

HP Route Analytics Management System

Software Version: 8.10

User's Guide

Manufacturing Part Number: T9424-90003

Document Release Date: December 2008

Software Release Date: December 2008



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 1999–2008 Hewlett-Packard Development Company, L.P.

Contains software from Packet Design, Inc.

© Copyright 2008 Packet Design, Inc.

Trademark Notices

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

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

Unix® is a registered trademark of The Open Group.

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

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

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software Support web site at:

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

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

HP Software Support Online 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 valued support customer, you can benefit by using the HP Software Support web site to:

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

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

To find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Contents

1	Introduction	17
	About Route Analytics Management System	18
	How Route Analytics Management System Operate	19
	Key Components of Route Analytics Management System	19
	Using Route Analytics Management System	23
	The Web Interