MED oscillations, and “leaky” routes.



Animation Approx 108900 prefixes shifted on 128.32.0.70>11423.calren_2

2003-07-23 05:14:26
to
2003-07-23 05:57:06

00:03:35

Current edge:128.32.0.70 -->
11423.calren_2
Max: 108902 (100% of 108981)
Now: 56611 (52% of max)
Min: 0 (0% of max)
x-axis: 20 min/div
y-axis: 14K prefixes/div

Figure 61 Root Cause Analysis Animation Window

The upper pane of the window displays the visualization. The lower pane of the window contains the following elements:

- **Clock** – Indicates elapsed time during animation.
- **Playback** controls – Control the animation. These are identical to the playback controls on the *History Navigator* window (see Playback Controls on page 185).
- **Go to Start** and **Go to End** buttons – Reposition the yellow cursor in the graph. In addition, you can move the cursor by clicking the position in the graph to which you want to move.
- **Graph** – Represents the change in number of prefixes carried by an edge. By default, the edge on which the graph is based is the most active edge, that is, the edge that lost or gained the most prefixes. You can change the perspective of the graph by clicking on another edge in the visualization.

  To the right of the graph is a list of details about the graph, including the nodes at either side of the edge on which the graph is based, the maximum, current, and minimum number of prefixes carried by the edge, and the scale of the *x* and *y* axes of the graph.

Playing an Animation

When you animate the visualization using one of the playback controls, the group of related events you selected is replayed in both the visualization pane and the graph pane.

- In the visualization pane of the window, the thickness and color of an edge indicates the level of activity on the edge.
  - The thickness of the line representing an edge changes based on the number of unique prefixes that are routed over the edge. The thickness of a grey shadow surrounding a line indicates the maximum number of prefixes the edge ever carried, while the thickness of the colored portion of the line indicates the current number of prefixes the edge carries.
  - The color of the edge changes as the edge gains or loses prefixes. A black line indicates that no changes are occurring. Green indicates that the edge is gaining prefixes, while blue indicates that the edge is losing prefixes.

- In the graph pane of the window, a yellow line indicating the current position in the animation moves from left to right, while the clock indicates elapsed time.

To play an animation, perform the following steps:

1. Choose a playback mode:

   - Step mode advances the cursor. The step interval depends upon the actual duration covered by the visualization.

     The formula for calculating the interval in milliseconds is $I = (A/P) \times 25$, where *A* is the actual duration in seconds of the period covered by the animation, and *P* is 30 for step mode or 15 for fast step mode.

   - Fast step mode advances the cursor by twice the interval of step mode.
   - Animate mode advances the cursor in a continuous series of steps through the time range covered by the visualization. The animation completes in 30 seconds, regardless of the actual interval covered by the visualization.
   - Fast Animate mode advances the cursor through the time range covered by the visualization. The animation completes in 15 seconds, regardless of the actual interval covered by the visualization.

2. Click the corresponding playback button to begin the animation.

   Note If the RAMS's adjacency to its peers was down at the specified start point, the *Animation* window may initially be blank except for the rectangle representing the RAMS. However, when you click a playback button, the tree is filled in as adjacencies stabilize.

To replay an animation, perform the following steps:

1. Click the `Go to Start` button to move the yellow cursor back to the left side of the graph.
2. Click a playback button to begin the animation.

To animate a different edge, perform the following steps:

1. In the visualization pane of the *Animation* window, click another edge to select it.

The graph pane of the *Animation* window now displays information about the selected edge, and the graph displays the change in prefixes on the selected edge.

2 Click a playback button to begin the animation.

Saving an Animation

You can save an animation for later viewing by clicking **`Save`** in the upper right corner of the *Animation* window. The animation is saved in SVG format (Scalable Vector Graphic, file extension `.svg`) on the RAMS hard disk. SVG is a W3C standard for producing high quality graphics. SVG support is not yet standard in most browsers, so you may need to download a plug-in to view saved animations.

Adobe has a free SVG plug-in (see **http://www.adobe.com/svg/viewer/install/main.html**). HP has used the Adobe plug-in with a variety of browsers on Linux, Mac OS X and Microsoft Windows platforms.

Alternatively, the Apache Batik project has a standalone SVG viewer called *squiggle* which can be downloaded from **http://xml.apache.org/batik/install.html#distributions**. Because *squiggle* is written in Java, it runs on almost any platform, but the current version seems to take more CPU than the Adobe viewer.

To view a saved animation, perform the following steps:

1 Open a browser and navigate to the RAMS *Home* page.

2 Click the **`Saved Files`** link.

The *Login* page appears.

3 Enter your username and password. You do not need Administrator privilege to access the *Saved Files* page.

4 On the *Saved Files* page, click the **`BGP Animations`** link under Saved Reports.

The *SVG Animations* page displays a list of all saved SVG files, and contains a link to the installation page for the Adobe plug-in.

5 Click the title of the animation you wish to view to open an *Animation* window for that animation. All of the information and controls present in the original animation are available in the saved animation.

RIB Visualization

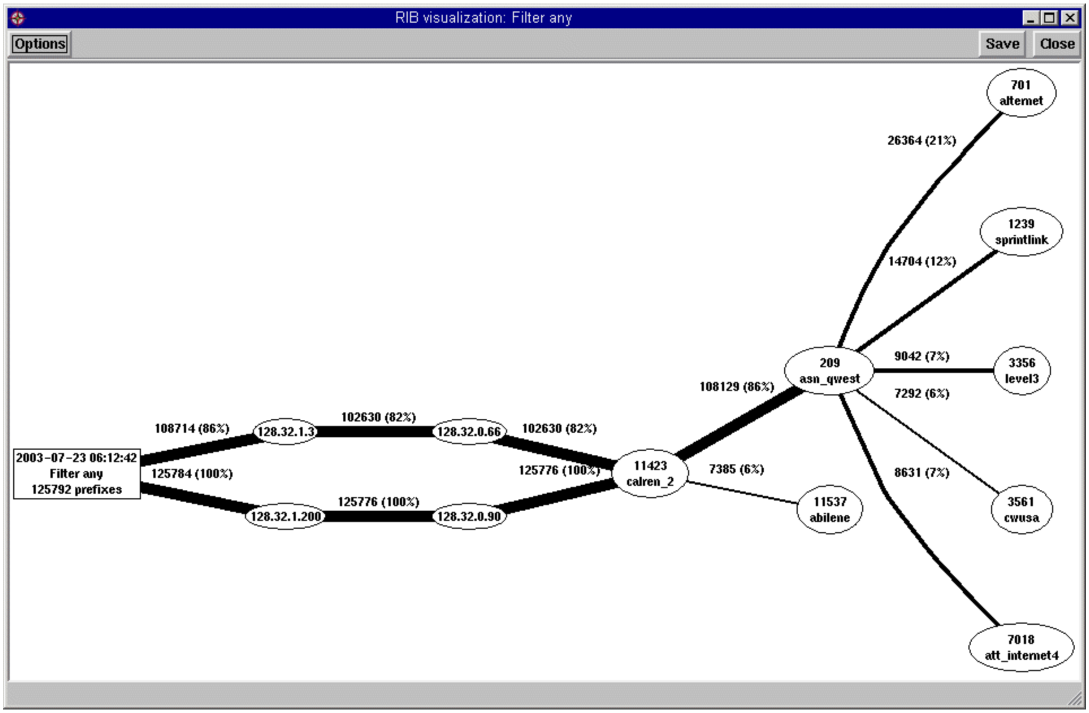
The RIB Visualization function provides you with a still image that represents the BGP Routing Information Base (RIB) at the time indicated by the current History Navigator cursor position. Visualizations can help you identify difficult-to-diagnose problems such as prefix load-balancing issues.

To generate a RIB visualization, perform the following steps:

1 Move the History Navigator cursor to the time desired.

2 Click **`Analysis`**.

3 Select **`RIB Visualization`**.



The *RIB Visualization* window opens, as shown in Figure 62.

Figure 62 RIB Visualization Window

A BGP router’s routes form a virtual tree rooted at the router. The Visualization function creates a graphical representation of this tree from the viewpoint of each BGP edge router (or core route reflector) and merges these trees into a single tree. The RAMS appears at the left side of the tree.The RAMS rectangle indicates the date and time of the RIB snapshot and the total number of prefixes. In addition, the rectangle indicates how the routes were filtered before the picture was generated. In the example shown in Figure 62, “Filter any” indicates that all routes were included. You can create visualizations filtered to include only a subset of the routes from the *RIB Browser* as described on page •199.

To the right of the RAMS are its BGP Peers, followed by its BGP NextHops; to their right are the ASs that the NextHops serve; to the right of the ASs are any downstream ASs; to the right of the downstream ASs are the prefixes they advertise.

The RIB Visualization function assigns a weight to each edge (that is, each trunk or branch or twig) of the tree that is equivalent to the number of unique prefixes carried by the edge, and uses this weight to determine the thickness of the line representing that edge. The thickness of an edge displayed on the *RIB Visualization* window is based solely on the number of prefixes that are routed over that edge, not how much traffic is flowing over the edge. The visualization function is a routing diagnostic tool, not a traffic diagnostic tool.

Each entity in the visualization is identified, and each edge is labeled with the number of unique prefixes advertised on that edge and the percentage of the total number of prefixes in the network.

Entities are included in the visualization (or excluded from it) based on these percentages. You can change the default thresholds on a global basis (see Analysis Options on page 169 for information). You can also change the thresholds for the current visualization only.

To change RIB visualization thresholds, perform the following steps:

1 In the *RIB Visualization* window, click **`Options`**.

The Visualization options are displayed in the left pane of the window. These options are identical to the options described in Analysis Options on page 169.)

2 Change thresholds as desired.

Lowering a threshold increases the number of entities that are included in the visualization, giving you a more detailed picture. Conversely, raising a threshold decreases the number of entities and level of detail.

Note If choosing one of the Always options would create a visualization too big or crowded to read, that option is disabled.

3 Click **`Redraw`**, and then select **`In Place`** or **`In New Window`**.

   If you select `In Place`, your changes are applied only to the current window. If you select `In New Window`, your changes are applied only to the new window, not to the original window.

Saving a Visualization

You can save a visualization for later viewing by clicking **`Save`** in the upper right corner of the *Visualization* window. The visualization is saved in SVG format (Scalable Vector Graphic, file extension `.svg`) on the RAMS hard disk. SVG is a W3C standard for producing high quality graphics. SVG support is not yet standard in most browsers, so you may need to download a plug-in to view saved visualizations. See Saving an Animation on page 193 for available plug-ins.

To view a saved visualization, perform the following steps:

1. Open a browser and navigate to the RAMS *Home* page.
2. Click the **`BGP Reports`** link.
3. Enter your username and password in the *Login* page. You do not need Administrator privilege to access the *BGP Reports* page.
4. On the *BGP Reports* page, click the **`SVG Animations`** link under Saved Reports.

   The *SVG Animations* page displays a list of all saved SVG files, as well as a link to the installation page for the Adobe plug-in.
5. Click the title of the visualization you wish to view to open a *Visualization* window for that visualization.

RIB Browser

Use the Routing Information Base (RIB) Browser to display the following:

- For IGP, links and prefixes that went down during a specified historical time period.

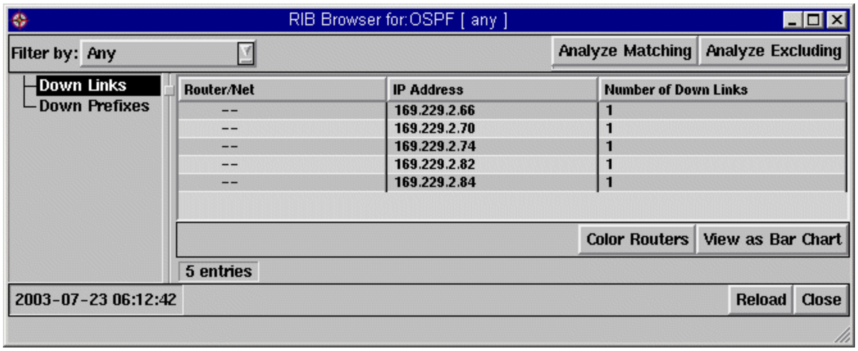
- For BGP, distribution of routes based on attributes such as Peer, Nexthop, MED, and so on.

To open the *RIB Browser* dialog, click the **Analysis** button and select **RIB Browser**.

IGP Protocols

For IGP protocols, the *RIB Browser* dialog displays a list of links and prefixes that went down in the time period displayed at the bottom of the *History Navigator* window. Figure 63 shows an example of the *RIB Browser* dialog with IGP link data.

On the left side of the *RIB Browser* dialog, click **Down Links** or **Down Prefixes** to view the list of links or prefixes, respectively, that went down during the specified period. The *Router* column identifies the router that corresponds to each link or prefix while the *Count* column displays the number of times the link or prefix went down. To view the list of links or prefixes as a bar chart, click **View as Bar Chart**.



Router/Net	IP Address	Number of Down Links
--	169.229.2.66	1
--	169.229.2.70	1
--	169.229.2.74	1
--	169.229.2.82	1
--	169.229.2.84	1

5 entries

2003-07-23 06:12:42

Figure 63 RIB Browser Dialog For IGP

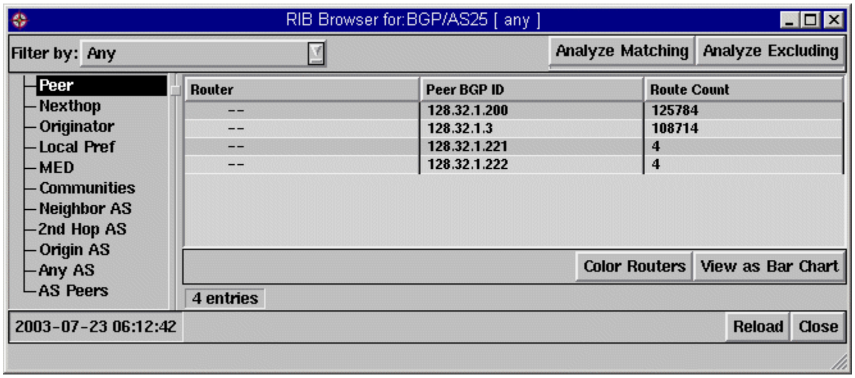
To locate one of the identified routers on the routing topology map, click the list entry for that router. That entry will be highlighted in the list and the router will flash yellow on the routing topology map. Alternatively, click **Color Routers** to color all the listed routers on the map at the same time using a spectrum of red to green for highest to lowest number of times the link or prefix went down.

To view the details for a particular router, right-click the corresponding list entry, and then select one of the following choices from the pop-up menu:

- **Show Links/Show Prefixes** – Displays a list of detailed information about all the links or prefixes associated with that router.
- **Filter Analysis** – Displays a new *RIB Browser* window with data for the selected router only.

BGP Protocol

Figure 64 shows an example of the *RIB Browser* dialog with BGP peer data.



Router	Peer BGP ID	Route Count
--	128.32.1.200	125784
--	128.32.1.3	108714
--	128.32.1.221	4
--	128.32.1.222	4

Figure 64 RIB Browser Dialog For BGP

For BGP protocol, the RIB Browser dialog displays distributions of the advertised prefixes their attributes. A tree structure on the left side of the dialog presents the following attribute options:

- **Peer** – For each peer, displays the number of routes advertised by that peer.
- **Nexthop** – For each Nexthop, displays the number of routes that list that Nexthop router among their attributes.
- **Originator** – For each Originator, displays the number of routes that list that Originator among their attributes.
- **Local Pref** – For each Local Pref, displays the number of routes that list that Local Pref among their attributes.
- **MED** – For each MED, displays the number of routes that list that MED among their attributes.
- **Communities** – For each community, displays the number of routes that list that community among their attributes.

- **Neighbor AS** – For each Neighbor AS, displays the number of routes that list that neighbor AS among their attributes.
- **2nd Hop AS** – For each 2nd Hop AS, displays the number of routes that list that 2ndHopAS among their attributes.
- **Origin AS** – For each Origin AS, displays the number of routes that list that origin AS among their attributes.
- **Any AS** – For each AS, displays the number of routes that list that AS among their attributes.
- **AS Peers** – For each pair of AS peers, displays the number of routes that list that peer-pairing among their attributes.

For the Peer, Nexthop and Originator options, click a router in the list and the corresponding node flashes yellow on the routing topology map. To view any of the lists as a bar chart, click **`View as Bar Chart`**.

To view additional information for a particular entry, right-click the entry, and then select one of the following choices on the pop-up menu:

- **Show Routes** – Displays a list of the routes that include that entry among their attributes.
- **Visualize** – Displays a visualization of the BGP tree as seen by the selected entity (see RIB Visualization on page 194).
- **Filter Analysis** – Displays a new *RIB Browser* window with data for the selected entity only.

RIB Browser Comparison

Use this option to compare the state of the network at two points in time. This option is useful for analyzing the before and after state of the network when an unusually large number of events occur within a given period of time. Figure 65 provides an example of one such instance.

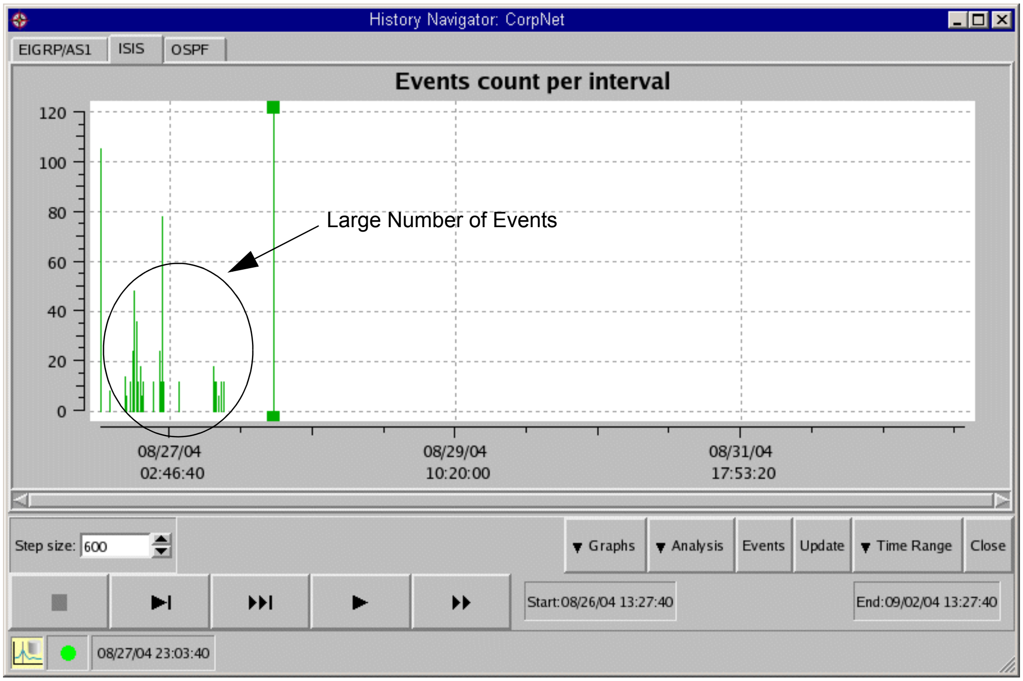


Figure 65 Large Number of Events in Short Space of Time

To analyze the state of the network just before these events occurred against the state of the network just after, use the RIB Comparison function.

To use the RIB Browser Comparison, perform the following steps:

1 Click the **`Analysis`** button.

2 Select **`RIB Comparison`**.

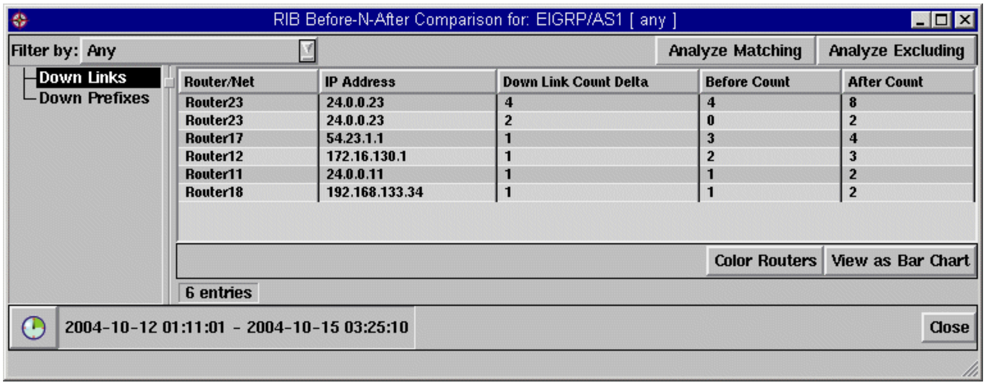
3 Click in the graph just before the events occurred.

4 Click in the graph just after the events occurred.

The *RIB Before-N-After Comparison* dialog opens. This dialog is very similar to the *RIB Browser* dialog.

IGP Protocols

For IGP protocols, the *RIB Before-N-After Comparison* dialog includes columns for the link and prefix counts before and after the events, and also a column for the difference between the two. Figure 66 show an example of the *RIB Comparison* dialog with IGP link data.



RIB Before-N-After Comparison for: EIGRP/AS1 [any]

Filter by: Any

Router/Net	IP Address	Down Link Count Delta	Before Count	After Count
Router23	24.0.0.23	4	4	8
Router23	24.0.0.23	2	0	2
Router17	54.23.1.1	1	3	4
Router12	172.16.130.1	1	2	3
Router11	24.0.0.11	1	1	2
Router18	192.168.133.34	1	1	2

6 entries

2004-10-12 01:11:01 - 2004-10-15 03:25:10

Figure 66 RIB Comparison Dialog for IGP

Click the **`Down Link`** and **`Down Prefix`** options to view information about the down links and prefixes, respectively. To view the list of links or prefixes as a bar chart, click **`View as Bar Chart`**.

To locate one of the identified routers on the routing topology map, click the list entry for that router. That entry will be highlighted in the list and the router will flash yellow on the routing topology map.

Alternatively, click **`Color Routers`** to color all of the listed routers on the map at the same time using a spectrum of red to green for highest to lowest number of times the link or prefix went down.

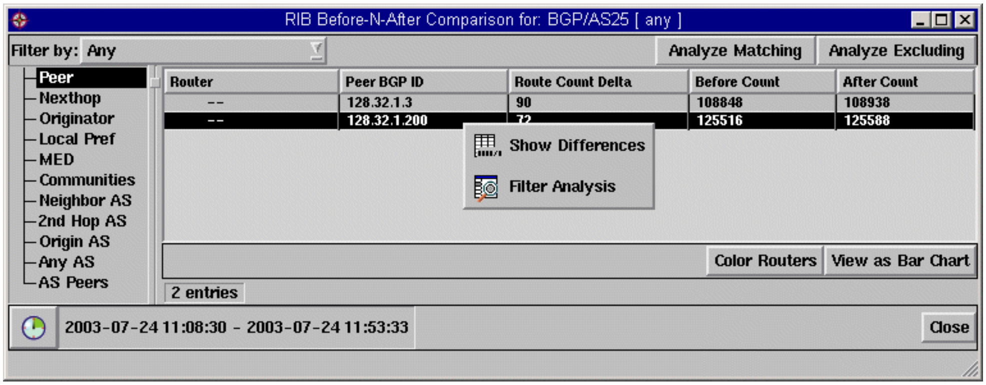
To view additional information for a particular entry, right-click the corresponding list entry and select one of the following choices on the pop-up menu:

- **Show Events** – Displays a list of the events reported by that entry. This window is similar to the *Events* window described in Events List on page 206.
- **Filter Analysis** – Displays a new window with data for the selected router only.

BGP Protocols

For BGP protocols, the same options appear in the *RIB Before-N-After Comparison* dialog as those that appear in the *RIB Browser* dialog. The only difference is the addition of the *Before*, *After*, and *Delta* columns that display the route count before and after the specified events and the difference between the two counts.

For the Peer, Nexthop and Originator options, click any entry in the list, and the corresponding node flashes yellow on the map. To view any of the lists as a bar chart, click **`View as Bar Chart`**.



RIB Before-N-After Comparison for: BGP/AS25 [any]

Filter by: Any

Router	Peer BGP ID	Route Count Delta	Before Count	After Count
--	128.32.1.3	90	108848	108938
--	128.32.1.200	72	125516	125588

2 entries

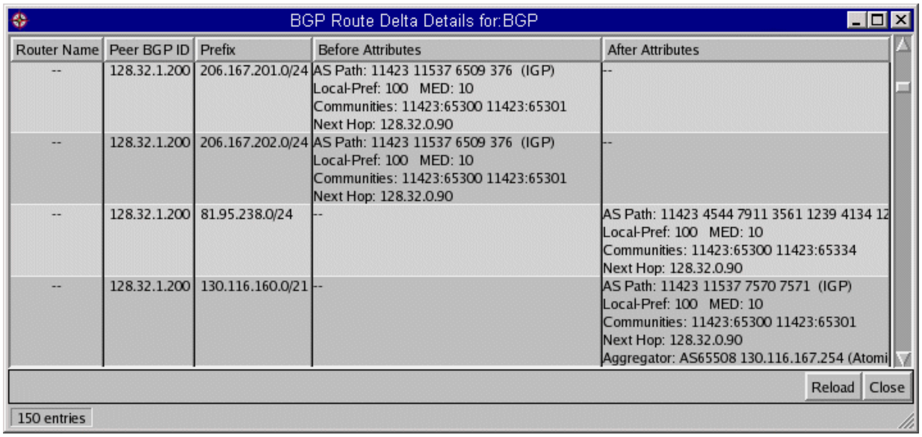
2003-07-24 11:08:30 - 2003-07-24 11:53:33

Figure 67 RIB Comparison Dialog for BGP

In Figure 67, the *RIB Comparison* dialog is shown with the pop-up menu that opens when you right-click an entry in the list.

To view additional information for a particular entry, select and right-click the entry, and then select one of the following choices from the pop-up menu:

- **Show Differences** – Displays detailed information about the delta between the *before* state and the *after* state, based on the attribute selected in the *RIB Comparison* dialog. See Figure 68 for an example of the display.
- **Filter Analysis** – Displays a new *RIB Browser* window with data for the selected entity only.



BGP Route Delta Details for:BGP

Router Name	Peer BGP ID	Prefix	Before Attributes	After Attributes
--	128.32.1.200	206.167.201.0/24	AS Path: 11423 11537 6509 376 (IGP) Local-Pref: 100 MED: 10 Communities: 11423:65300 11423:65301 Next Hop: 128.32.0.90	--
--	128.32.1.200	206.167.202.0/24	AS Path: 11423 11537 6509 376 (IGP) Local-Pref: 100 MED: 10 Communities: 11423:65300 11423:65301 Next Hop: 128.32.0.90	--
--	128.32.1.200	81.95.238.0/24	--	AS Path: 11423 4544 7911 3561 1239 4134 12 Local-Pref: 100 MED: 10 Communities: 11423:65300 11423:65334 Next Hop: 128.32.0.90
--	128.32.1.200	130.116.160.0/21	--	AS Path: 11423 11537 7570 7571 (IGP) Local-Pref: 100 MED: 10 Communities: 11423:65300 11423:65301 Next Hop: 128.32.0.90 Aggregator: AS65508 130.116.167.254 (Atomi

150 entries

Figure 68 Show Differences Display

Event Analysis

When a large cluster of routing events occurs, it may be difficult to grasp the nature of the problem by looking at individual events. RAMS can help you analyze the series of routing events to determine the distribution of events according to which routers, links, prefixes, and BGP attributes were involved. These distributions are presented as tables or bar charts.

To analyze a series of events, proceed as follows:

1. Click the **`Analysis`** button to open a menu of analysis functions.
2. Select **`Event Analysis`** from the menu.
3. Click in the Events graph just before the events occurred.
4. Click in the Events graph just after the events occurred.

   The *Event Analysis* dialog appears.

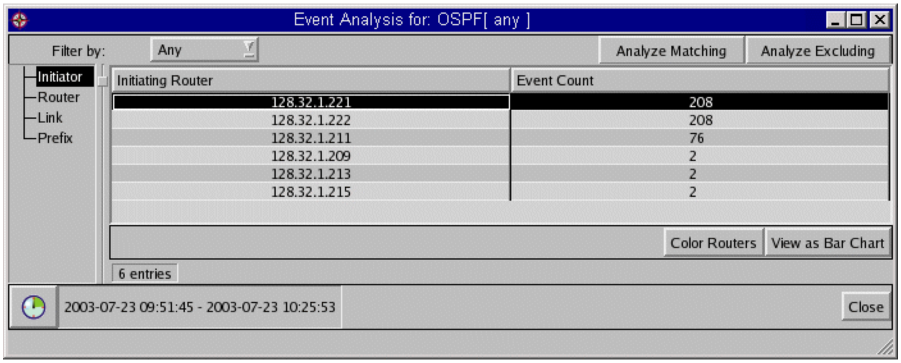
IGP Protocols

For IGP protocols, this dialog displays the number of routing events that occurred in the specified time interval for each involved initiator, router, link, or prefix. Figure 69 shows an example of this dialog.

To locate a router on the routing topology map, select the entry for that router. The selected entry is highlighted in the list and the router flashes yellow on the routing topology map. Alternatively, click **`Color Routers`** to color all the listed routers on the map at the same time using a spectrum of red to green for highest to lowest number of events per router.

To view additional information for a particular entry, select and right-click the corresponding list entry, and then select one of the following choices on the pop-up menu:

- **Show Events** – Displays a list of events reported by the selected entity. See Events List Controls on page 207 for information on the controls that allow you to replay the listed events.
- **Filter Analysis** – Displays a window with data for the selected entity only.



Initiating Router	Event Count
128.32.1.221	208
128.32.1.222	208
128.32.1.211	76
128.32.1.209	2
128.32.1.213	2
128.32.1.215	2

2003-07-23 09:51:45 - 2003-07-23 10:25:53

Figure 69 Event Analysis Dialog for IGP

BGP Protocol

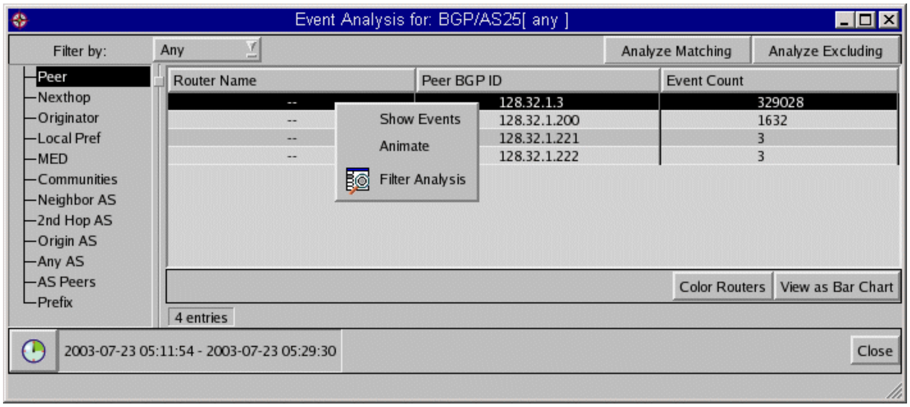
For BGP, the *Event Analysis* dialog displays the number of routing events that occurred in the specified time interval with particular values for the Peer, Nexthop, Originator, Local Pref, MED, Communities, Neighbor AS, 2nd Hop AS, Origin AS, Any AS, AS Peers, or Prefix attributes.

To locate a router on the routing topology map, select the list entry for that router. The selected entry is highlighted in the list and the router flashes yellow on the routing topology map. Alternatively, click **`Color Routers`** to color all the listed routers on the map at the same time using a spectrum of red to green for highest to lowest number of events per router.

To view additional information for a particular entry, select and right-click the corresponding list entry, and then select one of the following choices on the pop-up menu:

- **Show Events** – Displays a list of events reported by the selected entity. See Events List on page 206 for information about this window.
- **Animate** – Displays an *Animation* window that animates the events reported by the selected entity. No RCA Analysis is performed. See Root Cause Analysis on page 188 for information about the controls present in this window.
- **Filter Analysis** – Displays a window with event data for the selected entity only.

Figure 70 shows an example of the *Event Analysis* dialog for BGP, and includes the pop-up menu that appears when you right-click an entry in the list.



Filter by: Any

Router Name	Peer BGP ID	Event Count
--	128.32.1.3	329028
--	128.32.1.200	1632
--	128.32.1.221	3
--	128.32.1.222	3

4 entries

2003-07-23 05:11:54 - 2003-07-23 05:29:30

Figure 70 Event Analysis Dialog for BGP

Events List

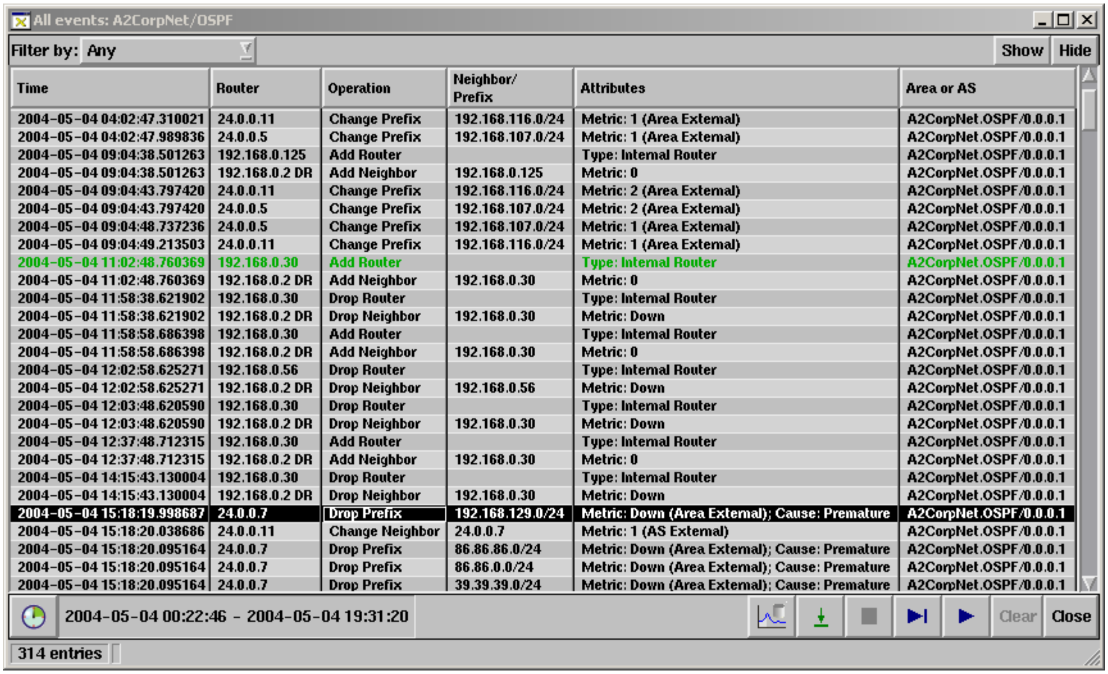
After the general nature of a routing problem has been identified, you may want to look at individual routing events to determine what caused the problem. The *All Events* list shows a sequential list of all routing events recorded in the database for a selected time interval. For each event, the list shows several columns of details, such as the router that initiated the event.

To view a list of individual events, perform the following steps:

1. Click **`Events`** in the *History Navigator* window.
2. Move the mouse cursor, displayed as blue crosshairs, to the desired starting time in the graph and left-click to leave a blue line marking that time.
3. Move the mouse cursor to the ending time and left-click again to mark that time.

   The *All Events* window opens displaying details of the events that occurred within the selected time period, as shown in Figure 71.

Caution If the time period selected has a large number of events associated with it, a warning appears stating that the table will take time to load and may exceed memory capacity.



Time	Router	Operation	Neighbor/ Prefix	Attributes	Area or AS
2004-05-04 04:02:47.310021	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 1 (Area External)	A2CorpNet.OSPF/0.0.0.1
2004-05-04 04:02:47.989836	24.0.0.5	Change Prefix	192.168.107.0/24	Metric: 1 (Area External)	A2CorpNet.OSPF/0.0.0.1
2004-05-04 09:04:38.501263	192.168.0.125	Add Router		Type: Internal Router	A2CorpNet.OSPF/0.0.0.1
2004-05-04 09:04:38.501263	192.168.0.2 DR	Add Neighbor	192.168.0.125	Metric: 0	A2CorpNet.OSPF/0.0.0.1
2004-05-04 09:04:43.797420	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 2 (Area External)	A2CorpNet.OSPF/0.0.0.1
2004-05-04 09:04:43.797420	24.0.0.5	Change Prefix	192.168.107.0/24	Metric: 2 (Area External)	A2CorpNet.OSPF/0.0.0.1
2004-05-04 09:04:48.737236	24.0.0.5	Change Prefix	192.168.107.0/24	Metric: 1 (Area External)	A2CorpNet.OSPF/0.0.0.1
2004-05-04 09:04:49.213503	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 1 (Area External)	A2CorpNet.OSPF/0.0.0.1
2004-05-04 11:02:48.760369	192.168.0.30	Add Router		Type: Internal Router	A2CorpNet.OSPF/0.0.0.1
2004-05-04 11:02:48.760369	192.168.0.2 DR	Add Neighbor	192.168.0.30	Metric: 0	A2CorpNet.OSPF/0.0.0.1
2004-05-04 11:58:38.621902	192.168.0.30	Drop Router		Type: Internal Router	A2CorpNet.OSPF/0.0.0.1
2004-05-04 11:58:38.621902	192.168.0.2 DR	Drop Neighbor	192.168.0.30	Metric: Down	A2CorpNet.OSPF/0.0.0.1
2004-05-04 11:58:58.686398	192.168.0.30	Add Router		Type: Internal Router	A2CorpNet.OSPF/0.0.0.1
2004-05-04 11:58:58.686398	192.168.0.2 DR	Add Neighbor	192.168.0.30	Metric: 0	A2CorpNet.OSPF/0.0.0.1
2004-05-04 12:02:58.625271	192.168.0.56	Drop Router		Type: Internal Router	A2CorpNet.OSPF/0.0.0.1
2004-05-04 12:02:58.625271	192.168.0.2 DR	Drop Neighbor	192.168.0.56	Metric: Down	A2CorpNet.OSPF/0.0.0.1
2004-05-04 12:03:48.620590	192.168.0.30	Drop Router		Type: Internal Router	A2CorpNet.OSPF/0.0.0.1
2004-05-04 12:03:48.620590	192.168.0.2 DR	Drop Neighbor	192.168.0.30	Metric: Down	A2CorpNet.OSPF/0.0.0.1
2004-05-04 12:37:48.712315	192.168.0.30	Add Router		Type: Internal Router	A2CorpNet.OSPF/0.0.0.1
2004-05-04 12:37:48.712315	192.168.0.2 DR	Add Neighbor	192.168.0.30	Metric: 0	A2CorpNet.OSPF/0.0.0.1
2004-05-04 14:15:43.130004	192.168.0.30	Drop Router		Type: Internal Router	A2CorpNet.OSPF/0.0.0.1
2004-05-04 14:15:43.130004	192.168.0.2 DR	Drop Neighbor	192.168.0.30	Metric: Down	A2CorpNet.OSPF/0.0.0.1
2004-05-04 15:18:19.998687	24.0.0.7	Drop Prefix	192.168.129.0/24	Metric: Down (Area External); Cause: Premature	A2CorpNet.OSPF/0.0.0.1
2004-05-04 15:18:20.038686	24.0.0.11	Change Neighbor	24.0.0.7	Metric: 1 (AS External)	A2CorpNet.OSPF/0.0.0.1
2004-05-04 15:18:20.095164	24.0.0.7	Drop Prefix	86.86.86.0/24	Metric: Down (Area External); Cause: Premature	A2CorpNet.OSPF/0.0.0.1
2004-05-04 15:18:20.095164	24.0.0.7	Drop Prefix	86.86.0.0/24	Metric: Down (Area External); Cause: Premature	A2CorpNet.OSPF/0.0.0.1
2004-05-04 15:18:20.095164	24.0.0.7	Drop Prefix	39.39.39.0/24	Metric: Down (Area External); Cause: Premature	A2CorpNet.OSPF/0.0.0.1

2004-05-04 00:22:46 - 2004-05-04 19:31:20

314 entries

Figure 71 Events List

Events List Controls

Use the **Filter By** drop down list and the **Show** and **Hide** buttons at the top of the *Events* window to filter the results displayed in the events list (see Filtering the Events List on page 213).

The following controls are arranged from left to right across the bottom bar of the *Events* window:

- **Time Range** button – Opens the *Select Time Range* dialog, which allows you to change the time range covered by the Events list. To the right of the icon is a box that indicates the start and end of the current time range.
- **Online Update** button – Refreshes the Events list with events that occurred within the past 10 minutes. This button is disabled when the History Navigator is in History mode.

- ⤓ **Show Current Event**, ■ **Stop Execution**, ▶| **Execute One Event**, and ▶ **Start Execution** buttons – See Moving Time and Executing Events on page 214 for information about using these buttons.
- **Clear** button – Clears all events from the *Events* window. This button is only functional in Online mode.
- **Close** button – Closes the *Events* window.

Event Details

The entries shown in the events list are a generalized representation of the state changes communicated in the routing protocol.

For link-state protocols, these are adjacency changes for neighbors or prefixes that are carried in OSPF Link State Advertisement (LSA) packets or IS-IS Link State Packets (LSP). EIGRP is a distance-vector protocol, so it does not communicate link-state changes directly. However, RAMS determines what link-state changes caused the distance change, and inserts those link-state changes into the events list.

For BGP, peers communicate a stream of prefix (route) announcements and withdrawals. In addition to the events indicating network state changes, entries are inserted in to the events list when RAMS's peering with a neighbor router is established or lost.

Several state changes may be communicated at once within the routing protocol; these are displayed as separate events in the list, but all having the same timestamp. The timestamp is the first of several columns of details that are displayed for each event in the events list as described in Table 6.

Table 6 **Events List Columns**

Name	Description
Time	Date and time of the event.
Router	The router to which the event is related. In OSPF and EIGRP, the router ID is displayed in dotted decimal. For IS-IS, the router is identified by SysID, the unique value that is programmed into the router. The router name is shown for protocols that provide it.

Operation	The operation can be Add, Drop, or Change of a Router, a Neighbor, a Prefix, or a RexPeering. For EIGRP, the operation can also be an EIGRP Update or an Unresolved EIGRP Change. For BGP, the operation may be Open or Close of the peering, or Announce or Withdraw of a prefix.
Neighbor/Prefix	Displays either the neighbor router for neighbor operations or the prefix for prefix operations.
Attributes	Displays the affected attributes of the router or prefix.
Area or AS	The OSPF area, IS-IS level, or EIGRP or BGP AS where the event took place.

The format of the *Attributes* column will vary depending on the protocol and the event type, but generally includes details such as the type of a router or the metric to a prefix or neighbor.

For example, starting at the first event in the list shown in Figure 71, router 24.0.0.11 changes its metric for prefix 192.168.116.0/24 to 1, and then, in subsequent Change Prefix events, changes its metric to 2 and back to 1. In the *Attributes* column, the type of the prefix, Area External, indicates that this prefix is being redistributed by router 24.0.0.11 in its role as an Area Border Router. The highlighted Add Router event in the middle of the list indicates that a new router 192.168.0.30 of type Internal (meaning, not a border router) is being added to the routing topology. This event was implicitly generated as a result of the next event in which router 192.168.0.2, acting as Designated Router (DR) for its subnet, added router 192.168.0.30 as a neighbor with metric 0. (The metric from a pseudonode to a router is always 0). About 56 minutes later, the adjacency was dropped and the router along with it.

There are many different possible combinations of event operations and attributes. While the event list format is generalized to allow a consistent representation in multiprotocol networks, there are some protocol-specific characteristics due to the differences in nomenclature and behavior of the protocols:

- OSPF: In the *Router* column, the letters “DR” (Designated Router) following a router address or DNS name indicate events pertaining to the pseudonode representing a LAN subnet. These letters may appear in the *Router* column for events originated by the Designated Router in its role as the DR for the LAN (versus its role as an individual router). The letters may also appear in the *Neighbor/Prefix* column for events for which that column lists the neighbor router, such as an Add Neighbor event, which indicates that the router sending the event has added an adjacency to the pseudonode represented by the DR.

The router types are Internal, Area BR (Area Border Router), ASBR (Autonomous System Border Router), a combination of these, or LAN Pseudo-Node. The prefix metric type is Internal if not explicitly identified as one of Area External, AS External Comparable (Type 1), or AS External (Type 2). The *Attributes* column for a Drop Prefix or Drop Neighbor event may indicate "Cause: Expired" if the router's prefix advertisement has been timed out without a refresh, or "Cause: Premature" when the router advertises a graceful withdrawal (for example, on shutdown). For protocol details, see the following RFCs:

— RFC 2328, OSPF Version 2

— RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option

- IS-IS: Since IS-IS is a link-state protocol like OSPF, the event list details are similar. Routers are identified by a 7-byte hexadecimal SystemID in the form C0A8.00E0.0000.00, or by a name communicated within the protocol. The 7th byte of the SystemID is non-zero when a router is acting as the Designated Router for a LAN. Different values of this byte distinguish different subnets. In the *Router* column the Designated Router is indicated by the SystemID followed by "DR" or by the router name followed by a period, the hexadecimal subnet byte, and "DR". RAMS labels an IS-IS router that is just in level 1 or level 2 as "Internal", while a router that participates in both level 1 and level 2 as "Area BR". Nodes representing subnets are labeled "LAN Pseudo-Node". The prefix metric type is Internal unless explicitly identified as External or TE (Traffic Engineering). For protocol details, see the following RFCs:

  — ISO 10589, or RFC 1142 (ISO 10589 draft), OSI IS-IS Intra-Domain Routing Protocol

  — RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments

  — RFC 2763, Dynamic Hostname Exchange Mechanism for IS-IS

  — RFC 3784, IS-IS Extensions for Traffic Engineering

- EIGRP: Since EIGRP is a distance-vector protocol, the only routing events recorded directly from the protocol are EIGRP Update events, which tell the distance from one of RAMS's peer routers to a prefix. These events are obtained from EIGRP Update and EIGRP Query packets.

  The distance is measured in the EIGRP metric with two components:

  — Inverse bandwidth (bw)

  — Delay (dly).

  The prefix metric type is Internal, if it is not specified. For External prefixes, the originating router is identified. Several special-case prefix types are identified:

  — Loopback, the prefix of a loopback interface

  — Dialup, a /32 prefix that is contained within a less-specific prefix advertised by the same router

  — Auto-Summary and Manual Summary

  — Static prefixes that are redistributed in EIGRP

  RAMS analyzes the EIGRP Update events to determine what link-state changes caused the EIGRP distances to change, then issues CLI queries to the affected routers to verify the change. One or more link-state events are then synthesized and recorded in the routing topology database.

  The basic link-state events have the same format as OSPF and IS-IS events: Add/Drop of Router/Neighbor/Prefix. In addition, for the EIGRP protocol the database records other changes in the routing configuration that are learned through CLI queries to the routers: Add/Drop of Route Filter, Route ACL, or Static Route. These events are interspersed with the EIGRP Update events. Since the analysis may take tens of seconds, the link-state events will appear later in the events list than the EIGRP Update events.

  In case the analysis of EIGRP Updates cannot determine what link-state change was the cause, an Unresolved EIGRP Change event will be written to the database. The *Attribute* column gives the reason:

  — Unknown path – Due to the nature of the EIGRP metric, it is possible, although rare, that the changed state of a link not on the shortest path between two end points will affect the choice of that path. RAMS cannot infer the link change in this case.

  - Not on old path; new path broken – If RAMS's internal routing topology model has become inaccurate, perhaps due to a previous Unresolved EIGRP Change, the analysis algorithm may not be accurately locate the shortest path between two nodes. If this happens, RAMS will not be able to infer a link failure that partitions some nodes from RAMS's viewpoint.
  - Query failed – RAMS's query to the problematic node failed, perhaps because the node itself became unreachable or was busy, so the link state is unknown.
  - Unexpected value – The analysis algorithm lost track while inferring a topology change. This may happen for various reasons; for example, while tracing a changed route, the route may change again.
  - Fast route flap – The link state changed back before the change could be verified to have existed.

  When RAMS detects a route that appears to be stuck in active state, it follows the stuck route until it gets to the last responding router before the nonresponding router. The table entry for this event (*EIGRP Stuck in Active*) identifies the router waiting for the nonresponding router to communicate, and the *Attribute* column reports the statistics from the *show ip eigrp neighbor* command on the last responding router on the route about the nonresponding router. The cause of this event could be that the nonresponding router is down but has not yet been reported down by its neighbor.

  Since EIGRP is a Cisco proprietary protocol, there is no RFC to specify the protocol. Documentation for EIGRP is available on the Cisco web site:

  - **http://www.cisco.com/warp/public/103/eigrp-toc.html**

- BGP: The set of event operations for BGP is small: Open or Close of a peering, or Announce or Withdraw of a prefix. However, the number of different attributes is much larger than for IGP events: AS Path, Local-Pref, MED, Communities, Next Hop, Originator ID, Cluster List, and Aggregator. For protocol details, see the following RFCs:

  - RFC 1771, BGP Version 4 (this RFC is obsolete and is to be replaced by draft-ietf-idr-bgp4-23.txt)
  - RFC 2796, BGP Route Reflection
  - RFC 1997, BGP Communities Attribute

In addition to the protocol-specific events outlined above, there are Add/Drop RexPeering events that indicate when RAMS established or lost peering with its neighbor router. Routing topology changes cannot be recorded when the peering is lost.

Highlighting Associated Nodes

Selecting an event in the list highlights that entry in reverse color, as shown for the *Drop Prefix* event at 15:18:19 in Figure 71, and also causes any associated nodes to flash on the routing topology map. (If the map is displaying the routing topology at a different time than the time of the event, it is possible that no nodes will flash, because the associated nodes are not present.)

Filtering the Events List

When many events occur during a period of interest, it may be difficult to isolate the events relevant to a particular problem. To make finding the desired events easier, the displayed list of events may be filtered by a wide range of criteria, which differ depending on the protocol represented by the current tab of the *History Navigator* window from which you generated the Events list.

Use the **`Filter By`** drop-down list to select the filter parameters and the **Show** or **Hide** buttons to list only those events that match the filter criteria, or exclude those events that match the filter criteria, respectively.

Some parameters require that you enter a value in a text box (for example, if you filter by router, you must enter the name or IP address of the router in the text box to the right of the *Filter By* list. Other parameters require that you choose one or more items from a list (for example, if you filter by event operation, you are presented with a list of event types from which to choose).

Using Filters on page 226 explains how to combine filter parameters using the **Expressions** option on the filter drop-down list.

See page 227 for information about how to compose complex filters.

Alternatively, you can focus in on events related to a particular node or link on the routing topology map. Right-click on the object of interest to display the node information panel or link information panel (page 132 and page 134, respectively), and then click **Events** on the information panel. A new *Events List* window is displayed showing only the events originated by the selected router or related to adjacency changes on the selected link.

Adjusting the Time Range

The initial time range for the *All Events* list is selected by setting the blue lines on the *History Navigator* Events graph, as described in steps 2 and 3 on page 2206. You can adjust the time range as needed.

To adjust the start and end of the time range, do the following:

1. Click 🕒 located in the lower left-hand corner of the *Events* window to display the *Set Time Range* dialog.
2. You can then adjust the time range in any of the following ways:
   - Type new values into the *From* and *To* fields, or adjust the values with the up and down triangle buttons.
   - Select one of the predefined time ranges from the **Select Time Range** menu: one hour, day, week or month. The time range will be centered around the currently displayed point in time.
   - Select **Recent** from the **Select Time Range** menu. This displays a drop-down list of recently used time ranges from which you can select.
   - Select **All** from the **Select Time Range** menu to include all events recorded in the database.
3. Click **OK** to accept the adjusted time range.

Caution If the time period selected has a large number of events associated with it, a warning appears stating that the table will take time to load and may exceed memory capacity.

Moving Time and Executing Events

The current time for the routing topology map may be moved to the time of any event in the list so that the map shows the state of the network at the time just before the event occurred.

If you right-click an event in the list, its text temporarily changes to blue, and a pop-up dialog asks if you want to move time to before or after that event. When you choose an option, the event text changes to green to indicate that it is the next event to be executed. In the example events list shown in Figure 71, the next event is the *Add Router* event at 11:02:48.

Click ▶ **`Start Execution`** to execute events one after another starting with the next event and continuing to the last event in the Events list, and observe their effect on the network. During execution, the routing topology map marks nodes or links that go DOWN as a result of event execution with a red cross (✕), while nodes and links that change state to UP are marked with a green dot (●). When an EIGRP Update event is executed, indicating a change in the distance to a prefix, the routers to which that prefix is attached are marked with a blue dot (●). As each event is executed, the text for the next event in the list turns green and the current time for the routing topology map advances as shown by the green time cursor moving to the right on the Events graph in the *History Navigator* window. To stop the execution, click ■ **`Stop Execution`**.

Click ▶| **`Execute One Event`** to execute events one at a time and observe their effect on the network.

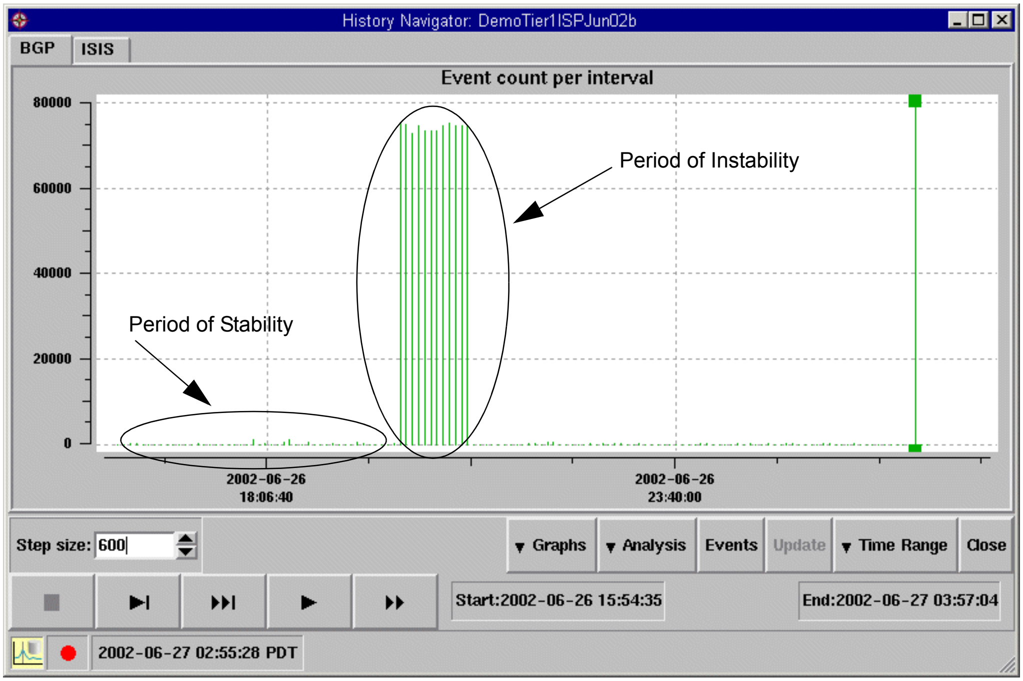
Conversely, you can drag the time cursor to any point of interest on the time line. This displays the state of the network corresponding to that point in time in the routing topology map. There are three possible situations:

- If the time cursor is within the time range covered by the events list (between the blue lines), you can click ⤓ **`Show Current Event`** to quickly find the next event to be executed. The next event, highlighted by green text, scrolls to the top of the list.
- If the time cursor is earlier than the start of the time range of the events list, the next event to be executed is the first event in the list. The time cursor jumps to the time of the first event if it is executed.
- If the time cursor is later than the end of the time range, the **Show Current** and **Execute** buttons are disabled and no event is highlighted by green text.

Example: Using the History Navigator as a Forensic Tool

When diagnosing a network outage or performing forensic analysis after an outage, having complete historical data and analysis capability is invaluable. RIB Browser Comparison on page 199 showed how the History Navigator displays event churn in a time line and analyzes the state of the RIB before and after network churn. This section provides an example of the steps you can take to use RAMS to help to narrow down the event churn to its root cause.

In the example shown in Figure 72, a period of instability (a high level of churn) lasts for more than an hour. Using the History Navigator's Event Analysis tool, you can focus on a small part of the total churn period.



Step size: 600

Start:2002-06-26 15:54:35

End:2002-06-27 03:57:04

2002-06-27 02:55:28 PDT

Figure 72 Stability and Instability

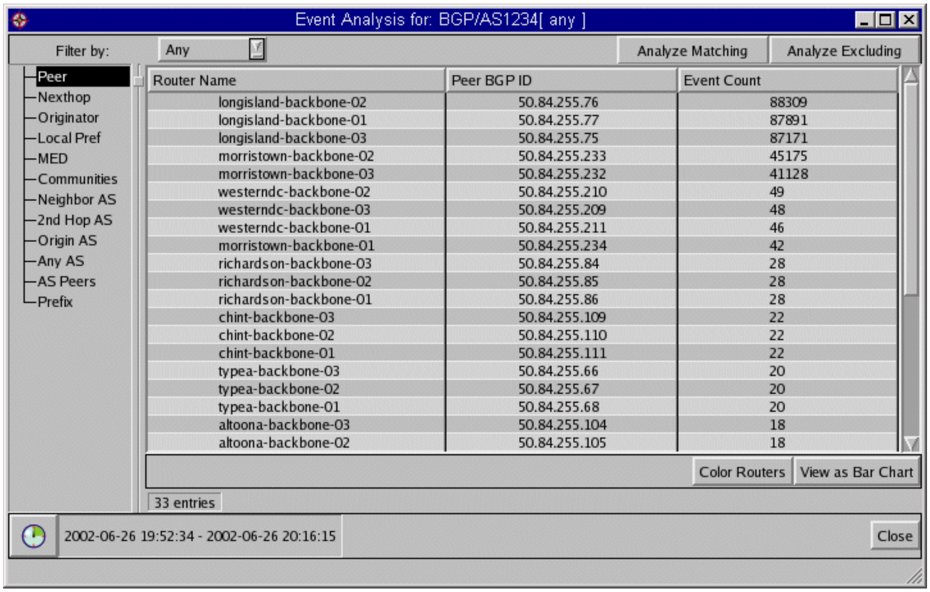
To perform an events analysis, perform the following steps:

1 Click **Analysis** in the *History Navigator* window.

2 Select **Event Analysis** from the pop-up menu that appears.

3 Mark the start and end time for the analysis using the blue cross-hairs.

The *Event Analysis* window appears, as shown in Figure 73.



Event Analysis for: BGP/AS1234[any]

Filter by: Any

Router Name	Peer BGP ID	Event Count
longisland-backbone-02	50.84.255.76	88309
longisland-backbone-01	50.84.255.77	87891
longisland-backbone-03	50.84.255.75	87171
morristown-backbone-02	50.84.255.233	45175
morristown-backbone-03	50.84.255.232	41128
westerndc-backbone-02	50.84.255.210	49
westerndc-backbone-03	50.84.255.209	48
westerndc-backbone-01	50.84.255.211	46
morristown-backbone-01	50.84.255.234	42
richardson-backbone-03	50.84.255.84	28
richardson-backbone-02	50.84.255.85	28
richardson-backbone-01	50.84.255.86	28
chint-backbone-03	50.84.255.109	22
chint-backbone-02	50.84.255.110	22
chint-backbone-01	50.84.255.111	22
typea-backbone-03	50.84.255.66	20
typea-backbone-02	50.84.255.67	20
typea-backbone-01	50.84.255.68	20
altoona-backbone-03	50.84.255.104	18
altoona-backbone-02	50.84.255.105	18

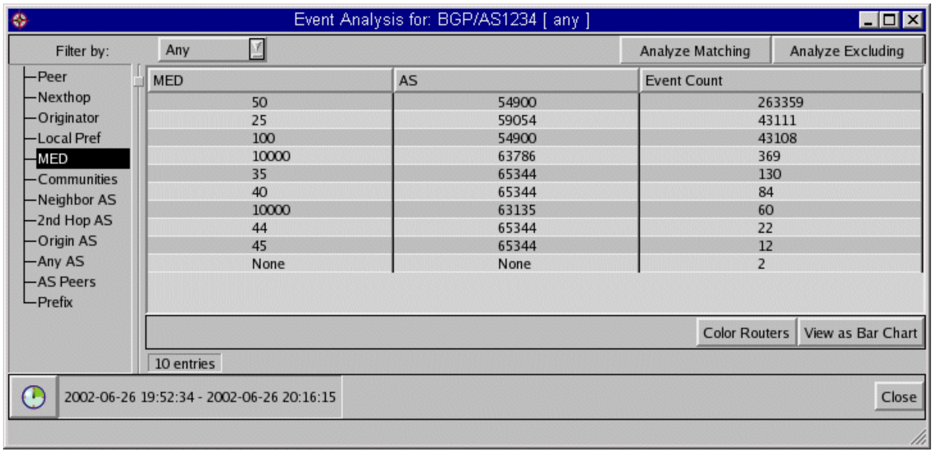
33 entries

2002-06-26 19:52:34 - 2002-06-26 20:16:15

Figure 73 Event Analysis Window

The *Event Analysis* table can be filtered, sorted by column heading, or viewed as a bar chart.

When the **MED** option is selected, a small number of MEDs (three in this example) have a large number of events associated with them, as show in Figure 74. This could represent a MED oscillation.



Event Analysis for: BGP/AS1234 [any]

Filter by: Any

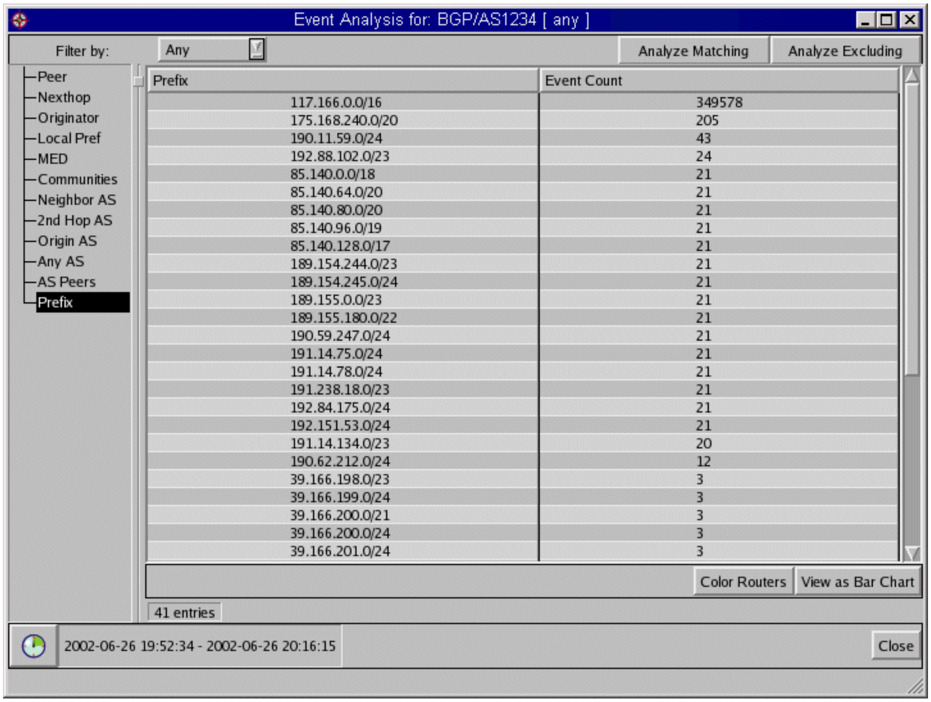
MED	AS	Event Count
50	54900	263359
25	59054	43111
100	54900	43108
10000	63786	369
35	65344	130
40	65344	84
10000	63135	60
44	65344	22
45	65344	12
None	None	2

10 entries

2002-06-26 19:52:34 - 2002-06-26 20:16:15

Figure 74 MEDs

To identify the prefixes affected by this possible MED oscillation, select the **`Prefix`** tab as shown in Figure 75.



Event Analysis for: BGP/AS1234 [any]

Filter by: Any

Prefix	Event Count
117.166.0.0/16	349578
175.168.240.0/20	205
190.11.59.0/24	43
192.88.102.0/23	24
85.140.0.0/18	21
85.140.64.0/20	21
85.140.80.0/20	21
85.140.96.0/19	21
85.140.128.0/17	21
189.154.244.0/23	21
189.154.245.0/24	21
189.155.0.0/23	21
189.155.180.0/22	21
190.59.247.0/24	21
191.14.75.0/24	21
191.14.78.0/24	21
191.238.18.0/23	21
192.84.175.0/24	21
192.151.53.0/24	21
191.14.134.0/23	20
190.62.212.0/24	12
39.166.198.0/23	3
39.166.199.0/24	3
39.166.200.0/21	3
39.166.200.0/24	3
39.166.201.0/24	3

41 entries

2002-06-26 19:52:34 - 2002-06-26 20:16:15

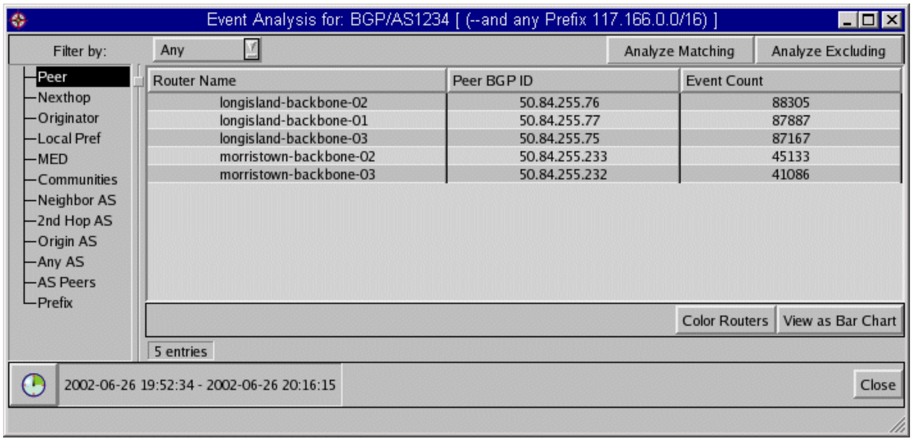
Figure 75 Prefix Details

A single prefix has a huge number of events associated with it. You can drill down to determine which BGP peers have generated these events by filtering the analysis to include just these events, and then observing the peers involved.

To drill down and view details, perform the following:

1. Right-click the prefix in question.
2. Click **`Filter Analysis`** in the pop-up window that appears.

   Figure 76 displays the results of the drill-down filter analysis.



Event Analysis for: BGP/AS1234 [(--and any Prefix 117.166.0.0/16)]

Filter by: Any

Router Name	Peer BGP ID	Event Count
longisland-backbone-02	50.84.255.76	88305
longisland-backbone-01	50.84.255.77	87887
longisland-backbone-03	50.84.255.75	87167
morristown-backbone-02	50.84.255.233	45133
morristown-backbone-03	50.84.255.232	41086

5 entries

2002-06-26 19:52:34 - 2002-06-26 20:16:15

Figure 76 Filtered Event Distribution

It appears that five peers have generated the majority of events. This increases the suspicion of a MED oscillation. To confirm this suspicion, you should look at the actual events in question in more detail.

Many routing instabilities are caused by interactions between multiple routers and are very difficult to isolate because routers do not keep an event history. Diagnosis of the outage can require login to multiple routers and the execution of *show ip bgp...* commands – a very tedious and time-consuming task.

RAMS's RIB analysis identified the possibility of a MED oscillation, and

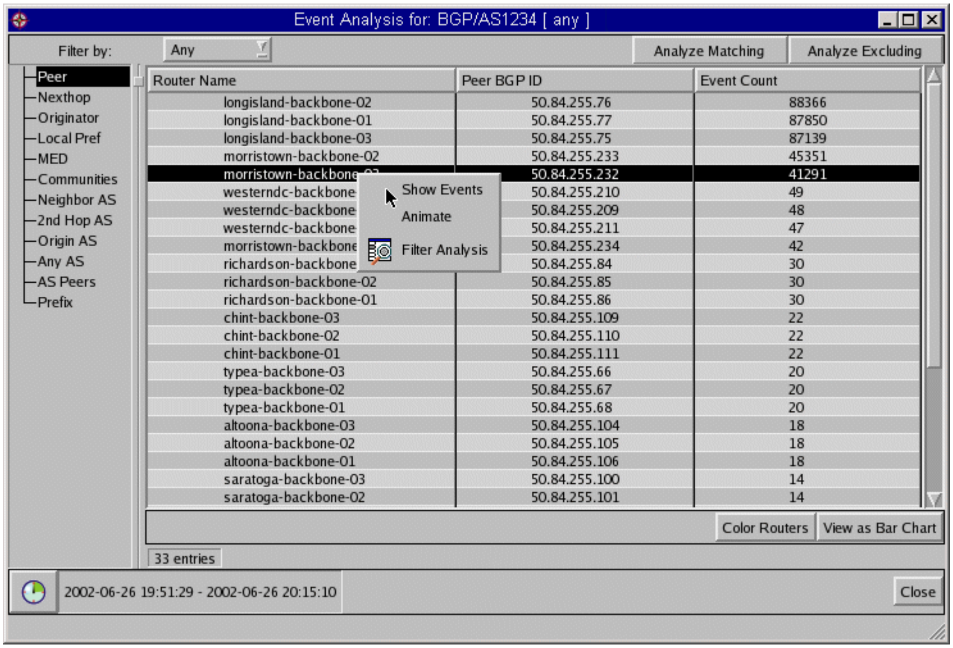
RAMS's Event Analysis identified the exact prefix and the peers involved in the oscillation. The following procedures show how you can confirm the exact cause of the problem by looking at the events list.

To view the events associated with a particular problem, perform the following steps:

1 In the *History Navigator* window, click **`Analyze,`** and then select **`Event Analysis`** from the pop-up menu that appears.

2 Select the desired start and end times with the blue cross-hairs.

3 To view the events associated with an individual table entry, right-click the entry, and then select **`Show Events`** in the pop-up menu that appears, as shown in Figure 77.



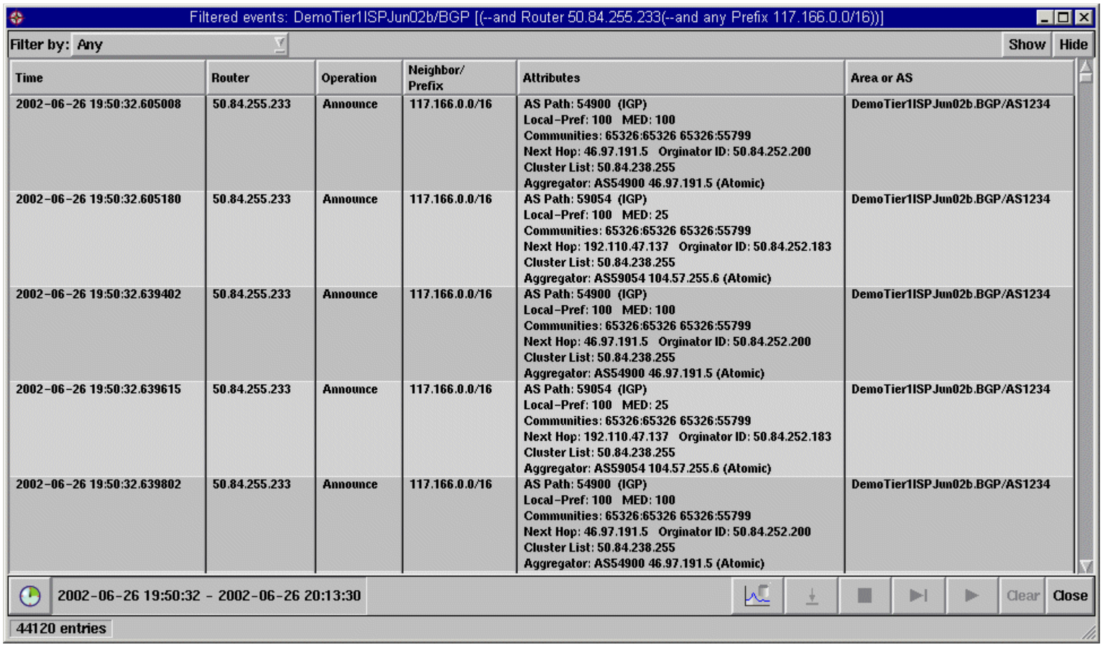
Router Name	Peer BGP ID	Event Count
longisland-backbone-02	50.84.255.76	88366
longisland-backbone-01	50.84.255.77	87850
longisland-backbone-03	50.84.255.75	87139
morristown-backbone-02	50.84.255.233	45351
morristown-backbone	50.84.255.232	41291
westerndc-backbone	50.84.255.210	49
westerndc-backbone	50.84.255.209	48
westerndc-backbone	50.84.255.211	47
morristown-backbone	50.84.255.234	42
richardson-backbone	50.84.255.84	30
richardson-backbone-02	50.84.255.85	30
richardson-backbone-01	50.84.255.86	30
chint-backbone-03	50.84.255.109	22
chint-backbone-02	50.84.255.110	22
chint-backbone-01	50.84.255.111	22
typea-backbone-03	50.84.255.66	20
typea-backbone-02	50.84.255.67	20
typea-backbone-01	50.84.255.68	20
altoona-backbone-03	50.84.255.104	18
altoona-backbone-02	50.84.255.105	18
altoona-backbone-01	50.84.255.106	18
saratoga-backbone-03	50.84.255.100	14
saratoga-backbone-02	50.84.255.101	14

33 entries

2002-06-26 19:51:29 - 2002-06-26 20:15:10

Figure 77 Show Details Button

The *Filtered Events* window appears, as shown in Figure 78. This window lists all of the events associated with the selected table entry.


Filtered events: DemoTier1ISPJun02b/BGP [(--and Router 50.84.255.233(--and any Prefix 117.166.0.0/16))]
Show
Hide
Clear
Close

Filter by: Any

Time	Router	Operation	Neighbor/ Prefix	Attributes	Area or AS
2002-06-26 19:50:32.605008	50.84.255.233	Announce	117.166.0.0/16	AS Path: 54900 (IGP) Local-Pref: 100 MED: 100 Communities: 65326:65326 65326:55799 Next Hop: 46.97.191.5 Orginator ID: 50.84.252.200 Cluster List: 50.84.238.255 Aggregator: AS54900 46.97.191.5 (Atomic)	DemoTier1ISPJun02b.BGP/AS1234
2002-06-26 19:50:32.605180	50.84.255.233	Announce	117.166.0.0/16	AS Path: 59054 (IGP) Local-Pref: 100 MED: 25 Communities: 65326:65326 65326:55799 Next Hop: 192.110.47.137 Orginator ID: 50.84.252.183 Cluster List: 50.84.238.255 Aggregator: AS59054 104.57.255.6 (Atomic)	DemoTier1ISPJun02b.BGP/AS1234
2002-06-26 19:50:32.639402	50.84.255.233	Announce	117.166.0.0/16	AS Path: 54900 (IGP) Local-Pref: 100 MED: 100 Communities: 65326:65326 65326:55799 Next Hop: 46.97.191.5 Orginator ID: 50.84.252.200 Cluster List: 50.84.238.255 Aggregator: AS54900 46.97.191.5 (Atomic)	DemoTier1ISPJun02b.BGP/AS1234
2002-06-26 19:50:32.639615	50.84.255.233	Announce	117.166.0.0/16	AS Path: 59054 (IGP) Local-Pref: 100 MED: 25 Communities: 65326:65326 65326:55799 Next Hop: 192.110.47.137 Orginator ID: 50.84.252.183 Cluster List: 50.84.238.255 Aggregator: AS59054 104.57.255.6 (Atomic)	DemoTier1ISPJun02b.BGP/AS1234
2002-06-26 19:50:32.639802	50.84.255.233	Announce	117.166.0.0/16	AS Path: 54900 (IGP) Local-Pref: 100 MED: 100 Communities: 65326:65326 65326:55799 Next Hop: 46.97.191.5 Orginator ID: 50.84.252.200 Cluster List: 50.84.238.255 Aggregator: AS54900 46.97.191.5 (Atomic)	DemoTier1ISPJun02b.BGP/AS1234

2002-06-26 19:50:32 - 2002-06-26 20:13:30

44120 entries

Figure 78 Filtered Events Window

The final step is to use the Root Cause Analysis function to distill this event information down to its root cause and display an animation of the events, so you can visualize the events as they occurred. This procedure is based upon the History Navigator example shown in Figure 72.

To perform a Root Cause Analysis, do the following:

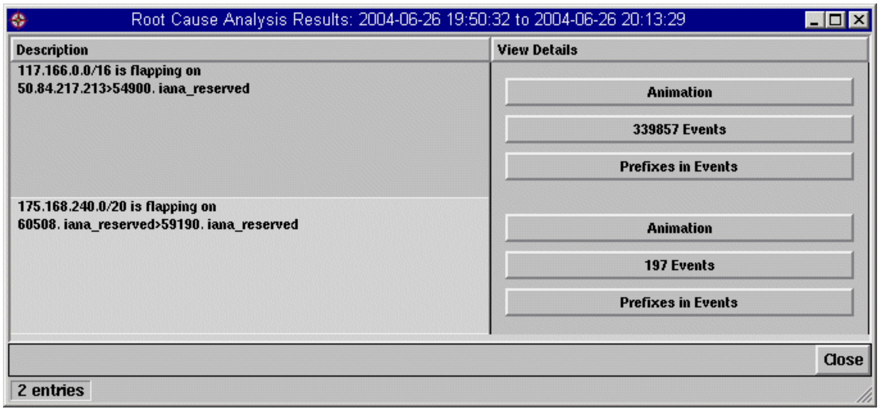
1 In the *History Navigator* window, select **`Root Cause Analysis`** from the Analysis menu.

2 Right-click just before the period of instability and again just after the period of instability to specify the time-frame of the analysis.

The *Root Cause Analysis* window appears, as shown in Figure 79. The window indicates that several prefixes are flapping, at least one of which is generating a very large number of events.

3 Click the **`Animation`** button for that prefix.

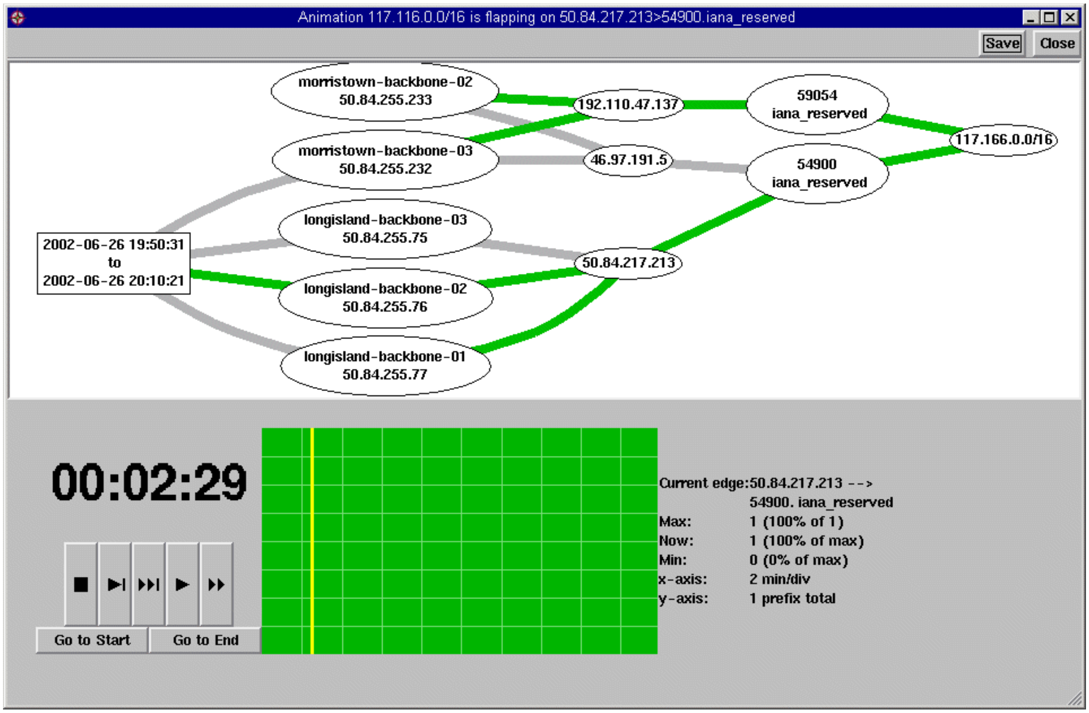
An *Animation* window appears, as shown in Figure 80. Playing the animation shows the network disturbance as it occurs. See Root Cause Analysis on page 188 for information about playback controls, the graph, and the procedures for manipulating the animation display.



Root Cause Analysis Results: 2004-06-26 19:50:32 to 2004-06-26 20:13:29

Description	View Details
117.166.0.0/16 is flapping on 50.84.217.213>54900. iana_reserved	Animation 339857 Events Prefixes in Events
175.168.240.0/20 is flapping on 60508. iana_reserved>59190. iana_reserved	Animation 197 Events Prefixes in Events

Figure 79 Root Cause Analysis Window



```
Current edge:50.84.217.213 -->
             54900. iana_reserved
Max:         1 (100% of 1)
Now:         1 (100% of max)
Min:         0 (0% of max)
x-axis:      2 min/div
y-axis:      1 prefix total
```

Figure 80 Root Cause Analysis Animation Window

The thickness of the grey lines indicate the maximum number of prefixes that were ever carried on each edge. Green lines indicate edges that are gaining prefixes. It is apparent that several of the backbone nodes experienced a high degree of instability, causing the routes to prefix 117.166.0.0/16 to flap. This information helps you to narrow down the possible sources of the instability to just a few nodes.

Correlating Time Series Data

RAMS extends the power of routing navigation by letting you import and display external time series data such as link utilization or jitter measurements in correlation with the state of the network at the routing layer. This makes it easier to identify the cause and effect of events visually by having all of the data on one screen. As routing data is played back from the RAMS database to visualize changes in routing, a time cursor simultaneously steps along the time line graph of the external time series data. The time series data correlation feature provides an unprecedented visualization and analysis capability. Intermittent and intractable problems can be approached from a new perspective and analyzed within seconds or minutes, rather than hours.

One popular source of time series data is the Multi Router Traffic Grapher (MRTG), a free tool that monitors the traffic load on network links. MRTG generates HTML pages that contain PNG graph images providing a live visual representation of this traffic. You can use MRTG graphs as a way of monitoring the health and status of your network. When an anomaly appears, importing the graph data into RAMS and performing a time correlation with routing events can help diagnose the root cause of the anomaly.

RAMS can import data in MRTG ASCII `.log` file format, Round Robin Database (RRDtool) `.rrd` binary format, and a simple, generic ASCII time series format called *graf* file format. The *graf* format consists of two floating-point numbers on each line; the first is the time coordinate and the second is the data value corresponding to that time. The first line of the graf file can optionally be a '#' character followed by a title for the graph.

Any external event data (jitter, packet loss, traffic statistics, server statistics, and so on) can be viewed if it can be transformed with text processing tools into graf format. Data exported from a two-column spreadsheet in tab-separated `.csv` format is one suitable source.

To view a time series data file, it must be uploaded to the RAMS appliance. The Administrator must first enable the FTP server on the RAMS appliance (see Configuring the FTP Server on page 48).

To upload files to the RAMS, proceed as follows:

1 FTP to the RAMS appliance using the IP address of the appliance.

2 Log in as user `rexftp`. The administrator sets the password.

3 Change directory to `pub`.

4 Transfer one or more files to the RAMS appliance.

To display a time series file (all formats), proceed as follows:

1 Select **`Correlate Time Series`** from the Tools menu.

2 Select the file to be displayed, and then click **`Select`**.

The time series graph is displayed in a separate window.

The green cursor in the time series graph is time-aligned with the cursor in the *History Navigator* and any other time series graphs already displayed. Moving the cursor in any displayed time series graph moves it in the others. If you move the cursor, the routing topology map updates to display the state of the network at the time indicated by the cursors.

Note If the time interval covered by a graph does not include the point in time chosen by moving a cursor in another window, the cursor for the first graph will be positioned either at the beginning or end of its timeline, whichever is closer to the chosen time. In this case, the cursors will not all be positioned at the same time.

Displaying MRTG data

MRTG files contain four datasets for the average and maximum bytes/second input and output on a network interface. The four datasets are displayed together in one graph window.

Using Filters

A filter feature is provided on several tables, including the RIB Browser and Events List, to allow you to focus in on items of interest. Figure 81 shows an example of the *Filter by* drop-down list on the *Events* window for BGP. Note that the items in the list differ depending on the current routing protocol.

The filter feature offers three levels of filtering:

- Simple filters let you choose a single operator (for example, “router”) from a list and specify one or more parameters (for example, router IP addresses or names) to be matched or excluded. See Expression Definitions on page 229 for examples of the parameter syntax as illustrated using filter expressions. (Note that with a simple filter, you enter only the parameter; the operator is selected from a list.)

  The filter is translated internally into a filter expression combining the filter operator with the parameters. Figure 82 shows an example of a filter specifying a router address.

- Advanced filters let you choose two or more different operators from a list and specify their corresponding parameters to be matched or excluded.

- Filter expressions let you manually enter a filter expression that is too complex to be set up with either simple or advanced filter menus.

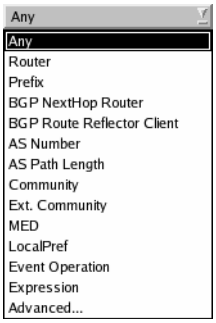


Figure 81 Filter By Drop Down List

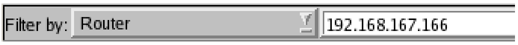
In many cases, the built-in **Filter by** selections, such as the ones shown in Figure 81, provide sufficient flexibility in filtering. For example, the `Router` filter accepts a list of router addresses or names when several specific routers are of interest.

To set up a simple filter, perform the following steps:

1 Select an operator from the **`Filter by`** drop-down list. For example, assume you want to see only events reported by a node whose IP address is 192.168.167.166. Select **`Router`** in the **`Filter by`** drop-down list.

A text box appears to the right of the **`Filter by`** parameter.

2 Enter the address of the node in the text box.



Filter by: Router 192.168.167.166

Figure 82 Parameter Text Box

3 Click **`Show`** to list only items that match the address, or click **`Hide`** to list only items that do not match the address.

To set up an advanced filter, perform the following steps:

1 Select **`Advanced`** from the **`Filter by`** drop-down list.

The *Advanced Filter* window appears, as shown in Figure 83.

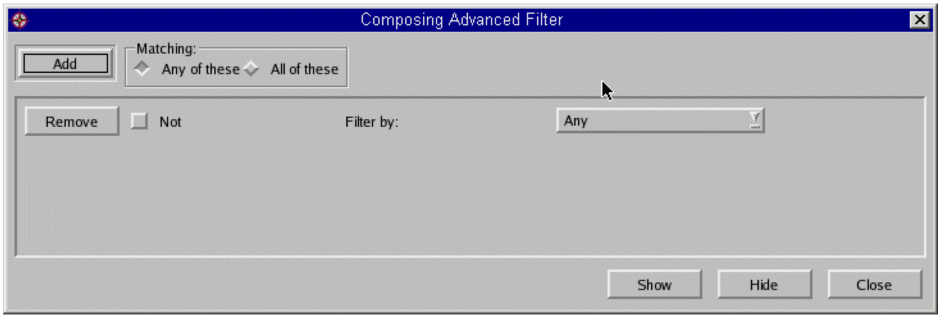


Figure 83 Advanced Filter Window

2 In the *Advanced Filter* window, select a filter operator from the **`Filter by`** drop-down list.

Some operators require that you enter the parameter in a text box, others let you choose among items in a list.

3 Specify the appropriate parameter, either by typing it into a text box or choosing it from a list, depending upon the operator.

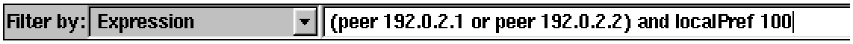
4. To exclude matching items, click **Not** for that operator.
5. To add another operator to the filter, click **Add** in the upper left corner of the window. Then repeat steps 2 through 4 to define the parameters for the new operator.
6. After you have added the desired filter operators (and their corresponding parameters), choose an option from the *Matching* box:
   - **Any of these** includes an item if it matches any one of the filter criteria.
   - **All of these** includes an item only if it matches every filter criteria.
7. Click **Show** to list all events that match the filter, or click **Hide** to list only events that do not match the filter.

   The filter is translated internally into a filter expression combining the filter operators with the parameters that you specified.

Multiple levels of advanced filters can be combined to construct any logical AND-OR expression you desire.

To enter a filter expression manually, perform the following steps:

1. Select **Expression** from the **Filter by** drop-down list.
2. Enter the desired expression in the adjacent text box. See Expression Syntax on page 228 for information about the syntax used to enter expressions, and Expression Definitions on page 229 for a complete list of operators and examples showing their use.



Filter by: Expression

(peer 192.0.2.1 or peer 192.0.2.2) and localPref 100

Figure 84 Expression Text Box

3. Click **Show** to display only those items that match the filter, or **Hide** to display only those items that do not match.

Expression Syntax

Filter expressions are specified in prefix notation, which means that the filter operator must be placed first with the parameter coming after the operator. An expression may be composed of multiple terms (operators and parameters) to form a complicated filter.

The following syntax rules apply:

- Operators are case-insensitive. Mixed capitalization is used in the examples for clarity.
- Operators and parameters are separated by whitespace.
- Operator `not` has higher precedence than operator `and`, which in turn has higher precedence than operator `or`.
- Parentheses may be used when needed to group subexpressions and override the precedence of operators.

Examples

The following expression is equivalent to selecting the **`Router`** option of the **`Filter by`** menu and supplying the three addresses 10.1.1.1, 10.2.2.2 and 10.3.3.3:

```
router 10.1.1.1 or router 10.2.2.2 or router 10.3.3.3
```

The following expression on the RIB browser would restrict the display to just the portion with BGP peers 192.0.2.1 and 192.0.2.2 that also has LocalPref 100:

```
(peer 192.0.2.1 or peer 192.0.2.2) and localPref 100
```

The previous example demonstrates the use of parentheses. Without them, the display would include the portion of the RIB with BGP peer 192.0.2.1 independent of LocalPref plus the portion of the RIB with both BGP peer 192.0.2.2 and LocalPref 100.

Instead, if the entries with LocalPref 100 were not interesting but other values were, then the expression could be modified as follows:

```
(peer 192.0.2.1 or peer 192.0.2.2) and not localPref 100
```

Expression Definitions

This section defines the filter operators used in RAMS, and also describes the function of each. The three conjunctive operators are listed first, followed by the others in alphabetical order.

not

Used to negate the next operator or parenthesized subexpression in the expression. For example,

```
not router 10.2.2.2
not (router 10.2.2.2 or router 10.3.3.3)
```

and

Requires that both the preceding and following operators in the expression be matched. For example,

```
router 10.1.1.1 and prefix 192.168.5.0/24
```

or

Matches if either the preceding or following operator in the expression matches. For example,

```
peer 10.1.1.1 or peer 10.2.2.2 or peer 10.3.3.3
```

asEdge <from-asn> <to-asn>

Matches an AS edge, meaning, a hop from one AS number to another, anywhere in the AS path. For example,

```
asEdge 1234 5678
```

asPath <asn> [atHead] [atTail]

Matches an AS number anywhere in the AS path, or optionally selects the AS at the head and/or tail. This example matches a singleton path containing only 1234:

```
aspath 1234 atHead atTail
```

asPathLen <n>
asPathLength <n>

Matches an AS path of length n. For example,

```
asPathLen 5
```

bgpState <state>

Matches BGP routes in the specified state with respect to the baseline. The states are as follows:

`bgpState Dead`(not in baseline and dead)
`bgpState Down`(not in baseline and down)

```
bgpState Up(not in baseline but up)
bgpState Down/B(in baseline but down)
bgpState Up/B(in baseline and up)
```

community <x:y>
community <x>

Matches a complete community attribute; it cannot match just the AS or just the value.

```
community 208:888
```

or

```
community 13632376
```

In the first form of notation, *x* is the first two octets (the AS number) and *y* is the second two octets (a value) of the community attribute. In the second form of notation, *x* is a four-octet quantity representing the complete community attribute.

eventType <operation>

Matches an event operation, meaning, a value in the *Operation* column of an events list, one of the following (where "*" is a wildcard to match any value):

```
eventType drop router
eventType add router
eventType change router
eventType drop neighbor
eventType add neighbor
eventType change neighbor
eventType drop prefix
eventType add prefix
eventType change prefix
eventType add rexpeering
eventType drop rexpeering
eventType change rexpeering
eventType drop *
eventType add *
eventType change *
eventType * router
eventType * neighbor
eventType * prefix
eventType * rexpeering
```

The following event types apply to EIGRP only:

```
eventType EIGRP Update
eventType Unresolved EIGRP Change
eventType EIGRP stuck-in-active
eventType start of exploration
eventType end of exploration
eventType drop static
eventType add static
eventType change static
eventType add route filter
eventType drop route filter
eventType change route filter
eventType add route acl
eventType drop route acl
eventType change route acl
eventType * static
eventType * route filter
eventType * route acl
```

The following event types apply to BGP only:

```
eventType open(open connection)
eventType close(close connection)
eventType announce(route announcement)
eventType withdraw(route withdrawal)
```

extCommunity RT:<route_target>
extCommunity SoO:<source_of_origin>

Matches a complete extended community attribute, including the type and all bits of the value. For either route_target or source_of_origin, the value can be expressed as a 16-bit global administrator value (AS number) followed by a 32-bit assigned value, or as a 32-bit value global administrator value, in the form of an IPv4 address or decimal number, followed by a 16-bit assigned value:

```
extCommunity RT:208:888
extCommunity RT:192.0.2.55:7
extCommunity SoO:13632376:123
```

externalOriginator <router>

Matches a router that is the originator of an external prefix in an EIGRP update event, using any of the forms of router identification described above for `router`. For example,

```
externaloriginator 192.168.0.36
```

igpPrefixType <type>

Matches the specified IGP prefix type. The available prefix types include the following:

- OSPF: Internal, AreaExt, ASExt_Type2, or ASExt_Type1
- ISIS: Internal, ASExt_Type2, ASExt_Type1, or TE
- EIGRP: Internal, ASExt_Type2, ASExt_Type1, Loopback, Dialup, AutoSum, ManualSum, StaticInt, StaticExt, NotFoundInt, NotFoundExt

For example, in an OSPF network:

```
igpPrefixType AreaExt
```

localPref <value>

Matches the BGP LocalPref value. For example,

```
localPref 888
```

med <value>

Matches the MED attribute only, and not the neighboring AS:

```
med 987
```

To match both the MED attribute and the neighboring AS, combine both operators:

```
and med 987 neighAS 208
```

neighbor <router>

Matches a neighbor router in an events list using any of the forms of router identification described above for `router`. For example,

```
neighbor labnet-gw
```

neighborAS <asn>
neighAS <asn>

Matches the neighbor (nexthop) AS, meaning, the first AS in an AS path. For example,

```
neighAS 288
```

nexthop <addr>

Matches a BGP Nexthop. For example,

```
nexthop 192.0.2.67
```

noCommunity

Matches a BGP route or event that has no community attribute.

noExtCommunity

Matches a BGP route or event that has no extended community attribute.

noLocalPref

Matches a BGP route or event that has no LocalPref attribute.

noMed

Matches a BGP route or event that has no MED attribute, which is different than a MED value of zero.

noOrig
noOrigin
noOriginator

Matches a BGP route or event that has no Originator ID.

orig <addr>
origin <addr>
originator <addr>

Match a BGP originator ID. For example,

```
originator 192.0.2.4
```

originAS <asn>

Matches the origin AS, meaning, the last AS in an AS path. For example,

```
originAS 289
```

peer <router>

Matches a specific BGP peer address using any of the applicable forms of router identification described above for `router`. For example,

```
peer 192.0.2.3
```

prefix <addr/masklen> [moreSpecifics][lessSpecifics][ge <masklen>][le <masklen>]

Matches a prefix; optionally followed by either or both of the `moreSpecifics` and `lessSpecifics` operators to also display prefixes more or less specific than the given prefix. Alternatively, the prefix can be specified by an address followed by either or both of the operators `ge` or `le` with a mask length to include prefixes with mask lengths greater-than-or-equal or less-than-or-equal to the given integer parameter. For example,

```
prefix 10.2.0.0/16
prefix 10.2.0.0/16 moreSpecifics
prefix 10.2.0.0 ge 16
prefix 10.2.0.0 ge 16 le 24
```

proto <proto>
protocol <proto>

Selects a particular protocol. The available protocols are ISIS, OSPF, EIGRP, BGP and Static (the last currently only available in an EIGRP topology):

```
proto isis
```

router <router>

Matches a specific router using any of the forms of identification that are shown in a table: name, address, prefix (for a LAN pseudonode), or SystemID (for ISIS). An address or name may be followed by "DR" to select the role of a router as the designated router for a subnet. When a router name is given, it matches all routers whose names begin with that string.. For example,

```
router labnet-gw
router 192.168.0.36
router 192.168.0.36/24
router 1921.6800.0036:00
router 192.168.0.36 dr
router labnet-gw:01 DR
```

secondHopAS <asn>

Matches the second hop AS, meaning, the one after the neighbor AS in an AS path. For example,

```
secondHopAS 288
```

staticNexthopType <type>

Matches the specified nexhop type for a static route. The available types are: Network, Interface, Gateway, Default. For example,

```
staticNexthopType Network
```

vpnPrefix <target:addr/masklen> [moreSpecifics][lessSpecifics][ge <masklen>][le <masklen>]

Matches a VPN prefix, which is composed of a route target (RT) plus a prefix; see Configuration on page 264 for a description of RT formats. The prefix is optionally followed by either or both of the `moreSpecifics` and `lessSpecifics` operators to also display prefixes more or less specific than the given prefix. Alternatively, the prefix can be specified by an address followed by either or both of the operators `ge` or `le` with a mask length to include prefixes with mask lengths greater-than-or-equal or less-than-or-equal to the given integer parameter. For example,

```
vpnPrefix 65522:101:10.2.0.0/16
vpnPrefix 65522:101:10.2.0.0/16 moreSpecifics
vpnPrefix 65522:101:10.2.0.0 ge 16
vpnPrefix 65522:101:10.2.0.0 ge 16 le 24
```

7

IGP Reports

RAMS features a comprehensive set of predefined reports that provide a quick, easy-to-understand view of routing events and problems in the network. When you require a report, select the desired time period from the RAMS database and generate a report for this time period. Reports are formatted in HTML and are accessible from the RAMS web server.

This chapter details how to generate IGP reports, describes the data each report provides, and illustrates the situations in which each report is useful.

IGP reports fall into three general categories:

- Summary Reports

  These reports provide a high-level view of network activity over a specified time period. Typically, these reports are run daily to display day-to-day changes and quickly flag potential problems. There are two types of summary reports:

  — Network Events Summary

  — Network Churn

- Drill-Down Reports

Drill-down reports provide in-depth information and are normally run after scheduled maintenance to verify that configuration changes were made correctly. They are also used to pinpoint and troubleshoot network problems once the cause of a problem has been identified. The various types of drill-down reports are:

  - Changed Metrics
  - Flapping Links
  - Prefix Origination Changes
  - New Prefixes
  - New Routers and Links
  - Prefixes Withdrawn

- Inventory Reports

  This group of reports is used to assess the resources available on the network for a certain time period. There are two types of inventory reports:

  - Prefix List
  - Prefix Origination from Multiple Sources

After you install RAMS for the first time, it is a good idea to generate and print all of the reports. This provides an overview of the network status, which is useful for baseline comparison in the future.

Preparing for IGP Reports

Before generating any reports, ensure that the appropriate database is active.

To find out which databases are active, perform the following steps:

1 Open the RAMS application using either X-Windows or VNC.

2 Select `Open Topology` from the Topology menu.

The database list opens.

3 Scroll through the list. Databases with names in green letters are actively recording data.

4 If the desired database is not recording data, ask the administrator to start the recording process for the desired database.

Note For each report, a database is selected from the *Administrative Domain* drop-down list. For database configurations with more than one level of administrative domains, the report will cover all databases sharing the same first-level administrative domain name.

Accessing the IGP Report Pages

To access the report pages, use a browser to connect to the RAMS Web server. Click **`IGP Reports`** and enter your user name and password. Administrator privileges are not required. The *IGP Reports* page appears, as illustrated in Figure 85.

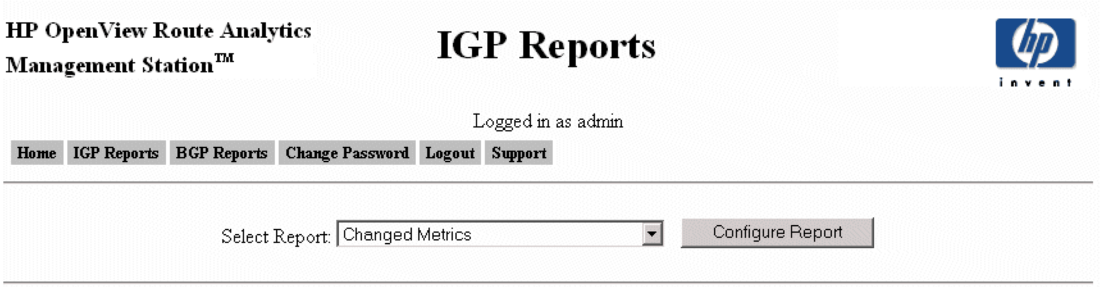


Figure 85 IGP Reports Page

Note Your browser must accept cookies to login.

The *IGP Reports* page contains the *Select Report* drop-down list and the **Configure Report** button.

Available IGP Reports

This section describes the reports available from the *Select Report* drop-down list.

Note In all of the following reports, to change the time period for any report and run it again, click **`Reconfigure Report`** at the bottom of the report page. To run a different report, click the **`IGP Reports`** link to return to the report list and select a different report.

Network Events Summary

The *Network Events Summary* report summarizes network changes. This report presents an overview of network status for a specific period of time and is a good place to start when diagnosing network problems or checking the general network status.

The report displays the following information:

- Number of Link Flaps
- Number of Links with Changed Metrics
- Number of Events
- Number of Prefix Origination Changes
- Number of Prefixes Withdrawn
- Number of New Prefixes Advertised

To configure the Network Events Summary report, do the following:

1. Select **`Network Events Summary`** from the *Select Report* drop-down list, and then click **`Configure Report`**.

   The *Network Events Summary* section appears on the *Reports* page, as shown in Figure 86.

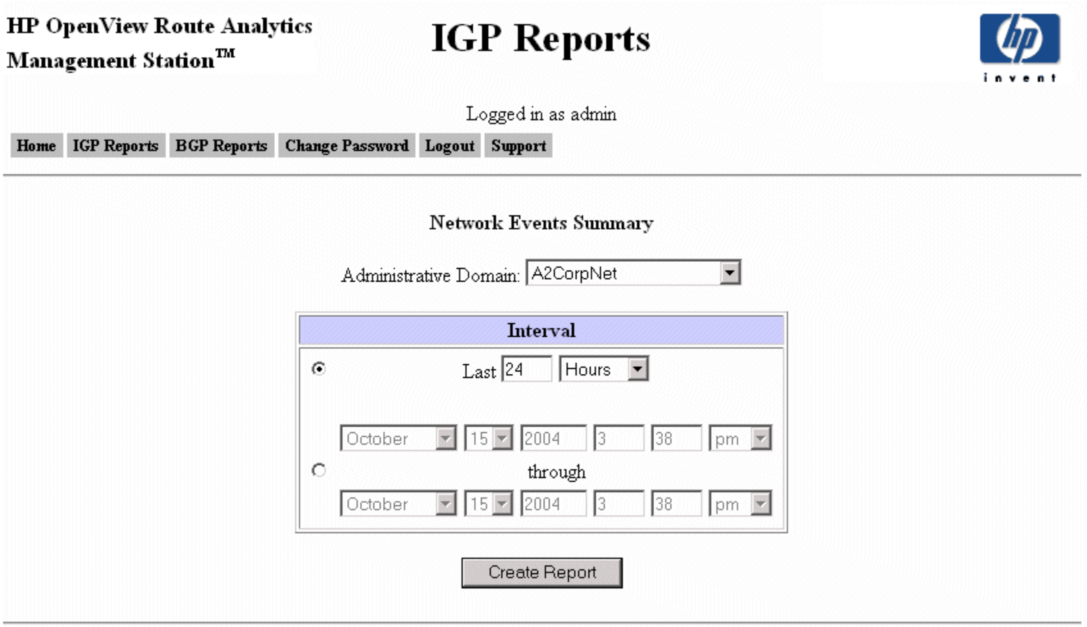
2. Select the desired database from the *Administrative Domain* drop-down list.

3 Specify the time period for the report in the *Interval* section. Check the top radio button to specify a time period up till the current time. Check the bottom radio button to specify an exact start and end time.

4 Click **`Create Report`**.

The time taken to generate a report depends on the input parameters and size of the database. Reports from large databases normally take longer to generate than those from small databases.

A report is generated from the selected database and displayed in a new page. You can use the browser's print command to print a copy of the report.



HP OpenView Route Analytics Management Station™

IGP Reports

Logged in as admin

Network Events Summary

Administrative Domain: A2CorpNet

Interval

● Last 24 Hours

○ October 15 2004 3 38 pm through October 15 2004 3 38 pm

Figure 86 Network Events Summary Section on Reports Page

Understanding the Report

The *Network Events Summary* report contains the fields described in Table 7.

Table 7 Network Events Summary Fields

Field	Description
Number of Link Flaps	The number of times the interface goes up and down.
Number of Links with Changed Metrics	The number of links that have had a metric change.
Number of Events	The number of events recorded in the database.
Number of Prefix Origination Changes	The number of prefixes advertised on a different router.
Number of Prefixes Withdrawn	The number of prefixes that have been withdrawn from the network.
Number of New Prefixes Advertised	The number of prefix advertisements recorded.

Note It is recommended that you run the *Networks Events Summary* report as the first step when trying to identify network problems, because it provides an overall view of network activity. After you identify an area of difficulty, you can run a report that focuses on that area to further assess the problem. For example, if the *Networks Events Summary* report displays a large number of flapping links, run a *Flapping Links* report to further analyze this problem.

Changed Metrics

The *Changed Metrics* report provides a quick summary of all link metrics that have changed in the network. It identifies the router that is advertising the changed metric, along with the original metric, the new metric, and the time when it changed.

This report is normally run after a scheduled maintenance to provide an easy way to verify that planned metric changes have occurred.

To configure the Changed Metrics report, do the following:

1. Select **`Changed Metrics`** from the *Select Report* drop-down list, and then click **`Configure Report`**.

   The *Changed Metrics Configuration* section appears.

2. Select the database for the report from the *Administrative Domain* drop-down list.

3. Select the time period for the report.

   Note If the time specified is earlier than the first entry in the database, the report will begin with the first entry in the database.

4. Click **`Create Report`**.

   A report is generated from the selected database and displayed in a new page. You can use the browser's print command to print a copy of the report.

Understanding the Report

The report has two main columns: *Source Router* and *Interface*. Table 8 details the fields in the *Source Router* column and Table 9 details the fields in the *Interface* column.

Table 8 Source Router Column Fields

Field	Description
IP Address	Address (router ID) of the source router.
Type	Could be: • unknown • internal • area-external • AS-external • both internal and area-external • both internal and AS-external • internal, area-external and AS-external
SysID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router.
Name	The router name provided by the routing protocol, if available.

Table 9 Interface Column Fields

Field	Description
Source IP	The IP address of the router interface.
Original Metric	The metric originally assigned to the interface.
New Metric	The new metric assigned to the interface.
Time	The date and time the change occurred.

Flapping Links

The *Flapping Links* report lists all routing links that have gone down and come up recently, facilitating the rapid isolation of problem links in the network. This report indicates the source router and interface that is flapping, how many times it has changed its status during the period, and when the last change occurred. You can sort the report so that the links with the highest flap count are listed at the top of the report for easy identification.

You would normally run this report after there is an indication of a problem with the links in the network. For example, the *Network Events Summary* report may display a high incidence of flapping link events. Use this report to find out which router links are flapping. This report is also useful in situations where the real-time topology map displays links that are going up and down. Run the *Flapping Links* report to quickly display the information required to identify exactly where the problem links are.

In cases where a route is flapping an abnormally high number of times, it is possible to set up a RAMS alert on the link to monitor it more closely for a period of time to ensure that an outage is avoided.

To configure the Flapping Links report, do the following:

1. Select **`Flapping Links`** from the *Select Report* drop-down list, and then click **`Configure Report`**.

   The *Flapping Links Configuration* section appears.

2. Select the database for the report from the *Administrative Domain* drop-down list.
3. Select the time period for the report.
4. Set the minimum number of flaps required for a link to be included in the report.
5. Click **`Create Report`**.

   A report is generated from the selected database and displayed in a new page. You can use the browser’s print command to print a copy of the report.

Understanding the Report

The report has two main columns: *Source Router* and *Interface*. Table 10 details the fields in the *Source Router* column and Table 11 details the fields in the *Interface* column.

Table 10 Source Router Column Fields

Field	Description
IP Address	Address of the source router.
Type	Could be: • unknown • internal • area-external • AS-external • both internal and area-external • both internal and AS-external • internal, area-external and AS-external
SysID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router.
Name	The router name provided by the routing protocol, if available.

Table 11 Interface Column Fields

Field	Description
Source IP	The router where the interface originated.
Count	The number of times the link has changed state.
Last State	Advertised or withdrawn.
Time	The date and time the last change occurred.

Network Churn

The *Network Churn* report displays a summary of the number of routing events that took place for a selected time period. This report identifies all of the sources (routers) that generated events and the number of events attributed to each source. The events are broken down into those describing the router itself, those related to prefixes, and those related to neighbor adjacencies. Routing events tabulation excludes “hello” packets, which are exchanged periodically.

You would normally run this report after the *Network Events Summary* report displays an unusually high level of network events. This report identifies the sources of churn to help isolate the location of a problem so that it can be further investigated. This high level summary report provides a unique insight into the overall level of routing control plane activity throughout the network.

To configure the Network Churn report, do the following:

1. Select **`Network Churn`** from the *Select Report* drop-down list, and then click **`Configure Report`**.

   The *Network Churn Configuration* section appears.

2. Select the database for the report from the *Administrative Domain* drop-down list.

3. Select the time period for the report.

4. Click **`Create Report`**.

   A report is generated from the selected database and displayed in a new page. You can use the browser’s print command to print a copy of the report.

Understanding the Report

The report has two columns: *Source Router* and *Number of Events*. Table 12 describes the fields in the *Router* column. Table 13 describes the fields in the *Number of Events* column.

Table 12 Router Column Fields

Field	Description
SysID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router.
Name	The router name provided by the routing protocol, if available.
IP Address	Address of the router originating the events.

Table 13 Number of Events Column Fields

Field	Description
Total	Cumulative total of all events.
Router	Number of router events.
Prefix	Number of prefix events for this router.
Link	Number of link events for this router.

Router events captured for this report include the following:

- Router dynamic hostname change (IS-IS only).
- IS-IS overload bit change.
- Router type change, for example between Internal and Area Border Router (ABR) for OSPF.

Prefix events captured for this report include the following:

- Addition and dropping of prefix adjacencies.
- Changes in the metric to a prefix.

Link events captured for this report include the following:

- Addition and dropping of neighbor router adjacencies, including RAMS peering.
- Changes in the metric on the link to a neighbor.

New Prefixes

The *New Prefixes* report lists all of the newly advertised prefixes during the report period, and how many times. Sources of new prefixes include new links, networks, tunnels, and routers. This report is useful after scheduled maintenance because it lets you quickly verify that planned routing topology changes were made appropriately. This report is valuable as it helps you to ensure that customers continue to receive the appropriate level of service after scheduled maintenances are performed.

To configure the New Prefixes report, do the following:

1. Select **`New Prefixes`** from the *Select Report* drop-down list, and then click **`Configure Report`**.

   The *New Prefixes Configuration* section appears.

2. Select the database for the report from the *Administrative Domain* drop-down list.
3. Select the time period for the report.
4. Click **`Create Report`**.

   A report is generated from the selected database and displayed in a new page. You can use the browser's print command to print a copy of the report.

   To sort the report by the totals in the *Count* column rather than the router's prefix, click **`Count`**. This sorts the report in ascending order by count. Click **`Count`** again to resort in descending order by count.

Understanding the Report

Table 14describes the fields in the *New Prefixes* report.

Table 14 New Prefixes Fields

Field	Description
Prefix	The IP address of the new prefix.
SysID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router.
Name	The router name.

IP Address	The IP Address of the router.
Time	The time the new prefix first appeared on the network.
Count	The number of times the prefix was advertised.

New Routers and Links

The *New Routers and Links* report lists newly advertised routers and links in the network. You would normally run this report after new routers are inserted into the network or new links are set up. This report provides you a quick way to verify that changes to the network have taken place as planned.

To configure the New Routers and Links report, perform the following steps:

1. Select **`New Routers and Links`** from the *Select Report* drop-down list, and then click **`Configure Report`**.

   The *New Routers and Links Configuration* section appears.

2. Select the database for the report from the *Administrative Domain* drop-down list.

3. Select the time period for the report.

4. Click **`Create Report`**.

   A report is generated from the selected database and displayed in a new page. You can use the browser's print command to print a copy of the report.

Understanding the Report

Understanding the Report

Table 15 describes the fields in the New Routers table.

Table 15 New Routers Table Fields

Field	Description
IP Address	IP Address of the newly advertised router.
Type	Could be: • unknown • internal • area-external • AS-external • both internal and area-external • both internal and AS-external • internal, area-external and AS-external
SysID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router. This is a 6-byte representation of the IP address written in hexadecimal.

The New Links table contains three main columns: *Source Router* (see Table 16), *Time* (see Table 17), and *Interface* (see Table 18).

Table 16 Source Router Fields

Field	Description
IP Address	IP Address of the router that is advertising the new link.
Type	Could be: • unknown • internal • area-external • AS-external • both internal and area-external • both internal and AS-external • internal, area-external and AS-external
Sys ID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router. This is a 6-byte representation of the IP address written in hexadecimal.
Name	The name of new interface

Table 17 Time Field

Field	Description
Time	The time the link was established.

Table 18 Interface Fields

Field	Description
Source IP	The IP address of the router advertising the interface.
Metric	The metric of the new interface.

Prefix List

The *Prefix List* report lists all of the prefixes currently advertised in the network, or advertised at any point in the recorded history. The report shows reachability into and out of the network.

This report is often run on a weekly basis to verify and assess the reachable networks inventory. It provides a way to quickly check that new networks have been added as planned or obsolete paths removed.

To configure the Prefix List report, do the following:

1. Select **`Prefix List`** from the *Select Report* drop-down list, and then click **`Configure Report`**.

   The *Prefix List Configuration* section appears.

2. Select the database for the report from the *Administrative Domain* drop-down list.
3. Select the time period for the report.
4. Click **`Create Report`**. A report is generated from the selected database and displayed in a new page. You can use the browser's print command to print a copy of the report.

Understanding the Report

Table 19 describes the fields in the *Prefix List* report.

Table 19 Prefix List Fields

Field	Description
Prefix	The address of the prefix.
Type	Could be: • unknown • internal • area-external • AS-external • both internal and area-external • both internal and AS-external • internal, area-external and AS-external

Router	The router advertising this prefix.
SysID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router.
Name	The name of the router advertising the prefix.
IP Address	IP address of the router advertising the prefix.

Prefix Origination Changes

The *Prefix Origination Changes* report lists all of the prefixes that have changed their source router over a specified time period. This is a summary of any changes to the entry points of routes into a network. External routes are not visible.

You would normally run this report every few days, as it provides a quick insight into potential problems. Problems like a router losing an interface or a flapping link will become apparent.

To configure the Prefix Origination Changes report, do the following:

1. Select **`Prefix Origination Changes`** from the *Select Report* drop-down list and click **`Configure Report`**.

   The *Prefix Origination Changes Configuration* section appears.

2. Select the database for the report from the *Administrative Domain* drop-down list.

3. Select the time period for the report.

4. Click **`Create Report`**.

   A report is generated from the selected database and displayed in a new page. You can use the browser's print command to print a copy of the report.

Understanding the Report

Table 20 describes the fields in the *Prefix Origination Changes* report. There are three major columns: *Prefix*, *Current Routers* (last advertising the prefix), and *Router Changes*. The SysID, Name and IP Address fields apply to both the *Current Router* and *Router Changes* columns.

Table 20 Prefix Origination Changes Report Fields

Field	Description
Prefix	The network’s prefix address.
SysID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router.
Name	The name of the router (if available in the routing protocol).
IP Address	The IP address (router ID) in dotted decimal notation.
Advertised	The number of times the router advertised the prefix. *indicates whether the route was recently advertised.
Withdrawn	The number of times the router withdrew the prefix. *indicates whether the route was recently withdrawn.
Time	The time when the route was most recently announced or withdrawn.

Prefix Origination from Multiple Sources

The *Prefix Origination from Multiple Sources* report lists all of the prefixes advertised by multiple routers. Reviewing this report provides a quick way to determine if redundant links or hosts (for example, redundant DNS servers, “Anycast” IP Multicast Rendezvous Points, and so on) are operating normally. The absence of a redundant link or host from the list indicates that a redundant link or host is down, possibly causing reduced service levels or other problems within the network. This report can also detect configuration errors.

This drill-down report is a logical next step after the *Prefix Origination Changes* report identifies a problem. This report may also be the first place to look when an alert is received that a redundant link has failed.

To configure the Prefix Origination from Multiple Sources report, do the following:

1 Select **`Prefix Origination from Multiple Sources`** from the *Select Report* drop-down list, and then click **`Configure Report`**.

The *Prefix Origination from Multiple Sources Configuration* section appears.

2. Select the database for the report from the *Administrative Domain* drop-down list.
3. Select the time period for the report.
4. Click `Create Report`.

   A report is generated from the selected database and displayed in a new page. You can use the browser's print command to print a copy of the report.

Understanding the Report

Table 21 describes the fields in the *Prefix Origination from Multiple Sources* report.

Table 21 Prefix Origination from Multiple Sources Report Fields

Field	Description
Prefix	The IP Address of the network prefix.
Type	Could be: • unknown • internal • area-external • AS-external • both internal and area-external • both internal and AS-external • internal, area-external and AS-external
SysID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router.
Name	The user- configured router name.
IP Address	The IP Address of the router.

Prefixes Withdrawn

The *Prefixes Withdrawn* report lists all of the prefixes that have been withdrawn from the network during the specified period. Use this report to quickly identify customers that can no longer access the network.

You would normally run this report after a scheduled maintenance to verify that no prefixes have been dropped unintentionally.

To configure the Prefixes Withdrawn report, do the following:

1. Select **`Prefixes Withdrawn`** from the *Select Report* drop-down list, and then click **`Configure Report`**.

   The *Prefixes Withdrawn Configuration* section appears.

2. Select the database for the report from the *Administrative Domain* drop-down list.
3. Select the time period for the report.
4. Click **`Create Report`**.

   A report is generated from the selected database and displayed in a new page. You can use the browser's print command to print a copy of the report.

Understanding the Report

Table 22 describes the fields in the *Prefixes Withdrawn* report.

Table 22 Prefixes Withdrawn Report Fields

Field	Description
Prefix	The IP Address of the network's prefix.
SysID	For IS-IS, the router is identified by SysID, the unique value that is programmed into the router.
Name	The user-configured name of the router.
IP Address	The IP Address of the router.
Time	The time the prefix was withdrawn.
Count	The number of times the prefix was withdrawn.

8

VPN Configuration and Reports

This chapter describes the procedures for configuring RAMS's MPLS VPN (Multi-Protocol Label Switching Virtual Private Network) protocol module and displaying VPN reports.

The information in this chapter only applies to RAMS units that have licenses for both the BGP protocol and the VPN protocol.

The BGP/MPLS VPN, as described in RFC 2547bis, is the most common form of service- provider-managed VPN.

A VPN customer's edge routers (CE routers) announce their routes to the service provider's edge routers (PE routers). The service provider then uses BGP to exchange the routes of the VPN among the PE routers associated with that VPN in a way that ensures that the routes from different VPNs are distinct and separate, even if the VPNs' address space overlaps. Because the CE routers do not peer with one another, there is no VPN overlay visible to the VPN's routing algorithm.

Each route within a VPN has an MPLS label. When BGP advertises a VPN route, it also announces the MPLS label for the route. Before a VPN data packet is sent across the service provider backbone, the packet is encapsulated with the MPLS label that corresponds to the VPN route to the packet's destination. The resulting packet is re-encapsulated so that it can be tunneled appropriately over the backbone to the target PE router. In this way, the backbone routers do not need to know the details of the VPN route, thus protecting the privacy and security of the VPN.

In RFC 2547bis, a single mesh of tunnels is required between the PE routers, resulting in a scalable solution both in terms of the effort needed to set up the tunnel mesh, and also the number of VPNs that can be supported on the service provider infrastructure.

However, a major source of complexity is the fact that although routes are stored in separate forwarding tables, the routes are still passed between PE routers using the same instance of BGP that exchanges Internet routes in the provider network. This means that any problems with BGP routes can potentially affect normal Internet connectivity.

Therefore, to manage a large-scale deployment of VPNs in a robust manner, it is critical to tie the protocol diagnostics capability with the VPN service metrics such as reachability and participation. RAMS has extended many of the BGP diagnostic tools to include the VPN protocol.

The RAMS VPN protocol module provides the following benefits:

- A VPN topology overlay that lets you visualize the VPN topology on a per-customer basis.
- Summary and detailed views of the reachability (that is, the existence of routes) for the prefixes advertised by the customer enterprise and the status of the PE routers that participate in a VPN help you to monitor and manage the VPN.
- Reports and customizable alarms alert you to potential or ongoing problems in the VPN.
- Integrated VPN and BGP routing diagnostics enable you to isolate reachability issues down to a single prefix, to determine the routers participating in any VPN, and to isolate and debug complex routing problems.

Reachability and Participation Index

RAMS dynamically tracks every prefix that is advertised from each customer on every VPN. RAMS also tracks the PE routers that participate in each VPN.

Although from a customer perspective, the reachability and participation metrics are expected to remain stable, from a service provider's perspective, these numbers can change constantly. The changes might be due to the periodic addition of new customer sites or VPN prefixes being added to existing sites, the addition of new PE routers to the network or the reallocation of prefixes between PE routers for load balancing or other reasons. Changes to the VPN overlay can also be introduced inadvertently due to BGP misconfiguration.

To provide a visual picture of the stability of a VPN with respect to reachability and participation, RAMS establishes a baseline of the number of prefixes seen at each PE router per VPN and the number of PE routers that participate in each VPN in a steady-state condition. This number is assigned a stability index of 100. As the number of prefixes or routers change, the corresponding index number changes accordingly.

RAMS displays the change in the reachability and participation index in both graphical and text-based reports. You can use these reports to prioritize the allocation of technical resources to resolve customer VPN problems. See Reports on page 269 for information about the available reports.

VPN Explorer

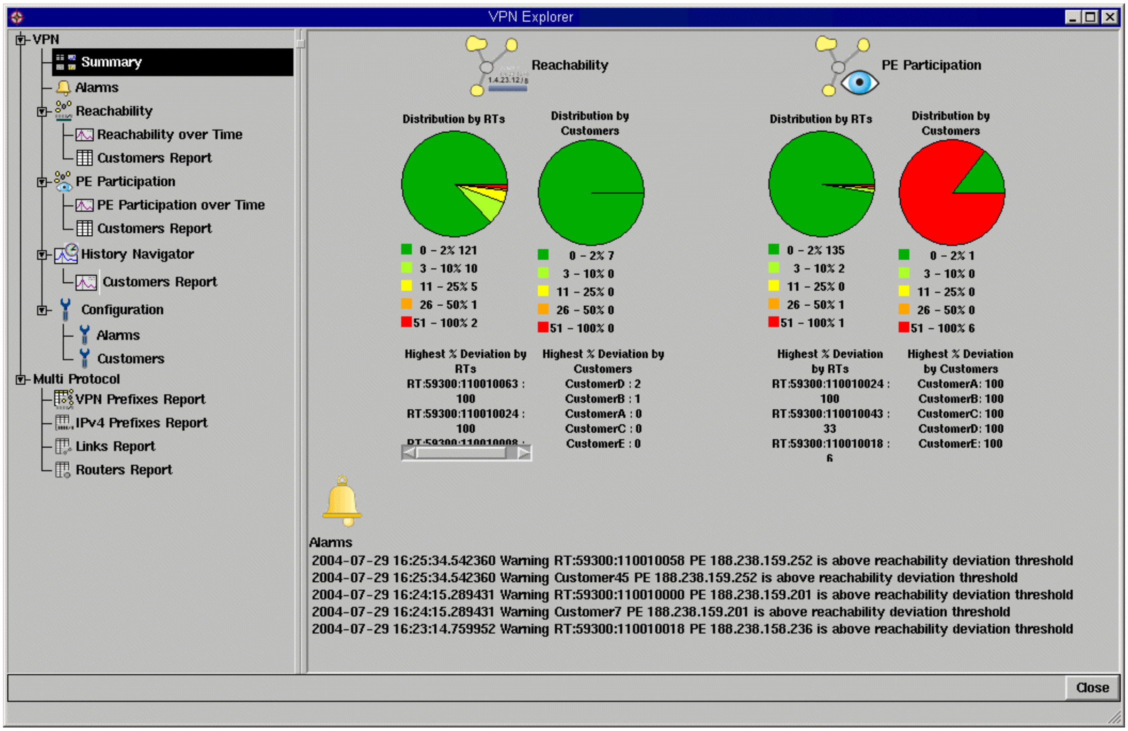
The *VPN Explorer* window provides all of the functions that you use to configure and monitor VPNs.

From the *Routing Topology Map* window, you can use either of the following methods to open the *VPN Explorer* window:

- Select **`VPN Explorer`** on the *Tools* menu.
- Click the VPN Explorer icon on the toolbar.

Figure 87 shows an example of the *VPN Explorer* window.

By default, the *VPN Explorer* window displays a summary of reachability and participation in pie-chart format, lists of deviation from a baseline index, and a list of the most recent VPN alarms. The other VPN reports and utilities are listed in the tree structure in the left-hand pane of the window. See VPN Summary Report on page 269 for more information about the VPN Summary report.



```
2004-07-29 16:25:34.542360 Warning RT:59300:110010058 PE 188.238.159.252 is above reachability deviation threshold
2004-07-29 16:25:34.542360 Warning Customer45 PE 188.238.159.252 is above reachability deviation threshold
2004-07-29 16:24:15.289431 Warning RT:59300:110010000 PE 188.238.159.201 is above reachability deviation threshold
2004-07-29 16:24:15.289431 Warning Customer7 PE 188.238.159.201 is above reachability deviation threshold
2004-07-29 16:23:14.759952 Warning RT:59300:110010018 PE 188.238.158.236 is above reachability deviation threshold
```

Figure 87 VPN Explorer Window

Configuration

Because the VPN's MPLS labels are carried in the MP-BGP protocol messages, the VPN protocol module does not require any additional configuration other than establishing peering with the PE routers when you install the RAMS appliance in the network. See Configure a BGP Instance on page 66 for information about enabling VPN when establishing peering.

However, to display summary reports on a per-customer or per-PE-router basis, you can associate a customer identifier with one or more Route Targets (RTs) by entering the association information manually in the *VPN Explorer* window. To configure many customer/RT associations, it is easier to copy-paste a comma-separated value (CSV) file.

You can specify one of two RT formats to match the conventions used in your network:

- `RT:<AS number>:<VRF ID>`

  This format consists of the letters RT, followed by the 16-bit AS number, followed by the unique 32-bit VPN routing and forwarding (VRF) ID. Separate each of the three elements with a colon; for example, `RT:65522:101`.

- `RT:<IPv4address>:<ID>`

  This format consists of the letters RT, followed by the 32-bit IPv4 address of the device announcing the routes, followed by a unique 16-bit ID number. Separate each of the three elements with a colon; for example, `RT:192.168.0.1:5`.

To set up customer/RT associations manually, perform the following steps:

1. Open the *VPN Explorer* window.
2. Select the **`Customers`** subcategory under **`Configuration`** in the left pane of the window.

   The *VPN Customer Configuration* table is displayed in the right pane of the window, with a text box above it into which you can enter new associations.
3. In the text box, enter customer data in the form "`cust_id,rt`", where "`cust_id`" is a customer identifier, and "`rt`" is the route target you want to associate with that customer. To associate multiple route targets for a given customer, separate the route targets with white space. For example:

```
customer1, RT:65522:101 RT:192.168.0.1:1
```

To set up more than one association, enter each association on a separate line.

4 After entering all of the required customer/RT associations, click **`Submit`**.

The new associations appear in the table in the lower portion of the pane. If a customer is associated with more RTs than can be displayed in the *Definition* column, placing the mouse pointer over the definition opens a pop-up dialog containing the complete list.

To set up associations by copy and pasting a file, do the following:

1 Create a text file.

2 Enter customer data in the text file in the form “`cust_id,rt`”, where “`cust_id`” is a customer identifier, and “`rt`” is the route target you want to associate with that customer. To enter multiple route targets for a given customer, separate the route targets with white space. Place each customer/RT association on a separate line. For example:

```
customer1, RT:65522:101 RT:192.168.0.1:1
customer2, RT:65511:102
customer3, RT:192.168.245.3:22
```

3 Copy the contents of the file and paste it into the text box in the *VPN Customer Configuration* window.

4 Click **`Submit`**.

The new associations are added to the table in the lower portion of the pane.

Alarms

When RAMS detects an exception from the baseline index, an alarm is generated. You can configure the threshold and severity of the alarms.

To configure an alarm, perform the following steps:

1. Open the *VPN Explorer* window.
2. Select the **`Alarms`** subcategory under **`Configuration`** in the left pane of the window.

   The *Configure VPN Alarms* table is displayed in the right-hand pane of the window. Initially, this table is empty.
3. Click **`Add`** to begin configuring alarms.

   Two drop-down menus, a text box, a **`Set`** button, and a **`Remove`** button appear in the Alarms table (see Figure 88 for an example).

   - The Category menu lists the alarm categories from which you can choose.
   - The Severity menu lists the severity levels that you can assign to an alarm category.
   - The Threshold text box specifies the threshold for the alarm.

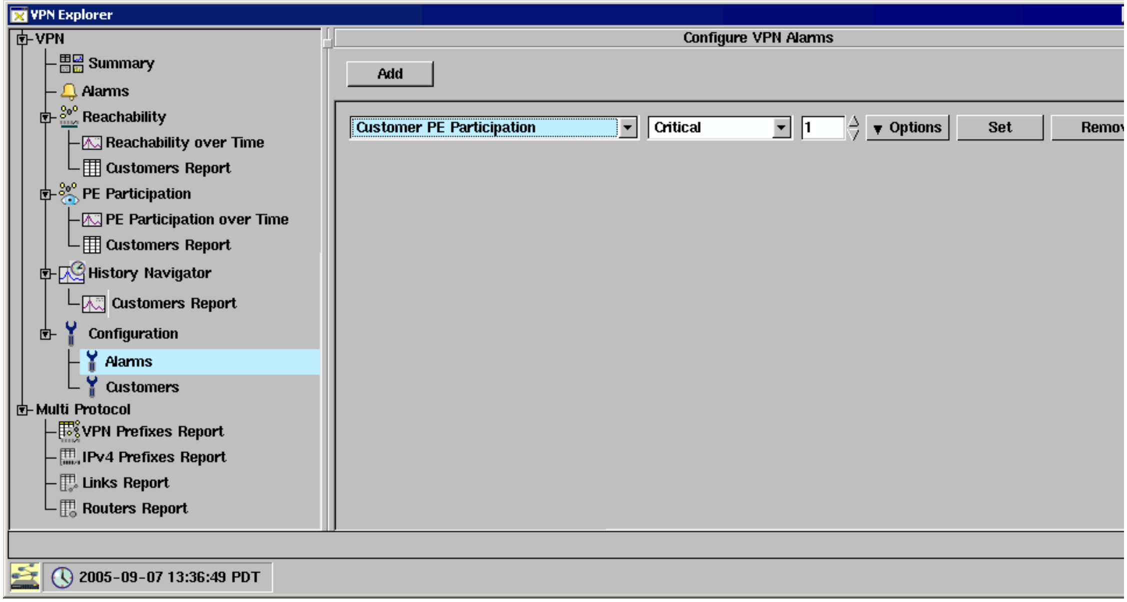


Figure 88 Configure VPN Alarms Window

4 Select an alarm category from the Category menu. The alarm categories are as follows:

- Customer Reachability – This alarm category notifies you if the number of routes to any customer changes.
- Customer Reachability by PE – This alarm category notifies you if the number of routes to any PE router changes.
- Customer PE Participation – This alarm category notifies you if the participation of any PE router in any customer VPN changes.
- New Customer PE – This alarm category notifies you if a router that is not included in the baseline begins to participate in a VPN. (Initially, no routers are in the baseline, so all routers participating in a VPN generate alarms; once the baseline is established, however, only a new router that begins to participate in a VPN generates an alarm.)

5 Select a severity level for that category from the Severity menu. The levels are as follows:

- Critical – Alarms at this level appear in red type in the Alarms report.

- Warning – Alarms at this level appear in orange type in the Alarms report.
- Notice – Alarms at this level appear in black type in the Alarms report.
- Normal – Not an alarm. Does not appear in the Alarms report. Use this level to render a configured alarm inactive.

6 Specify an alarm threshold in the Threshold text-box, either by entering a number or by using the up and down arrows to select a number. If an index varies from the baseline by this percentage, RAMS generates an alarm.

Note You can specify a severity level for the New Customer PE alarm category, but not a threshold. Any router that begins to participate in a VPN generates an alarm at the severity level specified (by default, severity is set to Critical).

7 From the **Options** menu, select one or both of the following delivery options:

- **SNMP Trap**
- **Remote Syslog**

8 Click **`Set`**.

9 Repeat steps 4 through 8 for each alarm you want to configure.

You can configure different severity levels and corresponding thresholds for a given category. For example, you might want to receive Critical alarms when Customer Reachability reaches a threshold of 25%, Warning alarms when Customer Reachability reaches a threshold of 10%, and Notice alarms when Customer Reachability reaches a threshold of 5%.

To permanently remove an alarm, do the following:

1 Open the *VPN Explorer* window.

2 Select the **`Alarms`** subcategory under **`Configuration`** in the left pane of the window.

3 Click **`Remove`** next to the alarm definition you want to remove.

Reports

Two groups of VPN reports are available. The first group of reports display information specific to the VPN protocol, and the second group of reports display multiprotocol data. To display a report, select the appropriate item in the hierarchical tree in the left pane of the *VPN Explorer* window.

VPN Summary Report

The VPN Summary report is the default report present when you open the *VPN Explorer* window. The report displays three types of information.

- At the top of the pane, the report contains four pie-charts that indicate reachability by RT and by customer and participation by RT and by customer, respectively.
- Below each pie-chart, the report lists customers and RTs that experienced the greatest deviation from the baseline index in the same categories (reachability and participation).
- At the bottom of the window, the report lists the most recent five alarms.

The summary report presents a snapshot of VPN data at the time the report is launched. To refresh the data, select a different report, and then select the summary report again.

VPN Alarms Report

The Alarms report lists all VPN alarms.

You can clear an alarm, for example, when changes in the index are caused by planned maintenance.

To display a list of recent alarms, perform the following steps:

1. Open the *VPN Explorer* window.
2. Select **`Alarms`**.

   The *Customer Alarms* report is displayed in the right-hand pane of the window.

By default, the report is sorted by time. You can sort the list by severity level, customer name, or message text by clicking the corresponding column heading. To change the sort order (that is, ascending versus descending order), click the column heading a second time.

In addition, you can filter the report by severity level, customer or RT name, or using a simple or advanced filter expression (see Using Filters on page 226).

Note The Route Target column in the Alarms report may occasionally contain an entry in the form "`Opaque:0xn:0xn`" rather than an RT number. This type of entry indicates an Extended Community attribute that is not Route Target or Source of Origin, and thus is not interpreted by the BGP/ MPLS VPN protocol.

To view routing events around the time of an alarm, perform the following steps:

1. Right-click the alarm in the *Customer Alarms* report.
2. In the pop-up menu that appears, select **`Move Time to Here`**.
3. In the left pane, select the **`Customers Report`** subcategory under **`History Navigator`**. The *History Navigator* pane appears, with its cursor set to the time of the alarm.

   To list the routing events that occurred around the time of the alarm, click the **`Events`** button and set the beginning marker just to the left of the cursor and the ending marker just to the right of the cursor. The *Events* window lists all events occurring in that time period.

   To replay the events that occurred around the time of the alarm, use the playback controls in the History Navigator to step through the events. As playback proceeds, the changes to the routing topology are reflected in the *Topology Map* window.

To clear an alarm, perform the following steps:

1. Open the *VPN Explorer* window.
2. Click **`Alarms`**.

   The *Customer Alarms* report is displayed in the right pane of the window.
3. Click the checkbox to the right of the message you want to clear.
4. Click the **`Apply`** button to redisplay the report without the cleared items.

To refresh the Customer Alarms report, perform the following steps:

To refresh the Customer Alarms list with any new alarms that may have been generated, click **Reload**.

VPN Reachability Reports

You can display reachability data as a graph or as a summary.

To display the Reachability graphs, perform the following steps:

1 Open the *VPN Explorer* window.

2 Select the **Reachability over Time** subcategory under **Reachability**.

The reachability graphs describing deviation from the baseline by RT and by customer are displayed in the right-hand pane of the window. In these graphs, the *x* axis is time and the *y* axis is percentage of deviation.

To display the Reachability summary, perform the following steps:

1 Open the *VPN Explorer* window.

2 Select the **Customers Report** subcategory under **Reachability**.

The reachability summary report is displayed in the right-hand pane of the window. The report includes the customer identifier or RT identifier, the number of PE routers that advertise that RT, and the numbers of active routes, baseline routes, withdrawn routes, new routes, and the deviation from the baseline.

Controls at the top of the pane let you specify whether you want to view data by customer or by RT.

The *Filter By* pull-down menu lets you filter the report to include only the data you want to see. In addition, you can re-sort the data by clicking any column heading in the report.

Note The Route Target column in the Reachability summary report may occasionally contain an entry in the form "`Opaque:0xn:0xn`" rather than an RT number. This type of entry indicates an Extended Community attribute that is not Route Target or Source of Origin, and thus is not interpreted by the BGP/MPLS VPN protocol.

VPN Participation Reports

You can display participation data as a graph or as a summary.

To display the Participation graphs, perform the following steps:

1. Open the *VPN Explorer* window.
2. Select the **`PE Participation over Time`** subcategory under **`PE Participation`**.

   The participation graphs describing deviation from the baseline by RT and by customer are displayed on the right side of the window. In these graphs, the *x* axis is time and the *y* axis is number of customers experiencing a given percentage of deviation.

To display the Participation summary, perform the following steps:

1. Open the *VPN Explorer* window.
2. Select the **`Customers Report`** subcategory under **`PE Participation`**.

   The participation summary report is displayed in the right-hand pane of the window. The report includes the customer identifier or RT identifier and the numbers of active PE participants, baseline PE participants, down PEs, new PEs, and the deviation from the baseline.

   Controls at the top of the pane let you specify whether you want to view data by customer or by RT.

   The *Filter By* pull-down menu lets you filter the report to include only the data you want to see. In addition, you can re-sort the data by clicking any column heading in the report.

Note The Route Target column of the Participation summary report may occasionally contain an entry in the form “`Opaque:0xn:0xn`” rather than an RT number. This type of entry indicates an Extended Community attribute that is not Route Target or Source of Origin, and thus is not interpreted by the BGP/MPLS VPN protocol.

Drilling Down in Summary Reports for More Detailed Information

Several tools are available in the Reachability and Participation Summary reports that allow you to display more detailed information and to focus your attention on specific RTs or customers.

To drill down in a summary report, perform the following steps:

1. Open the *Reachability Summary* report or the *Participation Summary* report.
2. Right-click an entry in the report. A pop-up menu appears containing four options:
   - Details by PE
   - Highlight PE
   - PE Participation/Reachability over Time
   - History Navigator

Details by PE Option

This option opens a new pane at the bottom of the VPN Explorer window that contains a list of all PE routers associated with the selected RT or customer. For each PE router, the report includes the PE router's identifier, IP address, type, state, and Area/AS.

The Details by PE pane contains the following buttons:

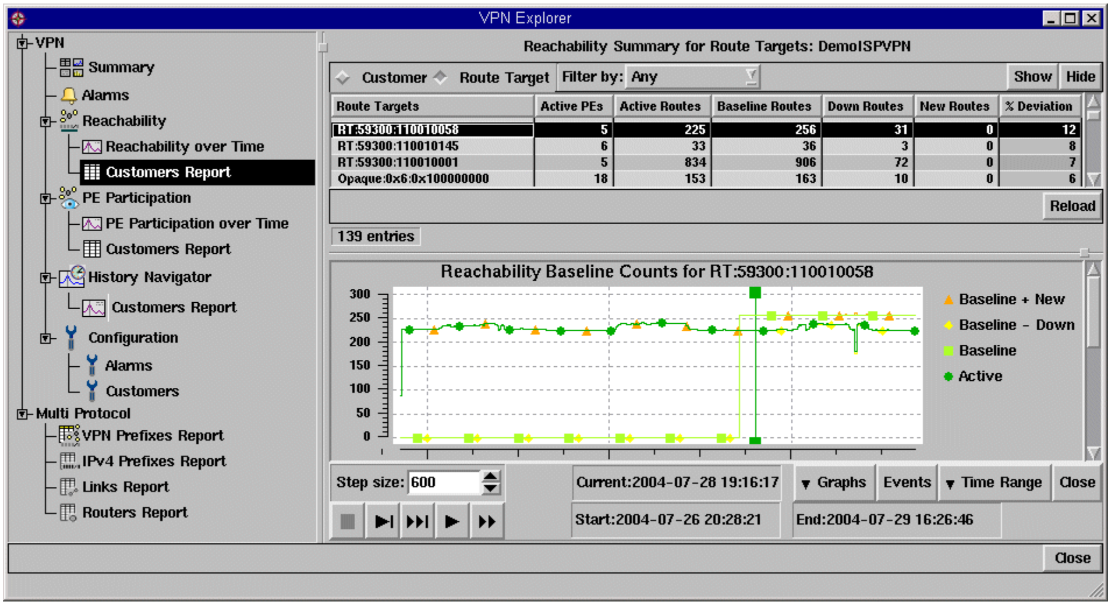
- **Tear Off** – Creates a new window for the Details by PE report, allowing you to have more than one *Details by PE* report open. If you do not use the Tear Off button, the next report you request replaces the current *Details by PE* report.
- **Highlight PE** – Highlights the PE routers listed in the summary report on the topology map in orange.
- **Reload** – Updates the report with new data.
- **Close** – Closes the *Details by PE* report.

Highlight PE

This option highlights the PE routers that advertise the selected RT or are associated with the selected customer VPN on the routing topology map.

PE Participation over Time

This option opens a new pane at the bottom of the VPN Explorer window that contains a graph of participation or reachability data for the selected RT or customer (see Figure 89 for an example).



Reachability Summary for Route Targets: DemoISPVPN

Route Targets	Active PEs	Active Routes	Baseline Routes	Down Routes	New Routes	% Deviation
RT:59300:110010058	5	225	256	31	0	12
RT:59300:110010145	6	33	36	3	0	8
RT:59300:110010001	5	834	906	72	0	7
Opaque:0x6:0x100000000	18	153	163	10	0	6

139 entries

Step size: 600

Current:2004-07-28 19:16:17

Start:2004-07-26 20:28:21

End:2004-07-29 16:26:46

Figure 89 RT Reachability Summary with Graph

The graph pane contains playback controls and buttons similar to the *History Navigator* window (see The History Navigator Window on page 182 for more information), as well as a **Close** button. The current time is indicated in the graph by a green vertical line with green grab handles at top and bottom. You can move this time line by dragging it with the mouse.

Note If you move the time line, the data in the summary report above the graph does not change to reflect the new time until you click the **`Reload`** button in the summary report pane.

In the graph, the light green line represents the baseline route count for the selected RT, the dark green line represents the count of active routes for that RT, the yellow line represents the baseline route count minus the count of down routes for that RT, and the orange line represents the baseline route count plus the count of new routes for that RT. All counts are based on the indicated current time.

History Navigator

Opens a new pane at the bottom of the *VPN Explorer* window for the *VPN History Navigator* showing events related to the selected RT or customer (see VPN History Navigator on page 277 for more information).

Note Events related to a given RT that occurred before a customer/RT association is configured for that RT will show up in a per-RT report displayed later but not in a per-customer report. This is because the data for the report is recorded at the time of the event, and is not updated at the time the association is configured or the report is displayed. Customer/RT association information is recorded only for events that occur after the association is configured.

VPN Prefixes Report

The *VPN Prefixes* report lists all prefixes advertised by VPNs in the network. For each prefix listed, the report lists the router, attributes, state, and area or AS.

The **Filter By** menu lets you filter the report to include only the prefixes you want to see. In addition, you can re-sort the data by clicking any column heading in the report.

IPv4 Prefixes Report

The *IPv4 Prefixes* report lists all prefixes in the network. This report is equivalent to the list generated by the **List Prefixes** option on the *Tools* menu of the *Topology Map* window or the **List Prefixes** button on the topology map toolbar.

Links Report

The *Links* report lists all links in the network. This report is equivalent to the list generated by the **List Links** option on the *Tools* menu of the *Topology Map* window or the **List Links** button on the topology map toolbar.

Routers Report

The *Routers* report lists all routers in the network. This report is equivalent to the list generated by the **List Routers** option on the *Tools* menu of the *Topology Map* window or the **List Routers** button on the *Topology Map* toolbar.

VPN History Navigator

To open the *VPN History Navigator* window, click the **`Customer Report`** subcategory under **`History Navigator`** in the left-hand pane of the *VPN Explorer* window.

At the top of the *VPN History Navigator* window are controls you use to specify whether you want to display per-customer or per-RT information, and to choose the customer or RT on which you want to focus. If you have not yet configured any customer identifiers, the display defaults to per-RT information.

The *VPN History Navigator* window is very similar to the *History Navigator* window described in Chapter , “The History Navigator.” See Chapter for descriptions of the controls and buttons in the lower portion of the *VPN History Navigator* window.

9

BGP Reports

RAMS features a comprehensive set of predefined reports that provide a quick, easy-to-understand view of routing events and problems in the network. When you require a report, select the desired time period from the RAMS database and generate a report for this time period. Reports are generated from the RAMS web server and are formatted in HTML.

This chapter details how to run BGP reports, describes the data each report provides, and illustrates the situations in which each report is useful.

BGP reports fall into two basic categories:

- Activity Reports

  These are high level reports that include data about recent BGP event activity. You will often use these reports to quickly check the general status on a day-to-day or shift-to-shift basis and to quickly identify potential problems and areas of particular interest.

  - BGP Activity Summary
  - BGP Activity by AS
  - BGP Activity by Peer
  - Route Flap Report

  - Prefix Event Detail

- Logical Topology

  These reports provide an in-depth insight into the state of the routing tables for a particular point in time. These reports are typically used during problem identification and resolution. These reports also provide an easy-to-read summary that is accessible in a few seconds, so you do not need to go to each individual router to collect the data.

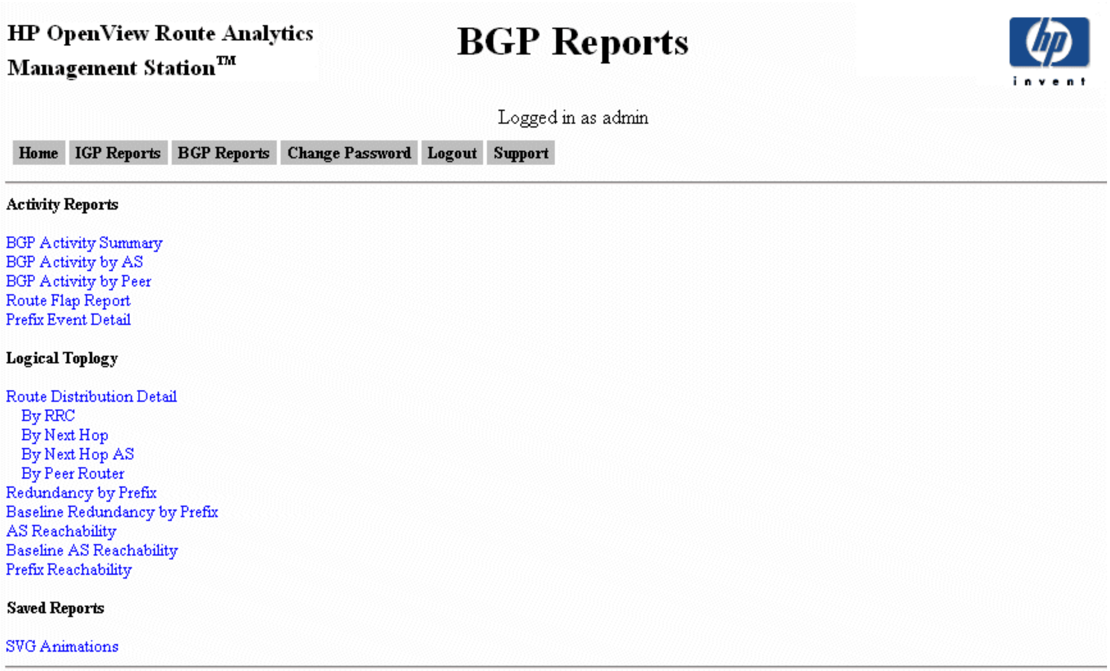
  - Route Distribution Detail by RRC, Origin Router, Next Hop, or Next Hop AS
  - Redundancy by Prefix
  - Baseline Redundancy by Prefix
  - AS Reachability
  - Baseline AS Reachability
  - Prefix Reachability

When RAMS is installed for the first time, it is a good idea to run and print all of the reports. This provides an overview of the network status and should prove useful for network baseline comparison in the future.

Accessing the BGP Report Pages

To access the report pages, use a browser to connect to the RAMS Web server. Click **`BGP Reports`**, and then enter your user name and password. Administrator privilege is not required. The *BGP Reports* page appears, as shown in Figure 90.

Note The browser must accept cookies to login.



HP OpenView Route Analytics Management Station™

BGP Reports

Logged in as admin

Activity Reports

BGP Activity Summary
BGP Activity by AS
BGP Activity by Peer
Route Flap Report
Prefix Event Detail

Logical Toplogy

Route Distribution Detail
By RRC
By Next Hop
By Next Hop AS
By Peer Router
Redundancy by Prefix
Baseline Redundancy by Prefix
AS Reachability
Baseline AS Reachability
Prefix Reachability

Saved Reports

SVG Animations

Figure 90 BGP Reports Page

The BGP reports are divided into two categories:

- Activity Reports – Includes BGP activity as a high-level summary or as detailed reports sorted in a variety of ways.
- Logical Topology – Includes information about the distribution of BGP routes, sorted in a variety of ways.

Available BGP Reports

This section describes the reports available from the *BGP Reports* page.

BGP Activity Summary Report

The *BGP Activity Summary* report provides a high-level overview of BGP network activity over a specified period of time. Any deviations, positive or negative, indicate changes or problems with the network. These deviations can include new peering sessions or routers appearing on the network.

This report is often run on a daily or per-shift basis as it provides a way to quickly determine if there is a problem within the BGP network. Problems can include instabilities caused by convergence failures, oscillations, or unstable links or routers. If an unusual amount of activity is spotted, you can run the *History Navigator* to obtain more information about the events occurring during this time period. If BGP activity is high and stays high, this might indicate that a configuration error occurred during scheduled maintenance. You can also use the data in this report to obtain a high-level view of the scaling characteristics of the network as new routes, routers, and peers are added to the network.

This report displays a list of the prefixes that have oscillated between announced and withdrawn from the BGP protocol.

To configure the BGP Activity Summary report, do the following:

1. Navigate to the *BGP Reports* page.
2. Click **`BGP Activity Summary`**.

   The *Time* and *DB* drop-down lists appear.
3. Select the desired time period from the *Time* drop-down list.

   Note If you specify a time period longer than the number of days of data in the database, the generated report begins with the first recorded data. This also causes the generated report to display an ending time that is in the future.
4. Select the desired database from the *DB* drop-down list.
5. Click **`Create Report`**.

If there was any BGP network activity for the time period selected, a graph appears with the recorded data displayed as lines on the graph. The lines represent the following data:

- Total churn – sum of all the types of churn.
- Internal update churn – number of internal prefixes.
- External update churn – number of updates from external peers.
- Internal withdrawals – number of withdrawn internal prefixes.
- External withdrawals – number of withdrawn prefixes from external peers.

To determine which routers are responsible for activity spikes, check the *Route Flap* report.

BGP Activity by AS Report

The *BGP Activity by AS* report provides a filtered view of BGP activity for individual autonomous systems (AS) that comprise the entire network. This report lets you drill down into each AS and identify specific sources of instability or excessive activity. This report is especially useful for private enterprise internets where multiple ASs are in use and are connected by BGP.

To configure the BGP Activity by AS report, do the following:

1. Navigate to the *BGP Reports* page.
2. Click **`BGP Activity by AS`**.

   The *Time*, *From*, and *To* drop-down lists appear.
3. Select the desired time period from the *Time* drop-down list.
4. Select the start database from the *From* drop-down list.
5. Select the end database from the *To* drop-down list.
6. Click **`List AS`**.

If there was any BGP network activity between the selected databases for the time period, a graph opens displaying incoming updates and withdrawals and outgoing updates and withdrawals.

After viewing this report, you may want to refer to the *BGP Activity Summary* report to view specific sources of instability. Alternatively, you can open the *History Navigator* window and perform an event analysis for the time period in question.

BGP Activity by Peer Report

The *BGP Activity by Peer* report is useful for quickly identifying which BGP peers are most active and for diagnosing internal churn. Since this report provides a greater level of detail, you will normally start with the *BGP Activity Summary* report and then run this report if you notice an unusual amount of churn activity. This report provides a quick way of pinpointing activity that exceeded the normal expected range.

To configure the BGP Activity by Peer report, do the following:

1. Navigate to the *BGP Reports* page.
2. Click **`BGP Activity by Peer`**.

   The *DB* drop-down list appears.
3. Select the desired database from the *DB* drop-down list.
4. Click **`List Peer`**.

   The *Peer* and *Time* drop-down lists appear.
5. Select the desired peer from the *Peer* drop-down list.
6. Select the desired time period from the *Time* drop-down list.
7. Click **`Create Report`**.

If there was any BGP network activity between the database and the selected peer, the report is displayed as a line chart over time, and displays the update churn (updated prefixes) and withdrawn churn (prefixes withdrawn).

Route Flap Report

The *Route Flap* report provides a list of prefixes that have oscillated between announced and withdrawn from the BGP protocol. It provides a way to quickly identify where service has been lost or degraded due to flapping links. In general, you would run this report as a periodic status check to determine if a problem requires further investigation.

To configure the Route Flap report, do the following:

1. Navigate to the *BGP Reports* page.
2. Click **`Route Flap Report`**.

   The *Time* and *DB* drop-down lists appear.
3. Select the desired time period from the *Time* drop-down list.
4. Select the desired database from the *DB* drop-down list.
5. Click **`Create Report`**.

If there was any BGP network activity, the report displays a table that provides the prefix ID, peer that announced or withdrew the prefix, time/date of the last update (date/time), and the current prefix state (announced or withdrawn).

The table can be sorted by prefix, the peer which announced/withdrew the prefix, the number of events, or the current state. To change the sort order, click the heading of the column on which you want to sort.

Prefix Event Detail

The *Prefix Event Detail* report is a detailed report that provides insight into how long a problem has been happening and identifies which prefixes are affected. For example, you might run this report if the *BGP Flap* report identifies a prefix that is flapping. The *Prefix Event Detail* report provides insight into how long a prefix has been experiencing intermittent service and identifies the customers that have been affected by the associated service degradation. This report can save substantial time because you do not have to log into each individual router and view the routing tables to try to identify the problem.

To configure the Prefix Event Detail report, do the following:

1. Navigate to the *BGP Reports* page.
2. Click **`Prefix Event Detail`**.

   The *DB*, *From*, and *To* drop-down lists appear.
3. Select the desired database from the *DB* drop-down list.
4. Select the desired start and end times from the *From* and *To* drop-down lists.

5 Enter the prefix number in the *Prefix* field.

6 Click **`Create Report`**.

The report is displayed in a tabular format, which can be sorted based on the headers of each column. The report provides the time of event, direct peer address, type of event (announced or withdrawn), and attributes (BGP announcement attributes of routes control mechanisms).

Route Distribution Detail Report

The *Route Distribution Detail* report provides an insight into the distribution of BGP routes as determined by BGP's path selection algorithm. These distributions are key in traffic engineering, capacity planning, and configuring maintenance activities. During troubleshooting, you can refer to this report if there is a problem with traffic getting to a particular AS from a particular AS over a BGP link.

To configure the Route Distribution Detail report, do the following:

1 Navigate to the *BGP Reports* page.

2 Click **`Route Distribution Detail`**, or click on one of the four available reports (By RRC, By Next Hop, By Next Hop AS, By Peer Router).

3 Select the desired database from the *DB* drop-down list.

4 Check the **`latest`** radio button, or check the **`select`** radio button and enter the desired time and date information.

5 Click **`Submit Query`**.

The report is displayed in a tabular format and can be sorted based upon Next Hop, Origin Router, or Next Hop AS. These three variables are critical in determining the BGP routing policies that will provide optimal routing across internal infrastructure, as well as network exits. These policies influence traffic distributions and can have dramatic effects on the costs and performance of the network as a whole.

The report specifies the prefix ID, next hop address(es) on the BGP path, address of the router that announced the prefix, AS number associated with the next hop, local preference (BGP mechanism that selects best path), AS path, MED, and BGP community.

The *Route Distribution Detail* report can be customized by sorting on the key variables of Next Hop (the address the router traffic will be sent to based on the BGP path selection algorithm), Origin Router (the router that announced the prefix), and Next Hop AS (the Autonomous System number associated with the next hop determined by the BGP path selection algorithm).

The *Next Hop Detail* report is a drill-down report that is accessed from the *Route Distribution Detail* report and provides a view of all prefixes over each BGP route.

To view the *RRC*, *Next Hop*, *Next Hop AS,* or *Peer Router* reports, click the desired report name and enter the database and time period details. Then click **`Create Report`**.

Redundancy by Prefix Report

The *Redundancy by Prefix* report displays the degree of redundancy available for each routed prefix on the network and the number of available hops for each route. This report is normally run periodically to review network redundancy and check that redundant paths are available as planned. If you are involved in network planning and design, you will also find this report useful as you plan network updates and expansion.

The report can be sorted by the number of available next hops, allowing you to quickly and easily identify prefixes that are only available through a single point path.

To configure the Redundancy by Prefix report, perform the following steps:

1. Navigate to the *BGP Reports* page.
2. Click **`Redundancy by Prefix`**.
3. Select the desired database from the *DB* drop-down list.
4. Check the **`latest`** radio button, or check the **`select`** radio button and enter the desired time and date information.
5. Click **`Submit Query`**.

The *Redundancy by Prefix* report is displayed in a tabular format and contains the following data; Prefix ID, baseline number of next hops*, number of next hops (based upon period for which report is run), next hop prefix, next hop AS ID.

*Baseline number of next hops is calculated based on an average sampled over a 1-week period (last 7 days) and any that have been in the routing table 80% of the time are included.

Baseline Redundancy by Prefix Report

The *Baseline Redundancy by Prefix* report identifies whether or not each routed prefix on the network is available from the RAMS appliance. Run this report to ensure that all network prefixes are available from the RAMS appliance.

To configure the Baseline Redundancy by Prefix report, do the following:

1. Navigate to the *BGP Reports* page.
2. Click **`Baseline Redundancy by Prefix`**.
3. Select the desired database from the *DB* drop-down list.
4. Enter the desired time and date information.
5. Click **`Submit Query`**.

The *Baseline Redundancy by Prefix* report is displayed in a tabular format.

AS Reachability Report

The *AS Reachability* report indicates the degree of connectivity, next hops, and AS paths toward all reachable ASs. The report enables you to quickly sort through the list of reachable ASs and the paths taken to reach them. This report can be used to validate security and routing policies and to ensure that there are no single points of failure between the network and key external ASs. You can refer to this report during planning to see whether there is adequate network redundancy.

To configure the AS Reachability report, do the following:

1. Navigate to the *BGP Reports* page.
2. Click **`AS Reachability`**.

3. Select the desired database from the *DB* drop-down list.
4. Enter the desired time and date information.
5. Click **`Submit Query`**.

The report is displayed in a tabular format with the following data: Baseline number of next hops*, number of next hops (based upon time query), ID of next hops, and AS path.

*Baseline number of next hops is calculated based on an average sampled over a 1-week period (last 7 days) and any that have been in the routing table 80% of the time are included.

Baseline AS Reachability Report

The *Baseline AS Reachability* report provides an insight into whether an entire AS is reachable from the RAMS appliance and via what AS paths. This report is normally run to ensure that RAMS is monitoring all ASs as planned (baseline) and to assist in network planning.

To configure the Baseline AS Reachability report, do the following:

1. Navigate to the *BGP Reports* page.
2. Click **`Baseline AS Reachability`**.
3. Select the desired database from the *DB* drop-down list.
4. Enter the desired time and date information.
5. Click **`Submit Query`**.

The report is displayed in a tabular format with the following data: AS number for next hop, next hops in baseline*, AS path in baseline*.

*Baseline number of next hops is calculated based on an average sampled over a 1-week period.

Prefix Reachability Report

The *Prefix Reachability* report indicates the degree of connectivity and BGP attributes for prefixes that are routable by BGP across the entire network. The report can be sorted by Prefix, Destination, AS, or Next Hop, so you can quickly validate routing policies and identify configuration errors. During network design, it provides a simple way to identify the paths chosen by BGP for a given prefix or set of prefixes.

To configure the Prefix Reachability report, do the following:

1. Navigate to the *BGP Reports* page.
2. Click **`Prefix Reachability`**.
3. Select the desired database from the *DB* drop-down list.
4. Enter the desired time and date information.
5. Click **`Submit Query`**.

The report is displayed in a tabular format with the following data; prefix address, destination AS, next hop, AS path.

10

Alerts

Overview

RAMS alerts are used to obtain immediate notification of any changes to routes or routers, based upon configurable thresholds. Alerts can be sent as SNMP traps to an SNMP-based network management system integrated with other network operations, or logged to a Syslog file.

By default, alerts are not enabled in RAMS. You must set and configure alerts that identify specific variables. These variables allow you to customize alerts and to turn alerts on and off for various types of routing events.

Alerts are set globally and affect all routing events for a particular routing protocol. For example, if you are monitoring a single or multiarea OSPF network, the alerts you select are applied to all the OSPF routing events for all the OSPF areas being monitored.

There are two groups of alerts, one for IGP protocols (this group includes OSPF, IS-IS, and EIGRP) and one for BGP protocols. This chapter provides an overview of RAMS alerts and explains how to configure these alerts using the Web browser interface. It also details the data that is contained in the various alerts and describes how alerts can be used to improve service availability and customer satisfaction.

Configuring an SNMP Server

Before setting any alerts, you must configure the global settings on the *Alerts Configuration* page. Additionally, you must download the *PacketDesign* Structure of Management Information (SMI) and the *pdRouteExplorer* Management Information Base (MIB) to the SNMP Agent software.

Note The RAMS SNMP dæmon does not support a full MIB walk. The value `integer 0` is returned for all queries to portions of the MIB that are not supported. This may be interpreted by the querying system as an error in the type of the returned value.

To download the Packet Design SMI and MIB, perform the following steps:

1. Use a browser to connect to the RAMS *Home* page, and then click **`Administration`**.
2. Enter your user name and password, and then click **`Login`**.

   The *Route Recorder Configuration* page appears.
3. Click **`Alerts`**.

   The RAMS *Alerts Configuration* page appears (see Figure 91).

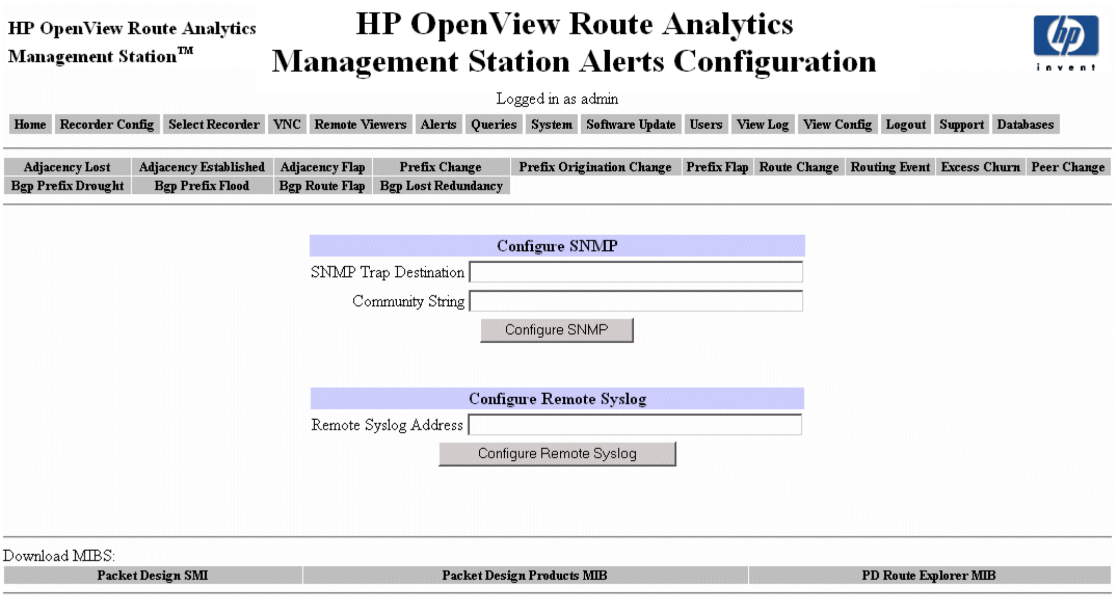


Figure 91 RAMS Alerts Configuration Page

4 Click the **Packet Design SMI** link at the bottom of the RAMS *Alerts Configuration* page.

5 When the page opens, select **File > Save As** and save the file in the directory containing the SNMP Agent software.

6 Click the **Packet Design Products MIB** link at the bottom of the RAMS *Alerts Configuration* page.

7 When the page opens, select **File > Save As** and save the file in the directory containing the SNMP Agent software.

8 Click the **PD Route Explorer MIB** link at the bottom of the RAMS *Configuration* page.

9 When the page opens, select **File > Save As** and save the file in the directory containing the SNMP Agent software.

To configure the SNMP Manager address, do the following:

1 Log in as an administrator and navigate to the *Alerts Configuration* page if you are not already there.

2 Enter the IP address or fully qualified domain name of the machine with the SNMP Agent software in the *SNMP Trap Destination* field.

3 Enter the community string in the *Community String* field.

4 Click **`Configure SNMP`**. This configures the SNMP manager address.

Configuring the Remote Syslog and RAMS

Before configuring RAMS to send alerts, you must set up the *syslogd* on the servers to accept RAMS's remote logging of events. Keep the following points in mind:

- The machine receiving syslog messages must have appropriate firewall settings to allow this. Some Linux systems come with Security Level set to *High*, which blocks the syslog port.
- The *syslogd* may default to starting with no remote reception capability. In order to receive remote syslog messages, you may need to restart *syslogd* with the *-r* option. If in doubt, look in `/var/log/messages` for a "`syslogd started < remote reception >`" log entry.

After you have configured the remote syslog, you can configure the syslog settings on the RAMS *Alerts Configuration* page.

To configure syslog settings on RAMS, do the following:

1 Log in as an administrator and navigate to the *Alerts Configuration* page if you are not already there.

1 Enter the IP address of the remote system log in the *Remote Syslog Address* field.

2 Click **`Configure Remote Syslog`**.

Setting an Alert

This section provides an example of how a specific alert is set and an agent configured. In this instance, the agent is HP OpenView Network Node Manager (NNM) and a prefix flap alert is set.

Note The method used to configure all IGP alerts is virtually the same. The only difference is that some alerts contain an additional threshold configuration and some do not.

To set a Prefix Flap alert and configure an SNMP trap, perform the following steps:

1 Log in as an administrator and navigate to the *Alerts Configuration* page if you are not already there.

2 Click **`Prefix Flap`**. The *Prefix Flap Alerts Configuration* page appears, as shown in Figure 92.

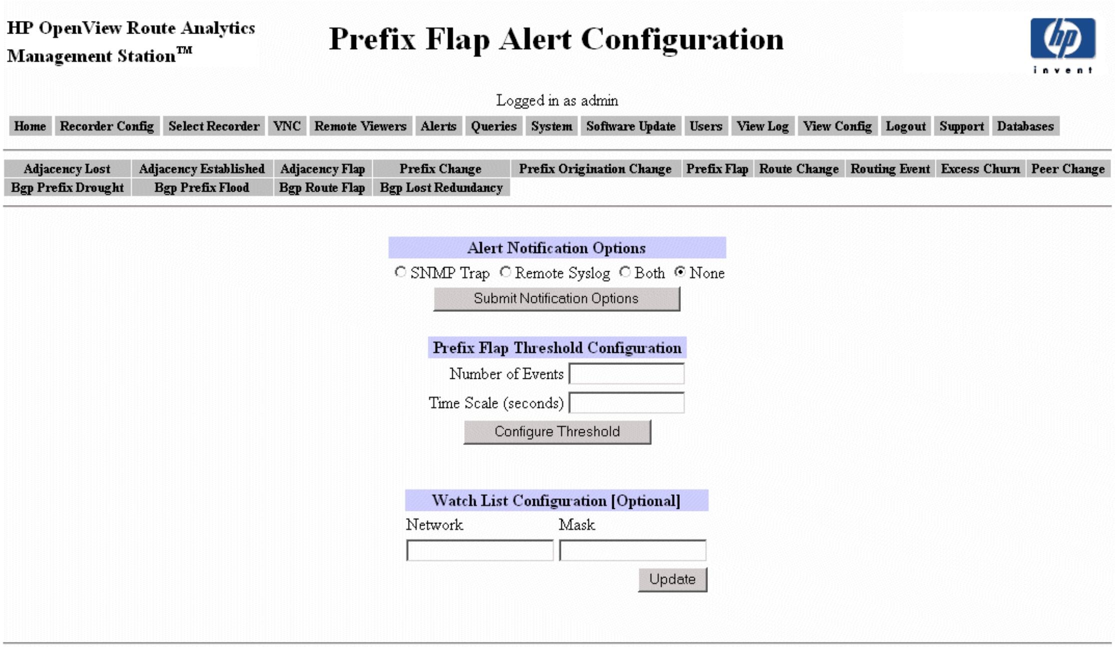
3 In the *Prefix Flap Threshold Configuration* section, enter the number of events that need to occur in the specified time for an alert to occur. For example, to send an alert if a minimum of ten events occur in thirty seconds, enter 10 in the *Events* field and 30 in the *Time Scale* field.

4 Click **`Configure Threshold`**.

5 If desired, enter network and mask details in the *Watch List Configuration* section. This is optional. The Watch List, if configured, limits alerts to events occurring in the specified network.

6 Check the desired alert type (SNMP Trap in this example) in the *Alert Notification Options* section, and then click **`Submit Notification Options`**.

7 Click **`Update`**.



HP OpenView Route Analytics Management Station™

Prefix Flap Alert Configuration

Logged in as admin

Alert Notification Options

○ SNMP Trap ○ Remote Syslog ○ Both ● None

Prefix Flap Threshold Configuration

Number of Events

Time Scale (seconds)

Watch List Configuration [Optional]

Network Mask

Figure 92 Prefix Flap Alerts Configuration Page

The next step is configuring the SNMP trap that will display the alarm in the network management system. In this example, the network management system is HP OpenView Network Node Manager (NNM).

To configure the SNMP trap in NNM, do the following:

1. In the *HP OpenView* main window, select **`Event Configuration`**.
2. Select the RAMS MIB.
3. Select the Prefix Flap event.
4. From the Edit menu, select **`Modify Event`**.
5. Enable the trap display as an Error Alarm.
6. Set the severity of the alarm
7. Set the event log pop-up notification.
8. Click **`OK`**.

9 From the Edit menu, select **`Save`**.

Now, when a prefix flap is detected, RAMS sends the trap to NNM and NNM displays the corresponding alarm in the alarm log and displays the alarm pop-up.

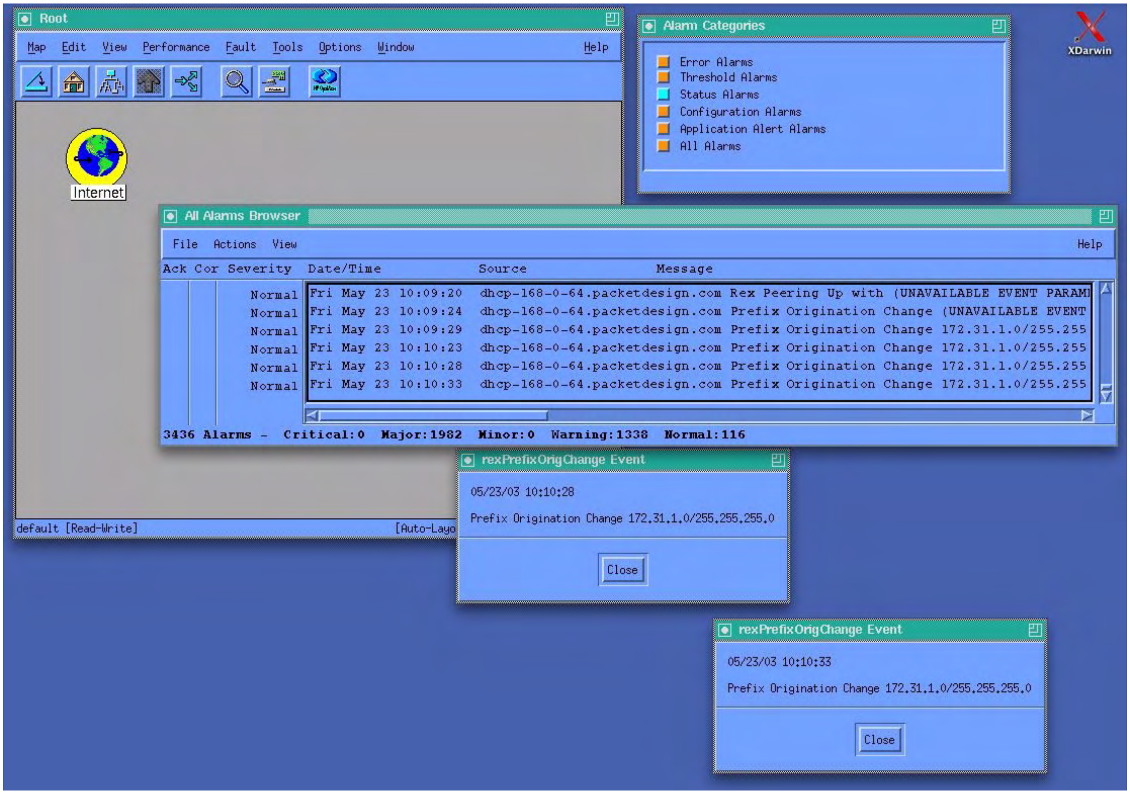
Most alerts have configurable watch lists that are specific to the selected alert, where it is possible to set the routers or prefixes that are focused on. Other alerts, like the *Prefix Flap* alert, have an additional configuration called Threshold Configuration.

Alert Format

Since all alerts have a different format, all of the possible alert formats are not covered in this guide. This section presents one example of a SNMP Trap alert and one example of a system log alert.

SNMP Trap Alert Format

Figure 93 displays an example of a *Prefix Origination Change* alert sent from RAMS to HP OpenView Network Node Manager.



```
Ack Cor Severity  Date/Time             Source                        Message
            Normal Fri May 23 10:09:20  dhcp-168-0-64.packetdesign.com Rex Peering Up with (UNAVAILABLE EVENT PARAM
            Normal Fri May 23 10:09:24  dhcp-168-0-64.packetdesign.com Prefix Origination Change (UNAVAILABLE EVENT
            Normal Fri May 23 10:09:29  dhcp-168-0-64.packetdesign.com Prefix Origination Change 172.31.1.0/255.255
            Normal Fri May 23 10:10:23  dhcp-168-0-64.packetdesign.com Prefix Origination Change 172.31.1.0/255.255
            Normal Fri May 23 10:10:28  dhcp-168-0-64.packetdesign.com Prefix Origination Change 172.31.1.0/255.255
            Normal Fri May 23 10:10:33  dhcp-168-0-64.packetdesign.com Prefix Origination Change 172.31.1.0/255.255
3436 Alarms -  Critical:0  Major:1982  Minor:0  Warning:1338  Normal:116
```

```
05/23/03 10:10:28

Prefix Origination Change 172.31.1.0/255.255.255.0
```

```
05/23/03 10:10:33

Prefix Origination Change 172.31.1.0/255.255.255.0
```

Figure 93 HP OpenView Network Node Manager Alarm

Syslog Alert Format

All syslog messages are sent with facility *Local0* and severity *Alert*. This is not currently configurable.

The following example illustrates an alert for a *Prefix Origination Change* alert sent from RAMS to a Syslog file, and assumes that the Syslog host has inserted timestamps.

```
Nov 13 13:23:04 dhcp-168-0-28 RouteAnalyzer[1264]: - Prefix
Origination Change 25.0.0.2/32
Nov 13 13:23:04 dhcp-168-0-28 RouteAnalyzer[1264]: -
rexPrefixFlap: rexPrefixNet = 25.0.0.2, rexPrefixMask =
255.255.255.255
Nov 13 13:23:04 dhcp-168-0-28 RouteAnalyzer[1264]: - Adjacency
Lost: Router(192.168.103.11) to PseudoNode(192.168.103.2)
```

IGP Alerts Definition

This section describes the types of IGP Alerts that you can activate and the configurable threshold variables. The RAMS *Alerts Configuration* page, shown in Figure 91, has two groups of buttons. The buttons in the upper row of the second group are all IGP Alerts.

Adjacency Lost Alert

When this alert is enabled, an alert is sent when an adjacency is lost between two routers in the network. This alert is normally used to monitor key adjacencies, like adjacencies between areas, adjacencies between a router and a server farm, and point-to-point links to remote areas on the backbone. When the alert is generated, the following information is included in the alert:

- Time and date the adjacency was lost.
- The IP address of the source and destination routers where the adjacency was lost.

When an *Adjacency Lost* alert is received, you can open the routing topology map to quickly view what effect the lost adjacency had. The *History Navigator* window is also useful for viewing routing events that may have taken place immediately preceding the adjacency loss to further analyze the problem.

To configure an Adjacency Lost alert, do the following:

1. Click **`Adjacency Lost`** on the RAMS *Alerts Configuration* page.
2. Check the desired alert notification option.
3. Click **`Submit Notification Options`**.
4. If desired, enter the watch list configuration details. In the *Source Router* and *Destination Router* fields, enter the interface IP addresses for the two ends of the adjacency. In the case of a pseudonode, use the IP address of the LAN interface of the Designated Router.
5. Click **`Update`**.
6. If an SNMP Trap was selected, follow the steps in Setting an Alert on page 296 to configure the SNMP trap.

Adjacency Flap Alert

This alert is triggered when the adjacency between two routers is flapping.

RAMS provides the flexibility to let you define the adjacency flap threshold by defining the number of transitions per second that will initiate an alert. When the alert is generated, the following information is included in the alert:

- The time and date of the adjacency flap.
- The IP address of the flapping route.

When an *Adjacency Flap* alert is received, you can quickly view what effects the flapping route has on the network in the real-time routing topology map. The *History Navigator* window is also useful for viewing routing events that may have taken place immediately preceding the alert to determine how long the problem has been occurring.

Note This alert is not effective for EIGRP, because the derivation of link-state events, such as an adjacency state change, from EIGRP events takes multiple seconds.

To configure an Adjacency Flap alert, do the following:

1. Click **`Adjacency Flap`** on the RAMS *Alerts Configuration* page.
2. Check the desired alert notification option.
3. Click **`Submit Notification Options`**.
4. Enter the adjacency flap threshold in transitions per second in the *Adjacency Flap Threshold Configuration* field.
5. Click **`Configure Threshold`**.
6. If desired, enter the watch list configuration details. In the *Source Router* and *Destination Router* fields, enter the interface IP addresses for the two ends of the adjacency. In the case of a pseudonode, use the IP address of the LAN interface of the Designated Router.
7. Click **`Update`**.
8. If an SNMP Trap was selected, follow the steps in Setting an Alert on page 296 to configure the SNMP trap.

Prefix Change Alert

This alert is sent when a prefix attribute, such as a metric or prefix type, changes. Prefix attribute changes normally occur during scheduled maintenance. This alert is used to carefully monitor that the correct changes have been made and that changes affecting critical routes continue to receive the appropriate service levels. When the alert is generated, the following information is included in the alert:

- The time and date of the prefix change.
- The prefix where the change occurred.

After receiving this alert, you would usually go to the router in question to see what metric change took place and review the service log to see if a prefix change had been planned, and if a change was planned, verify the change.

To configure a Prefix Change alert, do the following:

1. Click **`Prefix Change`** on the RAMS *Alerts Configuration* page.
2. Check the desired alert notification option.
3. Click **`Submit Notification Options`**.
4. If desired, enter the watch list configuration details.
5. Click **`Update`**.
6. If an SNMP Trap was selected, follow the steps in Setting an Alert on page 296 to configure the SNMP trap.

Prefix Origination Change Alert

This alert is sent when a prefix has been withdrawn or is newly advertised. A prefix withdrawal indicates that services have been disrupted which could present a number of possible problems, such as dropped packets, slowed service, and so on. This alert represents a significant time savings compared to telnetting to each router to determine which prefix was withdrawn or added – a very tedious and time consuming task. When this alert is generated, the following information is included in the alert:

- The time and date the prefix was withdrawn or advertised.
- The prefix ID.

After receiving a *Prefix Origination Change* alert, you normally open the *Online Update Monitor* and view the events panel to locate the prefix in question. You then drill down and find out the router, neighbor/prefix, attributes, and area for the prefix in question.

To configure a Prefix Origination Change alert, do the following:

1. Click **`Prefix Origination Change`** on the RAMS *Alerts Configuration* page.
2. Check the desired alert notification option.
3. Click **`Submit Notification Options`**.
4. If desired, enter the watch list configuration details.
5. Click **`Update`**.
6. If an SNMP Trap was selected, follow the steps in Setting an Alert on page 296 to configure the SNMP trap.

Prefix Flap Alert

This alert indicates that a prefix is flapping. This alert provides an early indication of a service becoming unavailable. In pinpointing the flapping prefix, RAMS saves significant time and effort and speeds up resolution of the problem. During the setup of this alert, you define the prefix flap threshold by entering the number of transitions that must occur within a number of seconds to initiate an alert. When the alert is generated, the following information is included in the alert:

- The time and date of the prefix flap.
- The prefix that is flapping.

When a *Prefix Flap* alert is received, you should select the **`List Prefixes`** option from the *Tools* menu in RAMS to obtain a list of all network prefixes and then select the prefix in question to identify the routers that are sourcing the prefix. This quickly identifies the routers sourcing the prefix so that you can go to the specific routers involved and troubleshoot the problem further.

For more information on configuring a *Prefix Flap* alert, refer to Setting an Alert on page 296 to configure the SNMP Trap.

Route Change Alert

This alert indicates that the route between an explicitly configured source and destination has changed. This alert provides an early indication of service degradation or even of an outage. You can define a set of source and destination router pairs for the end-to-end routes to be watched. When the alert is generated, the following information is included in the alert:

- The time and date of the route change.
- The endpoints of the route that has changed.

When a *Route Change* alert is received, you should investigate to find out the source by opening the *History Navigator* window and performing an event analysis for the time period in question. The *Event Analysis* window gives you greater detail about the route change. Details you can view include routers, links, and prefixes. Alternatively, you can run a *Prefix Origination Change* report or a *Prefix Withdrawn* report for the time period in question to further identify what routers changed sourcing.

To configure a Route Change alert, do the following:

1. Click **`Route Change`** on the RAMS *Alerts Configuration* page.
2. Check the desired alert notification option.
3. Click **`Submit Notification Options`**.
4. Enter the watch list configuration details, which are the source and destination routers for the routes to be watched. The source is a router IP address, which can be the router ID. The destination must be a routable IP address (not all router ID's are routable addresses).
5. Click **`Update`**.
6. If an SNMP Trap was selected, follow the steps in Setting an Alert on page 296 to configure the SNMP trap.

Routing Event Alert

This alert is triggered when a routing event is received after a *quiet period*. This alert is normally used in a quiet network to catch anomalies or unexpected events. If a particular router is experiencing problems, this alert can be set so that the router can be carefully watched to determine if it is operating correctly. The *Routing Event* alert lets you identify a potential problem early, often before it causes a more serious problem.

All routing events are included in the total routing event count. You can set the threshold for the number of routing events per second that trigger the *Routing Event* alert. When no routing events have occurred for the threshold number of seconds, whatever routing event occurs next triggers the alert. When the alert is generated, the following information is included in the alert: the time and date when the first routing event occurred after a quiet period.

To configure a Routing Event alert, do the following:

1. Click **`Routing Event`** on the RAMS *Alerts Configuration* page.
2. Check the desired alert notification option.
3. Click **`Submit Notification Options`**.
4. Enter the event threshold in the *Hold Time* field.
5. Click **`Configure Threshold`**.
6. If an SNMP trap was selected, follow the steps in Setting an Alert on page 296 to configure the SNMP trap.

Excess Churn Alert

This alert is sent when the number of routing messages transmitted in the network reaches a threshold you define. This alert is enabled so that notification is received of higher than normal activity levels, which could be an early indicator of a problem, before a more serious event occurs.

Keep the following points in mind when configuring this alert:

- The Excess Churn alert is based upon number of *routing messages*, not *routing events*.
- A routing message may contain information about multiple events.
- Routing messages may be redundant. For example, multiple routers may report the same event.
- All routing messages (not Hellos) are included in the total message count. For EIGRP, this alert is based directly on the distance-vector EIGRP Update messages, not the derived link-state events.

- The number of routing messages per second that are generated during normal operation vary depending on factors such as the size of the network and the protocols being used. EIGRP, for example, typically generates more routing messages than other IGP protocols.

Determining an appropriate threshold for this alert may require some experimentation. Generally, you should set the threshold at the upper bound of what you expect will occur during normal network operation. If the number of alerts generated is too high (or low), adjust the threshold.

After receiving this alert, you should open the *History Navigator* and view the Events List to find out more detail about the sources of the unusual activity, and to determine if further investigation is required.

To configure the Excess Churn alert, do the following:

1. Click **`Excess Churn`** on the RAMS *Alerts Configuration* page.
2. Check the desired alert notification option.
3. Click **`Submit Notification Options`**.
4. Enter the event threshold in the *Excess Churn Threshold Configuration* field.
5. Click **`Configure Threshold`**.
6. If an SNMP trap was selected, follow the steps in Setting an Alert on page 296 to configure the SNMP trap.

Peer Change Alert

This alert is sent if RAMS's peering adjacency has changed by going up or down. This is an alert you might want to enable all of the time so that you are aware when RAMS is unable to monitor certain parts of the network. When the alert is generated, the following information is included in the alert:

- The time and date.
- The IP address of the new peer.

When this alert is received, it is usually easiest to log into the peered router to check on the link status of the link in question.

To configure a Peer Change alert, do the following:

1. Click **`Peer Change`** on the RAMS *Alerts Configuration* page.
2. Check the desired alert notification option.
3. Click **`Submit Notification Options`**.
4. If an SNMP trap was selected, follow the steps in Setting an Alert on page 296 to configure the SNMP trap.

BGP Alerts Definition

This section describes the types of BGP Alerts that you can set for RAMS and the configurable threshold variables for these alerts. The RAMS *Alerts Configuration* page, shown in Figure 91, has two groups of buttons. The buttons in the lower row of the second group are all BGP Alerts.

BGP Route Flap Alert

This alert is triggered when a route is repeatedly updated or withdrawn from the BGP table. This alert provides an early indication of a critical service becoming unavailable or degradation in performance. You set up the alert by identifying a flap period (for example, 10 minutes) and a threshold (the number of up and down cycles in a flap period that will trigger the alert, for example, 5). When the alert is generated, the following information is included in the alert:

- The time and date when the flap reached the threshold.
- The prefix length.
- The peer router.
- The peer AS.
- The next hop.
- The next hop AS.
- The current state (active/withdrawn).
- The time and date.

When a *Route Change* alert is received, you should run the *BGP Prefix Events Details* report for the prefix in question to see the duration of the flapping problem.

BGP Lost Redundancy Alert

This alert is triggered when a redundant link is lost, which can be an early indicator of a reduction in service level or higher cost for service. The ability to immediately become aware of a lost redundant link can also be critical in maintaining acceptable levels of customer satisfaction and SLAs. This alert is triggered when redundant prefixes are reduced to a single available next hop (calculated by baseline[1]). You have the flexibility to set the threshold (minimum number of next-hops that will trigger the alert) for this alert.

When the alert is generated, the following information is included:

- The prefix.
- The length of the redundancy.
- The source AS number.
- The baseline period.
- The number of baseline next-hops.
- The current number of next-hops.
- The time and date when the prefix redundancy was lost.

After receiving this alert, you would typically run the *Route Distribution Detail* report to view next hops from the prefix in question to see which peers withdrew routes and why.

BGP Prefix Flood/BGP Prefix Drought Alert

These alerts are initiated when a routing table size increases or decreases by a significant amount, relative to the calculated baseline[2]. This type of alert could indicate that a router misconfiguration has taken place, or possibly a security breech has occurred. You have the flexibility to define a threshold for this alert. For example, 20% above and below the baseline would trigger the alert.

When the alert is generated, the following information is included:

- The baseline period (n x days).
- The baseline table size.
- The current table size.

[1] The baseline is calculated based on an average redundancy for a prefix sampled over the last 7 days.

[2] The baseline is calculated based on an average sampled over a one week period (last 7 days).

- The percentage delta in the table size
- The time and date.
- The peer ID

When the *Prefix Flood* alert is received, you should telnet to the router in question to review the routing table, verify the problem, and begin looking into the possible cause.

BGP Acquired Redundancy Alert

This alert is triggered when the number of next hops for the prefix becomes greater than the threshold for the BGP Lost Redundancy Alert. In some cases, the BGP Acquired Redundancy Alert could indicate that a problem previously identified by a BGP Lost Redundancy Alert has been corrected.

When the alert is generated, the following information is included:

- The prefix.
- The peer IP address.
- The source AS (or the number associated with the AS where the link originated).
- The number of baseline next-hops.
- The current number of next-hops.
- The time and date when the prefix redundancy was acquired.

After receiving this alert, you would typically run the *Route Distribution Detail* report to view next hops from the prefix in question to see which peers added routes.

BGP AS Path Longer Alert

Each BGP prefix has an AS path associated with it. When a prefix begins advertising an AS path that is longer than previously advertised, the *AS Path Longer* alert is initiated. This alert indicates that traffic for this prefix will now take a longer path to arrive at the destination, possibly causing delays in service.

When the alert is generated, the following information is included:

- The prefix.
- The peer IP address.
- The source AS number.
- The time and date when the alert was triggered.

After receiving this alert, you would typically run the *Route Distribution Detail* report to view next hops by AS.

BGP Down to One Path and BGP Down to Zero Paths Alerts

These alerts perform similarly to the BGP Lost Redundancy Alert on page 309, with the following exceptions:

- The threshold for the BGP Down to One Path alert is pre-set to 1.
- The threshold for the BGP Down to Zero Paths alert is pre-set to 0.

A

XML RPC Queries

This appendix details how to make RAMS queries using an Application Programming Interface (API). RAMS Queries are specific queries that are initiated by an Extensible Markup Language Remote Procedure Call (XML RPC).

Normally, these queries are initiated from a computer program written in a computing language such as C, Java, or Perl. This appendix provides examples written in the Perl scripting language.

Initiating queries from a computer program allows you to:

- Acquire specific route analysis information from RAMS.
- Integrate RAMS with other tools you have that support XML RPC.

To use these queries from a program, it is necessary to link in the appropriate XML-RPC library or package.

For more information, refer to **www.xmlrpc.com**.

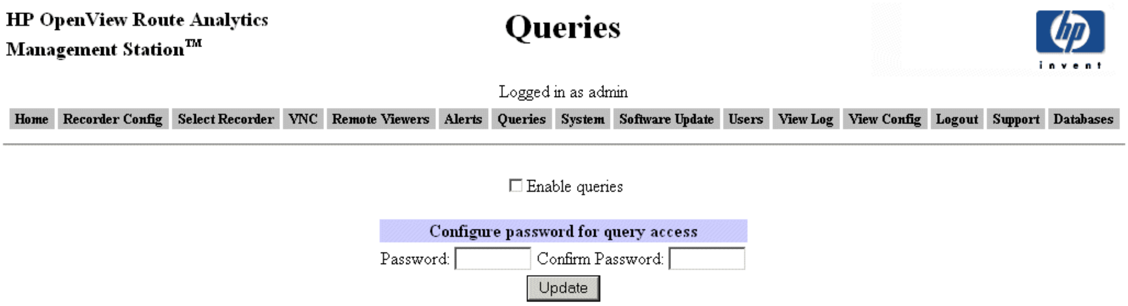
Configuring RAMS to Accept Queries

Before you can use queries, you must configure RAMS to accept queries.

To enable queries, do the following:

1 Log in to the *Administration Interface* and click **`Queries`**.

The *Queries* page opens, as shown in Figure 94.



HP OpenView Route Analytics Management Station™

Queries

Logged in as admin

□ Enable queries

Configure password for query access

Password: Confirm Password:

Figure 94 Queries Page

2 Select **`Enable queries`**.

3 Enter a password and confirm it. The password can be from one to eight alphanumeric characters in length, is case sensitive, and must not contain nulls, blanks or underscores.

4 Click **`Update`**.

Using Queries

This appendix specifies the input parameters and results for the XML RPC calls listed in Table 23. The *method name* for each call consists of the prefix "`RouteAnalyzer.`" plus the query name shown in the table. The queries with names beginning `api_mp_` may be used to obtain data from both IGP and BGP protocol domains. The `api_list_a_route` queries apply to paths crossing both IGP and BGP domains. The calls with names beginning `api_vpn_` apply only to BGP/MPLS VPN protocol domains. The remainder apply only to IGP protocol domains.

Note The Dumper function called by the example query programs converts XML, which uses the < and > separators and no new lines, into a more readable form. This readable form is displayed in the sample output shown throughout this appendix. The Dumper function is included in the standard Perl package called Data.

Table 23 XML RPC Queries

Query	Description	Page
api_del_watch_list	Delete the watch list for the specified alert.	-318
api_get_alert_destination_info	Return information about the destination to which the specified alert is sent.	-320
api_get_watch_list	Return the watch list for the specified alert.	-322
api_link_list	Return a list of links for the specified network.	-324
api_list_a_route	Return the total metric of a path (route) and the list of links.	-327
api_list_a_route_ECMP	Return the total metric of a path (route) and the list of links, including all ECMP paths.	-330

Query	Description	Page
api_mp_events	List all multi-protocol network events between two different times.	-333
api_mp_links	List links meeting filter criteria in a multi-protocol network.	-336
api_mp_routes	List prefix routes meeting filter criteria in a multi-protocol network.	-339
api_mp_routers	List routers meeting filter criteria in a multi-protocol network.	-342
api_prefix_events	Return a list of events for the specified prefix.	-345
api_prefix_list	List all prefixes advertised in the network.	-348
api_prefix_list_filtered	Return a list of prefixes for the specified router.	-350
api_prefix_list_multi_orig	Return a list of prefixes that are originated by more than one router for the specified network.	-353
api_prefix_list_same	List all prefixes advertised by multiple routers at the same time.	-356
api_router_events	Return a list of events associated with the specified router.	-358
api_router_list	Return a list of routers for the specified network.	-361
api_router_summarizable	List routers advertising multiple summarizable prefixes.	-364
api_vpn_cust_rt_list	List all customer names in VPN to RT (Route Target) mappings.	-366
api_vpn_customer_pe_participation	Return statistics of participating PEs for each VPN customer.	-368

Query	Description	Page
api_vpn_customer_pe_list	Return the list of participating PEs for the specified VPN customer.	-370
api_vpn_customer_reachability	Return reachability statistics for each VPN customer.	-372
api_vpn_customer_reachability_by_peer	Return reachability statistics at each PE for the specified VPN customer.	-374
api_vpn_route_target_pe_participation	Return statistics of participating PEs for each route target in the specified network.	-377
api_vpn_route_target_pe_list	Return the list of participating PE routers and their VPN state for the specified route target.	-380
api_vpn_route_target_reachability	Return reachability statistics for each route target in the specified network.	-382
api_vpn_route_target_reachability_by_peer	Return reachability statistics at each PE for the specified route target.	-385
api_vpn_routes	Return the list of VPN routes for the specified network.	-388

api_del_watch_list

RPC Call: Route Analyzer.api_del_watch_list {password} {alert}

This query deletes the watch list that was previously set up for an alert. A watch list limits alerts to events matching specific criteria, which could be a combination of (prefix and mask) or (source router and destination router) depending on the specific alert. By deleting the watch list, the limits on the alert will be removed. The query returns a 1 on success, 0 otherwise.

Input Parameters

- **password** – The password configured for queries.
- **alert** – The alert for which the watch list will be deleted. Currently, watch lists can be deleted for the following alerts: AdjLost, AdjEst, RtFlap, LnkFlap, RtOrigChange, RtChange, PeerChange, BgpRouteFlap, BgpLostRedund. Detailed information about alerts can be found in Chapter 10.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0])) {
    printf "usage: RouteAnalyzer.api_del_watch_list ip\n";
    exit(0);
}

my $rexip = $ARGV[0];

use strict;
use RPC::XML::Client;
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
my $alert = "RtFlap";
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_del_watch_list',
             RPC::XML::RPC_STRING($password),
             RPC::XML::RPC_STRING($alert)
             ));
foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper
($value1) );
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
'0'
```

api_get_alert_destination_info

RPC Call: RouteAnalyzer.api_get_alert_destination_info {password} {alert}

This query returns information about the alert destination. This includes the alert destination, the SNMP Trap Community, SNMP Trap Destination, the threshold, and the time scale.

Input Parameters

- **`password`** – The password configured for queries.
- **`alert`** – The alert for which destination information is requested. Currently, the following alerts are implemented: AdjLost, AdjEst, RtFlap, LnkFlap, RtOrigChange, RtChange, Event, EChurn, PeerChange, PrefixFlap, BgpPrefixDrought, BgpPrefixFlood, BgpRouteFlap, BgpLostRedund, BgpASPathLonger, BgpDownToOnePath, BgpDownToZeroPaths, BgpAcquiredRedund, RtrReachability, CustReachability, CustPrivacy, RtrIntrusion, BgpPeerLost. Detailed information about alerts can be found in Chapter 10.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0])) {
    printf "usage: RouteAnalyzer.api_get_alert_destination_info ip\n";
    exit(0);
}

my $rexip = $ARGV[0];

use strict;
use RPC::XML::Client;
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
my $alert = "RtFlap";
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_get_alert_destination_i
nfo',
           RPC::XML::RPC_STRING($password),
           RPC::XML::RPC_STRING($alert)
          ));
foreach (@reqs) {
```

```
my $res = $client->send_request($_);
if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper
($value1) );
}
```

Sample Output

```
 ---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'alert_dest' => {
    'snmp_trap_community' => 'public',
    'time_scale' => '60',
    'threshold' => '50',
    'alert_destination' => 'SNMP Trap',
    'snmp_trap_destination' => '192.168.0.123'
  }
}
```

api_get_watch_list

RPC Call: RouteAnalyzer.api_get_watch_list {password} {alert}

This query returns the watch list that have been set up for the specified alert. Watch lists limit alerts to events matching specific criteria, which could be a combination of (prefix and mask) or (source router and destination router) depending on the specific alert. The example output shows a watch list that has been set up for the RtFlap alert. The output shows the source router, the destination router, and an "op" value. The "op" value can be: "and," "or", or "none."

Input Parameters

- **`password`** – The password configured for queries.
- **`alert`** – The alert for which the list of set watch lists is requested. Currently, watch lists can be obtained from the following alerts: AdjLost, AdjEst, RtFlap, LnkFlap, RtOrigChange, RtChange, PeerChange, BgpRouteFlap, BgpLostRedund. Detailed information about alerts can be found in Chapter 10.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0])) {
    printf "usage: RouteAnalyzer.api_get_watch_list ip\n";
    exit(0);
}

my $rexip = $ARGV[0];

use strict;
use RPC::XML::Client;
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
my $alert = "RtFlap";
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_get_watch_list',
             RPC::XML::RPC_STRING($password),
            RPC::XML::RPC_STRING($alert)
           ));
foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper
($value1) );
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'wlists' => [
    {
      'src' => {
        'ip4_addr' => '192.168.0.123'
      },
      'dst' => {
        'ip4_addr' => '192.168.0.40'
      },
      'op' => 'and'
    }
  ]
}
```

api_link_list

RPC Call: RouteAnalyzer.api_link_list {password} {database name} {time}

This query returns a list of links for the specified network. The information includes, for each link, a description of the source node, destination node, and the interface between the two.

Note This query is deprecated and may be removed in a future release. New applications should use api_mp_links instead.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_link_list ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("24 Jul 2003 11:53:33 PST");
```

```
push (@reqs, RPC::XML::request->new('RouteAnalyzer.api_link_list',
            RPC::XML::RPC_STRING($password),
            RPC::XML::RPC_STRING($database),
            RPC::XML::datetime_iso8601->new(time2iso8601($t1))));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper($value1) );
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'network_name' => 'UCBJul03a',
  'report_time' => '20051027T18:46:09',
  'links' => [
    {
      'source' => {
        'nodeType' => 'Internal',
        'ip_addr' => {
          'ip4_addr' => '169.229.128.130'
        },
        'nodeState' => 'UP',
        'nodeProto' => 'OSPF',
        'name' => '',
        'nodeArea' => 'UCBJul03a.OSPF/169.229.128.128',
        'maskLen' => '32',
        'systemID' => '169.229.128.130'
      },
      'interfaces' => [
        {
          'source' => {
            'ip4_addr' => '169.229.128.130'
          },
          'bw' => '0',
          'destination' => {
            'ip4_addr' => '169.229.128.129'
          },
          'metric' => '1000',
          'delay' => '10000',
          'state' => '1'
        }
      ],
      'destination' => {
        'nodeType' => 'PseudoNode',
        'ip_addr' => {
          'ip4_addr' => '169.229.128.129'
        },
        'nodeState' => 'UP',
        'nodeProto' => 'OSPF',
        'name' => '',
        'nodeArea' => 'UCBJul03a.OSPF/169.229.128.128',
        'maskLen' => '29',
        'systemID' => '169.229.128.129 DR'
      }
    },
    ....
  ]
}
```

api_list_a_route

RPC Call: Route Analyzer.api_list_a_route {password} {database name} {source address} {dest prefix} {time}

This query returns the total metric (if calculable) and the list of links in the path from the source to the destination at the requested time. Only one path is listed even if multiple equal-cost paths exist. The list of links is in order.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`source address`** – An XML struct that contains the router ID or a router interface address as an IPv4 address and a mask length of 32. The mask address is included for backward compatibility, but this query ignores it.
- **`dest prefix`** – An XML struct that contains any destination prefix consisting of an IP4 address, such as `192.168.123.125`, and a mask length, such as `27`.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.

Example

```
#!/usr/bin/perl
my $rexip = $ARGV[0];
my $database = $ARGV[1];
use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client; my $req; my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = 1099528204;    #seconds since 1970-01-01 00:00:00 UTC
push (@reqs,RPC::XML::request->new('RouteAnalyzer.api_list_a_route',
        RPC::XML::RPC_STRING($password),
        RPC::XML::RPC_STRING($database),
        ##### source #####
        new RPC::XML::struct(ip_addr =>
                new RPC::XML::struct(ip4_addr => "192.168.99.99"),
                masklen => 32),
        ##### destination #####
        new RPC::XML::struct(ip_addr =>
                new RPC::XML::struct(ip4_addr => "10.23.113.0"),
                masklen => 27),
        RPC::XML::datetime_iso8601->new(time2iso8601($t1)) ));
foreach (@reqs) {
        my $res = $client->send_request($_);
        if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
        my $value1 = $res->value;
        print (join "\n", Dumper($value1));}
```

Sample Output

```
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'network_name' => 'tester',
  'report_time' => '20041104T00:31:49',
  'route' => {
    'route_cost' => '5',
    'time' => '20041104T00:30:04',
    'links' => [
      {
        'source' => {
          'nodeType' => 'AreaBR_ASBR',
          'ip_addr' => {
            'ip4_addr' => '192.168.99.99'
          },
          'name' => '',
          'nodeArea' => 'tester.OSPF/Backbone',
          'systemID' => '192.168.99.99',
          'nodeState' => 'UP',
          'nodeProto' => 'Unknown',
          'maskLen' => '32'
        },
        'interfaces' => [
          {
            'source' => {
              'ip4_addr' => '192.168.116.11'
            },
            'bw' => '0',
            'destination' => {
              'ip4_addr' => '192.168.116.17'
            },
            'metric' => '1',
            'delay' => '10000',
            'state' => '1'
          }
        ],
        'destination' => {
          'nodeType' => 'PseudoNode',
          'ip_addr' => {
            'ip4_addr' => '192.168.116.17'
          },
    'name' => '',
    'nodeArea' => 'tester.OSPF/Backbone',
    'systemID' => '192.168.116.17 DR',
    'nodeState' => 'UP',
    'nodeProto' => 'Unknown',
    'maskLen' => '24'
   }
  },
 ]
 ....
}
```

api_list_a_route_ECMP

RPC Call: RouteAnalyzer.api_list_a_route_ECMP {password} {database name} {source address} {dest prefix} {time}

This query returns the total metric (if calculable) and the collection of links comprising one or more equal-cost paths from the source to the destination at the requested time. The list of links is the result of a breadth-first search of the tree of path segments. Consequently, the links may not be listed in order for any of the paths and links that are present on multiple paths may be replicated in the list.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`source address`** – An XML struct that contains the router ID or a router interface address as an IPv4 address and a mask length of 32. The mask address is included for backward compatibility, but this query ignores it.
- **`dest prefix`** – An XML struct that contains any destination prefix consisting of an IP4 address, such as `192.168.123.125`, and a mask length, such as `27.`
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.

Example

```
my $rexip = $ARGV[0];
my $database = $ARGV[1];
use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client; my $req; my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";
```

```
my $t1 = str2time("3 Nov 2004 16:30:04 PST");
push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_list_a_route_ECMP',
        RPC::XML::RPC_STRING($password),
        RPC::XML::RPC_STRING($database),
        ##### source #####
        new RPC::XML::struct(ip_addr =>
                new RPC::XML::struct(ip4_addr => "192.168.99.99"),
                masklen => 32),
        ##### destination #####
        new RPC::XML::struct(ip_addr =>
                new RPC::XML::struct(ip4_addr => "10.23.113.0"),
                masklen => 27),
        RPC::XML::datetime_iso8601->new(time2iso8601($t1)) ));
foreach (@reqs) {
        my $res = $client->send_request($_);
        if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
        my $value1 = $res->value;
        print (join "\n", Dumper($value1));  }
```

Sample Output

```
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'network_name' => 'tester',
  'report_time' => '20041105T21:24:16',
  'route' => {
    'route_cost' => '8',
    'time' => '20041104T00:30:04',
    'links' => [
      {
        'source' => {
          'nodeType' => 'AreaBR_ASBR',
          'ip_addr' => {
            'ip4_addr' => '192.168.99.99'
          },
          'name' => '',
          'nodeArea' => 'tester.OSPF/Backbone',
          'systemID' => '192.168.99.99',
          'nodeState' => 'UP',
          'nodeProto' => 'Unknown',
          'maskLen' => '32'
        },
        'interfaces' => [
          {
            'source' => {
              'ip4_addr' => '192.168.99.99'
            },
            'bw' => '0',
            'destination' => {
              'ip4_addr' => '192.168.107.11'
            },
            'metric' => '2',
            'delay' => '10000',
            'state' => '1'
          }
        ],
        'destination' => {
```

```
        'nodeType' => 'PseudoNode',
        'ip_addr' => {
          'ip4_addr' => '192.168.107.11'
        },
        'name' => '',
        'nodeArea' => 'tester.OSPF/Backbone',
        'systemID' => '192.168.107.11 DR',
        'nodeState' => 'UP',
        'nodeProto' => 'Unknown',
        'maskLen' => '24'
      }
    },
  ]
  ....
}
```

api_mp_events

RPC Call: RouteAnalyzer.api_mp_events {password} {database name} {time t1} {time t2} {filter} {max entries}

This query lists all multi-protocol network events between times t1 and t2 that meet the specified filter criteria. Examples of events include BGP prefixes announced or withdrawn and IGP adjacencies added or dropped.

Note The query can return a large number of BGP events in a small amount of time. You can keep the number of events manageable by refining your filter and shortening the time period. You may also have to expand XML RPC client timeouts to accommodate the amount of time required for the query to acquire all BGP events within times t1 and t2. Alternatively, you can supply the optional {max entries} parameter to limit the number of entries returned.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`time t1, t2`** – Two times specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will include events that occurred between the two specified times.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.
- **`max entries`** – An optional 32-bit integer parameter specifying the maximum number of entries to return in the query.

Example

```
#!/usr/bin/perl
```

```
if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_mp_events ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";

$filter = $ARGV[2] if ($#ARGV >= 2);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("05 Nov 2004 11:09:04 PST");
my $t2 = str2time("05 Nov 2004 11:53:52 PST");

push (@reqs, RPC::XML::request->new('RouteAnalyzer.api_mp_events',
    RPC::XML::RPC_STRING($password),
    RPC::XML::RPC_STRING($database),
    RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
    RPC::XML::datetime_iso8601->new(time2iso8601($t2)),
    RPC::XML::RPC_STRING($filter), 150 ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print Dumper($value1);

}
```

Sample Output

```
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '150',
  'network_name' => 'baklab701',
  'report_time' => '20051107T23:13:37',
  'totalEntries' => '93971',
  'result' => [
    {
      'target' => '',
      'attributesText' => 'Type: Internal Router',
      'time' => {
        'seconds' => '1130545402',
        'useconds' => '966898'
      },
      'topology' => {
        'fullName' => 'baklab701.OSPF/0.0.0.1',
        'protocol' => 'OSPF'
      },
      'operation' => 'Drop Router',
      'router' => '192.168.0.87'
    },
    {
      'target' => '192.168.0.87',
      'attributesText' => 'Metric: Down',
      'time' => {
        'seconds' => '1130545402',
        'useconds' => '966898'
      },
      'topology' => {
        'fullName' => 'baklab701.OSPF/0.0.0.1',
        'protocol' => 'OSPF'
      },
      'operation' => 'Drop Neighbor',
      'router' => '192.168.0.2 DR'
    },
    ....
  ]
}
```

api_mp_links

RPC Call: RouteAnalyzer.api_mp_links {password} {database name} {time} {filter}

This query lists all network links present in the multi-protocol network at the specified time. The results may be filtered to select only the links connected to a single router, for example. The output consists of information about the source node, the destination node, and the link between them.

Input Parameters

- **password** – The password configured for queries.
- **database name** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **time** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **filter** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_mp_links ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";

$filter = $ARGV[2] if ($#ARGV >= 2);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
```

```
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("05 Nov 2004 02:11:27 PST");

push (@reqs, RPC::XML::request->new('RouteAnalyzer.api_mp_links',
             RPC::XML::RPC_STRING($password),
             RPC::XML::RPC_STRING($database),
             RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
             RPC::XML::RPC_STRING($filter)));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print Dumper($value1);
}
```

Sample Output

```
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '150',
  'network_name' => 'LabRight',
  'report_time' => '20050725T23:40:42',
  'totalEntries' => '150',
  'result' => [
    {
      'link' => {
        'srcNode' => {
          'type' => 'Route Explorer',
          'ipaddr' => '192.168.122.90'
        },
        'dstNode' => {
          'type' => 'IBGP Peer',
          'ipaddr' => '192.168.100.100'
        },
        'state' => {
          'down' => 'false'
        }
      },
      'topology' => {
        'fullName' => 'LabRight.ConfedsTest.ConfedTestTop.BGP/AS65510',
        'protocol' => 'BGP'
      }
    },
   {
      'link' => {
        'srcNode' => {'type' => ..., 'ipaddr' => ...},
        'dstNode' => {'type' => ..., 'ipaddr' => ...},
        'state' => {'down' => ...}, //end of link
      'dif' => ...,
      'sif' => ...,
        'topology' => {'fullName' => ..., 'protocol' => ...}
      }, //end of topology
      'metric' => ...
      }
    ]
  }
```

api_mp_routes

RPC Call: RouteAnalyzer.api_mp_routes {password} {database name} {time} {filter} {max entries}

This query lists all routes, i.e., all prefix announcements from all routers announcing the prefixes, at the specified time and meeting the specified filter criteria.

Note The query can return a large number of BGP routes in a small amount of time. You can keep the number of routes manageable by refining your filter. You may also have to expand XML RPC client timeouts to accommodate the amount of time required for the query to acquire all the routes. Alternatively, you can supply the optional {max entries} parameter to limit the number of entries returned.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.
- **`max entries`** – An optional 32-bit integer parameter specifying the maximum number of entries to return in the query.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_mp_routes ip database filter\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";
$filter = $ARGV[2] if ($#ARGV >= 2);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = time;

push (@reqs, RPC::XML::request->new('RouteAnalyzer.api_mp_routes',
             RPC::XML::RPC_STRING($password),
             RPC::XML::RPC_STRING($database),
             RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
             RPC::XML::RPC_STRING($filter), 150));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print Dumper($value1);
}
```

Sample Output

```
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '150',
  'network_name' => 'baklab701',
  'report_time' => '20051107T23:07:45',
  'totalEntries' => '680',
  'result' => [
    {
      'topology' => {
        'fullName' => 'AllStaticRoutes.Static',
        'protocol' => 'Static'
      },
      'attributes' => {
        'nextHops' => [
          {
            'nextHop' => '192.168.101.101/8'
          }
        ]
      },
      'prefix' => '0.0.0.0/0',
      'router' => {
        'type' => 'Static',
        'ipaddr' => '192.168.133.34'
      },
      'state' => {
        'inBaseline' => 'false',
        'down' => 'false'
      }
    },
    ....
  ]
}
```

api_mp_routers

RPC Call: RouteAnalyzer.api_mp_routers {password} {database name} {time} {filter}

This query lists all routers present in the multi-protocol network at the specified time. The results may be filtered to select only the routers running a particular protocol, for example.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_mp_routers ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";
$filter = $ARGV[2] if ($#ARGV >= 2);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("28 Feb 2005 15:50:22 PST");

push (@reqs, RPC::XML::request->new('RouteAnalyzer.api_mp_routers',
             RPC::XML::RPC_STRING($password),
             RPC::XML::RPC_STRING($database),
             RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
             RPC::XML::RPC_STRING($filter)));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print Dumper($value1);
}
```

Sample Output

```
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '100',
  'network_name' => 'pd353',
  'report_time' => '20051027T23:33:57',
  'totalEntries' => '100',
  'result' => [
    {
      'topology' => {
        'fullName' => 'pd353.Left.BGP/AS65522',
        'protocol' => 'BGP'
      },
      'numPrefixes' => '0',
      'router' => {
        'type' => 'Route Explorer',
        'ipaddr' => '192.168.0.49'
      },
      'state' => {
        'down' => 'false'
      }
    },
    {
      'topology' => {
        'fullName' => 'pd353.Left.ISIS/Level2',
        'protocol' => 'ISIS'
      },
      'numPrefixes' => '3',
      'router' => {
        'name' => 'labnet-gw',
        'type' => 'AreaBR',
        'ipaddr' => '192.168.104.254'
      },
      'state' => {
        'down' => 'false'
      }
    },
            ....
         ]
      }
```

api_prefix_events

RPC Call: RouteAnalyzer.api_prefix_events {password} {database name} {prefix}

This query returns a list of events for the specified prefix. Each event listing includes information about the prefix and the router that advertised that prefix.

Note The query returns the list of events for the specified prefix for the entire time interval covered by the requested database. This could result in a large number of entries returned in the result. To limit the number of entries, you can use the api_mp_events query instead by specifying the prefix as the filter.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`prefix`** – An XML struct that contains any prefix consisting of an IP4 address, such as `192.168.123.125`, and a mask length, such as `27.`

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_prefix_events ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_prefix_events',
             RPC::XML::RPC_STRING($password),
             RPC::XML::RPC_STRING($database),
             new RPC::XML::struct(ip_addr =>
                new RPC::XML::struct(ip4_addr => "169.229.147.0"),
                masklen => 25)));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper($value1) );

}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'network_name' => 'UCBJul03a',
  'report_time' => '20051027T18:42:29',
  'events' => [
    {
      'prefix' => {
        'eventType' => 'advertised',
        'time' => '20030722T22:10:56',
        'usec' => '521406',
        'prefix' => {
          'masklen' => '25',
          'ip_addr' => {
            'ip4_addr' => '169.229.147.0'
          }
        },
        'router' => {
          'nodeType' => 'AreaBR_ASBR',
          'ip_addr' => {
            'ip4_addr' => '128.32.1.209'
          },
          'nodeState' => 'UP',
          'nodeProto' => 'OSPF',
          'name' => '',
          'nodeArea' => 'UCBJul03a.OSPF/169.229.128.128',
          'maskLen' => '32',
          'systemID' => '128.32.1.209'
        }
      }
    },
    ....
  ]
```

```
        }
```

api_prefix_list

RPC Call: RouteAnalyzer.api_prefix_list {password} {database name} {time}

This query returns the list of all prefixes advertised in the database at a particular time. The example program below sends a request for the advertised prefixes at midnight on December 17, 2002 and displays the prefix information including the prefix IP address, type, area, and advertising routers.

Note This query is deprecated and may be removed in a future release. New applications should use api_mp_routes instead.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.

Example

```
#!/usr/bin/perl
use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $t1 = time2iso8601(str2time("17 Dec 2002 00:00:00 PST"));
my $request = RPC::XML::request->new(
      'RouteAnalyzer.api_prefix_list',
       RPC::XML::RPC_STRING( 'packet' ),  //password
       RPC::XML::RPC_STRING( 'CorpNet' ), //database name
       RPC::XML::datetime_iso8601->new($t1)
       );
my $client = new RPC::XML::Client 'http://hostname:2000/RPC2';
my $result = $client->send_request($request);
if ($result->is_fault) { print("--- XMLRPC FAULT ---"); }
print(STDERR join"\n","---XMLRPC RESULT---",Dumper($result->value), '');
```

Sample Output

```
--- XMLRPC RESULT ---
{
  'vinfo'=>{
    'software_version' => '3.7.2-R'
    'appliance_version' => '0.5.24',
  },
  'report_time' => '20030303T20:42:01',
  'network_name' => 'CorpNet',
  'prefixes' => [
  {
   'prefix_type' => 'Internal',
   'prefix_area' => '00000001/ospf',
   'prefix'=>{'ip_addr'=>{'ip4_addr'=>'192.168.240.1'},'masklen'=>'32'},
   'routers' => [
     {
      'nodeProto' => 'ospf',
      'ip_addr' => { 'ip4_addr' => '192.168.104.2' },
      'nodeType' => 'ASBR',
      'name' => '',
      'systemID' => '192168104002:00'
     }
     {'nodeProto'...'ip_addr'...'nodeType'...'name'...'systemID'...},
     {'nodeProto'...'ip_addr'...'nodeType'...'name'...'systemID'...}
     ] //end routers
     },
    {'prefix_type'...'prefix_area'...'prefix'...'routers'=> [...] },
    {'prefix_type'...'prefix_area'...'prefix'...'routers'=> [...] }
   ] //end prefixes
}
}
```

api_prefix_list_filtered

RPC Call: RouteAnalyzer.api_prefix_list_filtered {password} {database name} {router} {time}

This query returns a list of prefixes originated by the specified router at the specified time.

Note This query is deprecated and may be removed in a future release. New applications should use api_mp_routes instead.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`router`** – An XML struct that contains the router ID or a router interface address as an IPv4 address and a mask length of 32. The mask address is included for backward compatibility, but this query ignores it.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.

Example

```
#!/usr/bin/perl
if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_prefix_list_filtered ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
```

```
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("28 Feb 2005 15:50:22 PST");

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_prefix_list_filtered',
           RPC::XML::RPC_STRING($password),
           RPC::XML::RPC_STRING($database),
           RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
           new RPC::XML::struct (ip4_addr => "192.168.120.120") ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper($value1) );
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'network_name' => 'Lab',
  'report_time' => '20051031T22:58:04',
  'prefixes' => [
    {
      'routers' => [
        {
          'nodeType' => 'ASBR',
          'ip_addr' => {
            'ip4_addr' => '192.168.120.120'
          },
          'nodeState' => 'DOWN',
          'nodeProto' => 'Static',
          'name' => 'Router16',
          'nodeArea' => 'Lab.EIGRP/AS1',
          'maskLen' => '32',
          'systemID' => '192.168.120.120'
        },
        {
          'nodeType' => 'Internal',
          'ip_addr' => {
            'ip4_addr' => '192.168.220.20'
          },
          'nodeState' => 'DOWN',
          'nodeProto' => 'Static',
          'name' => 'Router20',
          'nodeArea' => 'Lab.EIGRP/AS1',
          'maskLen' => '32',
          'systemID' => '192.168.220.20'
        },
      ],
      'prefix_type' => 'Static',
      'prefix_area' => 'AllStaticRoutes.Static',
      'prefix' => {
        'masklen' => '0',
            'ip_addr' => {
              'ip4_addr' => '0.0.0.0'
            }
          }
        }
        ....
      ]
    }
```

api_prefix_list_multi_orig

RPC Call: RouteAnalyzer.api_prefix_list_multi_orig {password} {database name} {time}

This query returns a list of prefixes for the specified network that are originated by more than one router. This query returns a subset of the results returned by the api_prefix_list query.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_prefix_list_multi_orig ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = 1058927123;

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_prefix_list_multi_orig',
           RPC::XML::RPC_STRING($password),
           RPC::XML::RPC_STRING($database),
           RPC::XML::datetime_iso8601->new(time2iso8601($t1)) ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print (STDERR join "\n", Dumper($value1) );

}
```

Sample Output

```
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'network_name' => 'pd353',
  'report_time' => '20051028T00:45:15',
  'prefixes' => [
    {
      'routers' => [
        {
          'nodeType' => 'ASBR',
          'ip_addr' => {
            'ip4_addr' => '192.168.120.120'
          },
          'nodeState' => 'DOWN',
          'nodeProto' => 'Static',
          'name' => 'Router16',
          'nodeArea' => 'pd353.Left.EIGRP/AS1',
          'maskLen' => '32',
          'systemID' => '192.168.120.120'
        },
        {
          'nodeType' => 'ASBR',
          'ip_addr' => {
            'ip4_addr' => '192.168.122.122'
          },
          'nodeState' => 'DOWN',
          'nodeProto' => 'Static',
          'name' => 'Router26',
          'nodeArea' => 'pd353.Left.EIGRP/AS1',
          'maskLen' => '32',
          'systemID' => '192.168.122.122'
        },
        {
          'nodeType' => 'Internal',
          'ip_addr' => {
            'ip4_addr' => '192.168.220.20'
          },
          'nodeState' => 'DOWN',
          'nodeProto' => 'Static',
          'name' => 'Router20',
          'nodeArea' => 'pd353.Left.EIGRP/AS1',
          'maskLen' => '32',
          'systemID' => '192.168.220.20'
        },
      ],
      'prefix_type' => 'Static',
        'prefix_area' => 'AllStaticRoutes.Static',
        'prefix' => {
          'masklen' => '0',
          'ip_addr' => {
            'ip4_addr' => '0.0.0.0'
          }
        }
      }
      ....
    ]
  }
```

api_prefix_list_same

RPC Call: RouteAnalyzer.api_prefix_list_same {password} {database name} {time}

This query returns all routers advertising the same prefix or a more specific prefix for all prefixes advertised in the network by the specified database. Prefixes that are internal (native to the IGP) and those that are external (imported from another routing protocol) are compared separately.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.

Example

```
#!/usr/bin/perl
use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $t1 = time2iso8601(str2time("17 Dec 2002 00:00:00 PST"));
my $request = RPC::XML::request->new(
   'RouteAnalyzer.api_prefix_list_same',
    RPC::XML::RPC_STRING( 'admin' ),   //password
    RPC::XML::RPC_STRING( 'CorpNet' ),  //database name
    RPC::XML::datetime_iso8601->new($t1)
    );
my $client = new RPC::XML::Client 'http://hostname:2000/RPC2';
my $result = $client->send_request($request);
if ($result->is_fault) { print("--- XMLRPC FAULT ---"); }
print(STDERR join "\n", "--- XMLRPC RESULT ---", Dumper($result->value), '');
```

Sample Output

```
--- XMLRPC RESULT ---
{
  'vinfo' => {
```

```
  'software_version' => '3.7.2-R'
  'appliance_version' => '0.5.24',
},
'report_time' => '20030303T20:52:20',
'network_name' => 'CorpNet',
'prefixes' => [
  {
    'prefix_type' => 'Area-Ext',
    'prefix_area' => '00000001/ospf',
    'prefix' => {
       'ip_addr' => {
           'ip4_addr' => '192.168.200.200'
         },
    'masklen' => '24'
    },
    'routers' => [
      {
        'nodeProto' => 'ospf',
        'ip_addr' => {
            'ip4_addr' => '192.168.201.201'
            },
        'nodeType' => 'ASBR',
        'name' => '',
        'systemID' => '091001011001:00'
      },
      {'nodeProto'...'ip_addr'...'nodeType'...'name' ...'systemID' ...}
      {'nodeProto'...'ip_addr'...'nodeType'...'name' ...'systemID' ...}
    ] // end routers
  }, // end first prefix
   {'prefix_type'...'prefix_area'...'prefix'.... 'routers' => [...]},
   {'prefix_type'...'prefix_area'...'prefix'.... 'routers' => [...]}
  ] // end prefixes
}
```

api_router_events

RPC Call: RouteAnalyzer.api_router_events {password} {database name} {router}

This query returns a list of events associated with the specified router.

Note This query is deprecated and may be removed in a future release. New applications should use api_mp_events instead.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`router`** – An XML struct that contains the router ID or a router interface address as an IPv4 address and a mask length of 32. The mask address is included for backward compatibility, but this query ignores it.

Example

```
#!/usr/bin/perl
if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_router_events ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_router_events',
            RPC::XML::RPC_STRING($password),
            RPC::XML::RPC_STRING($database),
            new RPC::XML::struct(ip_addr =>
                new RPC::XML::struct(ip4_addr => "128.32.1.211"))
                ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper($value1) );
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'network_name' => 'UCBJul03a',
  'report_time' => '20051027T19:01:13',
  'events' => [
    {
      'router' => {
        'eventType' => 'advertised',
        'time' => '20030722T22:10:56',
        'usec' => '581591',
        'router' => {
          'nodeType' => 'ASBR',
          'ip_addr' => {
            'ip4_addr' => '128.32.1.211'
          },
          'nodeState' => 'DOWN',
          'nodeProto' => 'OSPF',
          'name' => '',
          'nodeArea' => 'UCBJul03a.OSPF/169.229.128.128',
          'maskLen' => '32',
          'systemID' => '128.32.1.211'
        }
      }
    },
    {
      'router' => {
        'eventType' => 'advertised',
        'time' => '20030722T22:10:52',
        'usec' => '851696',
        'router' => {
          'nodeType' => 'ASBR',
          'ip_addr' => {
            'ip4_addr' => '128.32.1.211'
          },
          'nodeState' => 'DOWN',
          'nodeProto' => 'OSPF',
          'name' => '',
          'nodeArea' => 'UCBJul03a.OSPF/169.229.128.168',
          'maskLen' => '32',
          'systemID' => '128.32.1.211'
        }
      }
    },
                ....
            ]
        }
```

api_router_list

RPC Call: RouteAnalyzer.api_router_list {password} {database name} {time}

This query returns a list of routers for the specified network.

Note This query is deprecated and may be removed in a future release. New applications should use api_mp_routers instead.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_router_list ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req; my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("24 Jul 2003 11:00:00 PST");

push (@reqs, RPC::XML::request->new('RouteAnalyzer.api_router_list',
             RPC::XML::RPC_STRING($password),
             RPC::XML::RPC_STRING($database),
             RPC::XML::datetime_iso8601->new(time2iso8601($t1))
```

```
            ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print ("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper($value1) );
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'routers' => [
    {
      'nodeType' => 'Internal',
      'ip_addr' => {
        'ip4_addr' => '169.229.128.130'
      },
      'nodeState' => 'UP',
      'nodeProto' => 'OSPF',
      'name' => '',
      'nodeArea' => 'UCBJul03a.OSPF/169.229.128.128',
      'maskLen' => '32',
      'systemID' => '169.229.128.130'
    },
    {
      'nodeType' => 'AreaBR_ASBR',
      'ip_addr' => {
        'ip4_addr' => '128.32.1.209'
      },
      'nodeState' => 'UP',
      'nodeProto' => 'OSPF',
      'name' => '',
      'nodeArea' => 'UCBJul03a.OSPF/169.229.128.128',
      'maskLen' => '32',
      'systemID' => '128.32.1.209'
    },
    {
      'nodeType' => 'Internal',
      'ip_addr' => {
        'ip4_addr' => '169.229.2.66'
      },
      'nodeState' => 'UP',
      'nodeProto' => 'OSPF',
      'name' => '',
      'nodeArea' => 'UCBJul03a.OSPF/169.229.128.168',
      'maskLen' => '32',
      'systemID' => '169.229.2.66'
    },
    ....
  ],
  'network_name' => 'UCBJul03a',
  'report_time' => '20051028T00:00:05'
}
```

api_router_summarizable

RPC Call: RouteAnalyzer.api_router_summarizable {password} {database name} {time}

This query returns a list of routers that, at the specified time, are advertising multiple prefixes that could be summarized as a single prefix. For each such router, RAMS provides a list of potential summary prefixes with their component prefixes. Prefixes that are internal (native to the IGP) and those that are external (imported from another routing protocol) are considered separately.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.EIGRP/AS100.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.

Example

```
#!/usr/bin/perl
use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $t1 = time2iso8601(time);
my $request = RPC::XML::request->new(
      'RouteAnalyzer.api_router_summarizable',
       RPC::XML::RPC_STRING( 'admin' ),   //password
       RPC::XML::RPC_STRING( 'CorpNet' ),  //database name
       RPC::XML::datetime_iso8601->new($t1)
       );
my $client = new RPC::XML::Client 'http://hostname:2000/RPC2';
my $result = $client->send_request($request);
if ($result->is_fault) { print("--- XMLRPC FAULT ---"); }
print(STDERR join "\n", "--- XMLRPC RESULT ---", Dumper($result->value), '');
```

Sample Output

```
--- XMLRPC RESULT ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R'
    'appliance_version' => '0.5.24',
  },
  'report_time' => '20030303T21:09:29',
  'network_name' => 'CorpNet',
  'routers' => [
    {
      'router' => {
        'nodeProto' => 'ospf',
        'ip_addr' => {
            'ip4_addr' => '192.168.140.140'
         },
        'nodeType' => 'AreaBR',
        'name' => '',
        'systemID' => '004001001012:00'
      },
      'summarizable_prefixes' => [
        {
          'summary' => {
            'ip_addr' => {
                'ip4_addr' => '192.168.150.150'
            },
            'masklen' => '31'
          }, // end summary
          'contributors' => [
            {
              'ip_addr' => {
                   'ip4_addr' => '192.168.150.150'
              },
              'masklen' => '32'
            },
            {
              'ip_addr' => {
                    'ip4_addr' => '192.168.150.151'
              },
              'masklen' => '32'
            }
          ] // end contributors
        },
        {'summary' ...  'contributors' },
        {'summary' ...  'contributors' }
          ] // end summarizable_prefixes
        }, // end first router
       {'router' => {...}, 'summarizable_prefixes' => [...]},
        {'router' => {...}, 'summarizable_prefixes' => [...]}
       ] // end routers
      }
```

api_vpn_cust_rt_list

RPC Call: RouteAnalyzer.api_vpn_cust_rt_list {password} {database name} {operation} {customer name} {route target}

This query returns a list of all VPN customer name to route target (RT) mappings for the specified database. When issued with the `get` operation, no change is made to the list of mappings. This query also supports additional operations (`add`, `del`, `reset`) to modify the list of mappings, as specified below, in addition to returning the list.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – May be an administrative domain, such as CorpNet, which selects the VPN database included in the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **`operation`** – The specific operation to be performed. This is indicated by a string that can have the value '`get`' to return the list of mappings, '`add`' to add a VPN customer, '`del`' to delete a VPN customer, and '`reset`' to delete all the mappings.
- **`customer name`** – The empty string for the `get` and `reset` operations; the name of the VPN customer for the `add` and `del` operations.
- **`route target`** – The empty string for the `get` and `reset` operations; the name of the route target for the `add` and `del` operations.

Example

```
#!/usr/bin/perl
if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_vpn_cust_rt_list ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_vpn_cust_rt_list',
                                    RPC::XML::RPC_STRING($password),
                                    RPC::XML::RPC_STRING($database),
                                    RPC::XML::RPC_STRING('get'),
                                    RPC::XML::RPC_STRING(''),
                                    RPC::XML::RPC_STRING('')
                                ));

foreach (@reqs) {
        my $res = $client->send_request($_);
        if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
        my $value1 = $res->value;

}
```

Sample Output

```
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'network_name' => 'CorpNet',
  'vpn_cust_rts' => [
    {
      'name' => 'Customer1',
      'rt' => 'RT:65535:101'
    },
    {
      'name' => 'Customer2',
      'rt' => 'RT:65533:101'
    }
  ]
}
```

api_vpn_customer_pe_participation

RPC Call: RouteAnalyzer.api_vpn_customer_pe_participation {password} {database name} {time} {filter}

This query returns statistics of participating PEs for each VPN customer.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_vpn_customer_pe_participation ip
database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";

$filter = $ARGV[2] if ($#ARGV >= 2);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("28 Feb 2005 15:50:22 PST");

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_vpn_customer_pe_particip
ation',
    RPC::XML::RPC_STRING($password),
    RPC::XML::RPC_STRING($database),
    RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
    RPC::XML::RPC_STRING($filter) ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print Dumper($value1);
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '50',
  'network_name' => 'VOD',
  'report_time' => '20051115T19:19:00',
  'totalEntries' => '50',
  'result' => [
    {
      'customer' => 'Cust747',
      'numActivePEs' => '0',
      'deviation' => '100',
      'numNewPEs' => '0',
      'numDownPEs' => '0',
      'definition' => 'RT:600:1',
      'numBaselinePEs' => '0'
    }
    ....
  ]
}
```

api_vpn_customer_pe_list

RPC Call: RouteAnalyzer.api_vpn_customer_privacy {password} {database name} {time} {customer name} {filter}

This query returns the list of participating PEs for the specified VPN customer.

Input Parameters

- **password** – The password configured for queries.
- **database name** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **time** – A time specified in ISO 8601 format in the UTC timezone, such as 20050725T21:47:35. The query results will be calculated based on the network state at the specified time.
- **customer name** – Name of the VPN customer for which the list of PEs is desired.
- **filter** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter "any" to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1]) || !defined($ARGV[2])) {
    printf "usage: RouteAnalyzer.api_vpn_customer_pe_list ip database 
customer\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $customer = $ARGV[2];
my $filter = "any";
$filter = $ARGV[3] if ($#ARGV >= 3);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("30 Aug 2005 00:26:30 PDT");

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_vpn_customer_pe_list',
    RPC::XML::RPC_STRING($password),
    RPC::XML::RPC_STRING($database),
    RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
    RPC::XML::RPC_STRING($customer),
    RPC::XML::RPC_STRING($filter) ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper($value1) );
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '1',
  'network_name' => 'VOD',
  'report_time' => '20051115T19:14:20',
  'totalEntries' => '1',
  'result' => [
    {
      'PE' => {
        'type' => 'Originator',
        'ipaddr' => '192.168.180.180'
      },
      'vpnState' => {
        'inBaseline' => 'false',
        'down' => 'true'
      }
    }
  ]
}
```

api_vpn_customer_reachability

RPC Call: RouteAnalyzer.api_vpn_customer_reachability {password} {database name} {time} {filter}

This query returns reachability statistics for each VPN customer. Reachability is specified in terms of the percentage deviation from the baseline reachability. For example, this could be negative if some routes are down and fewer routes are available than those at baseline. This could be positive if new routes have been added that were not known at baseline.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_vpn_customer_reachability ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";

$filter = $ARGV[2] if ($#ARGV >= 2);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("28 Feb 2005 15:50:22 PST");

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_vpn_customer_reachabilit
y',
    RPC::XML::RPC_STRING($password),
    RPC::XML::RPC_STRING($database),
    RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
    RPC::XML::RPC_STRING($filter) ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print Dumper($value1);
}
```

Sample Output

```
---XMLRPC RESULT value1 ---

{
    'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '50',
  'network_name' => 'VOD',
  'report_time' => '20051115T19:19:49',
  'totalEntries' => '50',
  'result' => [
    {
      'numDownRoutes' => '1',
      'numActiveRoutes' => '0',
      'numNewRoutes' => '0',
      'numPEs' => '0',
      'customer' => 'Cust747',
      'deviation' => '100',
      'numBaselineRoutes' => '1',
      'definition' => 'RT:600:1'
    }
   ....
  ]
}
```

api_vpn_customer_reachability_by_peer

RPC Call: RouteAnalyzer.api_vpn_customer_reachability_by_peer {password} {database name} {time} {customer name} {filter}

This query returns reachability statistics at each PE for the specified VPN customer. Reachability is specified in terms of the percentage deviation from the baseline reachability. For example, this could be negative if some routes are down and fewer routes are available than those at baseline. This could be positive if new routes have been added that were not known at baseline.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`customer name`** – Name of the VPN customer for which reachability information is desired.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter "any" to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1]) || !defined($ARGV[2])) {
    printf "usage: RouteAnalyzer.api_vpn_customer_reachability_by_peer ip
database customer\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $customer = $ARGV[2];
my $filter = "any";

$filter = $ARGV[3] if ($#ARGV >= 3);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("30 Aug 2005 00:26:30 PDT");

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_vpn_customer_reachabilit
y_by_peer',
RPC::XML::RPC_STRING($password),
RPC::XML::RPC_STRING($database),
RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
RPC::XML::RPC_STRING($customer),
RPC::XML::RPC_STRING($filter) ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper($value1) );
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '25',
  'network_name' => 'VOD',
  'report_time' => '20051115T19:12:35',
  'totalEntries' => '25',
  'result' => [
    {
      'numDownRoutes' => '0',
      'numActiveRoutes' => '1',
      'numNewRoutes' => '0',
      'PE' => {
        'type' => 'Originator',
        'ipaddr' => '192.168.180.180'
      },
      'deviation' => '0',
      'numBaselineRoutes' => '1',
            'vpnState' => {
              'inBaseline' => 'false',
              'down' => 'true'
            }
          }
        ]
      }
```

api_vpn_route_target_pe_participation

RPC Call: RouteAnalyzer.api_vpn_route_target_pe_participation {password} {database name} {time} {filter}

This query returns statistics of participating PEs for each route target in the specified network. This includes information about the route target, the deviation from baseline, and the number of PEs that are active, down, or newly added after baseline.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_vpn_route_target_pe_participation ip 
database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";

$filter = $ARGV[2] if ($#ARGV >= 2);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("28 Feb 2005 15:50:22 PST");

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_vpn_route_target_pe_par
ticipation',
    RPC::XML::RPC_STRING($password),
    RPC::XML::RPC_STRING($database),
    RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
    RPC::XML::RPC_STRING($filter) ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print Dumper($value1);
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '50',
  'network_name' => 'pd353',
  'report_time' => '20051028T00:23:42',
  'totalEntries' => '50',
  'result' => [
    {
      'routeTarget' => 'RT:65522:600',
      'numActivePEs' => '3',
      'deviation' => '100',
      'numNewPEs' => '3',
      'numDownPEs' => '0',
      'numBaselinePEs' => '0'
    },
    {
      'routeTarget' => 'RT:65522:2300',
      'numActivePEs' => '1',
      'deviation' => '100',
      'numNewPEs' => '1',
      'numDownPEs' => '0',
      'numBaselinePEs' => '0'
    },
    {
      'routeTarget' => 'RT:65522:500',
      'numActivePEs' => '2',
      'deviation' => '100',
      'numNewPEs' => '2',
        'numDownPEs' => '0',
        'numBaselinePEs' => '0'
      },
      {
        'routeTarget' => 'RT:65522:1500',
        'numActivePEs' => '2',
        'deviation' => '100',
        'numNewPEs' => '2',
        'numDownPEs' => '0',
        'numBaselinePEs' => '0'
      },
      ....
    ]
  }
```

api_vpn_route_target_pe_list

RPC Call: RouteAnalyzer.api_vpn_route_target_privacy_by_peer {password} {database name} {time} {route target} {filter}

This query returns the list of participating PE routers and their VPN state for the specified route target.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`route target`** – A label specifying the route target of interest, e.g., RT:600:1.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1]) || !defined($ARGV[2])) {
    printf "usage: RouteAnalyzer.api_vpn_route_target_pe_list ip database 
route-target\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $route_target = $ARGV[2];
my $filter = "any";

$filter = $ARGV[3] if ($#ARGV >= 3);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("28 Aug 2005 15:50:22 PDT");

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_vpn_route_target_pe_list
',
    RPC::XML::RPC_STRING($password),
    RPC::XML::RPC_STRING($database),
    RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
    RPC::XML::RPC_STRING($route_target),
    RPC::XML::RPC_STRING($filter) ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper($value1) );
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '25',
  'network_name' => 'VOD',
  'report_time' => '20051108T19:51:50',
  'totalEntries' => '25',
  'result' => [
    {
      'PE' => {
        'type' => 'Originator',
        'ipaddr' => '192.168.180.180'
      },
      'vpnState' => {
        'inBaseline' => 'false',
        'down' => 'true'
      }
    }
  ]
}
```

api_vpn_route_target_reachability

RPC Call: RouteAnalyzer.api_vpn_route_target_reachability {password} {database name} {time} {filter}

This query returns reachability statistics for each route target in the specified network. This includes information about the deviation from baseline and the number of routes that are down, active, and newly added after the baseline.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_vpn_route_target_reachability ip
database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";

$filter = $ARGV[2] if ($#ARGV >= 2);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";
my $t1 = str2time("28 Jul 2004 08:25:51 PST");

push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_vpn_route_target_reachab
ility',
    RPC::XML::RPC_STRING($password),
    RPC::XML::RPC_STRING($database),
    RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
    RPC::XML::RPC_STRING($filter) ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;
print Dumper($value1);
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '50',
  'network_name' => 'pd353',
  'report_time' => '20051027T23:25:19',
  'totalEntries' => '50',
  'result' => [
    {
      'routeTarget' => 'RT:65522:100',
      'numDownRoutes' => '0',
      'numActiveRoutes' => '0',
      'numPEs' => '0',
      'numNewRoutes' => '0',
      'deviation' => '100',
      'numBaselineRoutes' => '0'
    },
    {
      'routeTarget' => 'RT:65522:600',
      'numDownRoutes' => '0',
      'numActiveRoutes' => '0',
      'numPEs' => '0',
      'numNewRoutes' => '0',
      'deviation' => '100',
      'numBaselineRoutes' => '0'
    },
    {
      'routeTarget' => 'RT:65522:2400',
      'numDownRoutes' => '0',
      'numActiveRoutes' => '0',
      'numPEs' => '0',
      'numNewRoutes' => '0',
      'deviation' => '100',
                'numBaselineRoutes' => '0'
              },
              {
                'routeTarget' => 'RT:65522:700',
                'numDownRoutes' => '0',
                'numActiveRoutes' => '0',
                'numPEs' => '0',
                'numNewRoutes' => '0',
                'deviation' => '100',
                'numBaselineRoutes' => '0'
              }
              ....
            ]
          }
```

api_vpn_route_target_reachability_by_peer

RPC Call: RouteAnalyzer.api_vpn_route_target_reachability_by_peer {password} {database name} {time} {route target} {filter}

This query returns reachability statistics at each PE for the specified route target. This includes information about the deviation from baseline and the number of routes that are down, active, and newly added after the baseline.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`route target`** – A label specifying the route target of interest, e.g., RT:600:1.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter “any” to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1]) || !defined($ARGV[2])) {
    printf "usage: RouteAnalyzer.api_vpn_route_target_reachability_by_peer ip 
database route_target\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";
my $route_target = $ARGV[2];

$filter = $ARGV[3] if ($#ARGV >= 3);
```

```
use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("28 Aug 2005 16:16:45 PDT");


push (@reqs,
RPC::XML::request->new('RouteAnalyzer.api_vpn_route_target_reacha
bility_by_peer',
RPC::XML::RPC_STRING($password),
RPC::XML::RPC_STRING($database),
RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
RPC::XML::RPC_STRING($route_target),
RPC::XML::RPC_STRING($filter) ));

foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print (STDERR join "\n", "---XMLRPC RESULT value1 ---", Dumper($value1) );
}
}
```

Sample Output

```
---XMLRPC RESULT value1 ---
{
  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '20',
  'network_name' => 'VOD',
  'report_time' => '20051108T20:04:47',
  'totalEntries' => '20',
  'result' => [
    {
      'numDownRoutes' => '0',
      'numActiveRoutes' => '1',
      'numNewRoutes' => '1',
      'PE' => {
        'type' => 'Originator',
        'ipaddr' => '192.168.180.180'
      },
      'deviation' => '100',
      'numBaselineRoutes' => '0',
      'vpnState' => {
        'inBaseline' => 'false',
        'down' => 'true'
      }
    }
  ]
}
```

api_vpn_routes

RPC Call: RouteAnalyzer.api_vpn_routes {password} {database name} {time} {filter}

This query returns the list of VPN routes for the specified network.

Input Parameters

- **`password`** – The password configured for queries.
- **`database name`** – One or more space-separated names from the database hierarchy. Each name may be an administrative domain, such as CorpNet, which includes the subtree below it, or a complete database name, such as CorpNet.BGP/AS65522/VPN.
- **`time`** – A time specified in ISO 8601 format in the UTC timezone, such as `20050725T21:47:35`. The query results will be calculated based on the network state at the specified time.
- **`filter`** – A filter expression to limit the results to the subset matching the filter parameters. See Expression Syntax on page 228 for more information about filter expressions. Use the filter "any" to return the full results.

Example

```
#!/usr/bin/perl

if(!defined($ARGV[0]) || !defined($ARGV[1])) {
    printf "usage: RouteAnalyzer.api_vpn_routes ip database\n";
    exit(0);
}

my $rexip = $ARGV[0];
my $database = $ARGV[1];
my $filter = "any";

$filter = $ARGV[2] if ($#ARGV >= 2);

use strict;
use RPC::XML::Client;
use RPC::XML 'time2iso8601';
use Date::Parse;
use Data::Dumper; $Data::Dumper::Terse = 1; $Data::Dumper::Indent = 1;
my $client;
my $req;
my @reqs;
my $password = 'admin';
```

```
$client = new RPC::XML::Client "http://$rexip:2000/RPC2";

my $t1 = str2time("28 Feb 2005 15:50:22 PST");

push (@reqs, RPC::XML::request->new('RouteAnalyzer.api_vpn_routes',
    RPC::XML::RPC_STRING($password),
    RPC::XML::RPC_STRING($database),
    RPC::XML::datetime_iso8601->new(time2iso8601($t1)),
    RPC::XML::RPC_STRING($filter) ));
foreach (@reqs) {
my $res = $client->send_request($_);
if ($res->is_fault) {print("---XMLRPC FAULT ---"); }
my $value1 = $res->value;

print Dumper($value1);
}
```

Sample Output

```
---XMLRPC RESULT value1 ---

  'vinfo' => {
    'software_version' => '3.7.2-R',
    'appliance_version' => '0.5.24'
  },
  'numReturnedEntries' => '20',
  'network_name' => 'pd353',
  'report_time' => '20051027T21:40:07',
  'totalEntries' => '20',
  'result' => [
    {
      'topology' => {
        'fullName' => 'pd353.Left.BGP/AS65522/VPN',
        'protocol' => 'BGP'
      },
      'vpnPrefix' => {
        'labelStack' => '20543',
        'prefix' => '65522:700:192.168.230.230/24'
      },
      'attributes' => {
        'mpReachabilityNextHop' => '0:192.168.104.12',
        'extCommunities' => 'RT:65522:700 ',
        'origin' => 'INCOMPLETE',
        'localPref' => '100',
        'asPath' => '',
        'med' => '0'
      },
      'router' => {
        'type' => 'IBGP Peer',
        'ipaddr' => '192.168.200.200'
      },
      'state' => {
        'inBaseline' => 'false',
        'down' => 'false'
      }
    },
    ....

  ]
}
```

Index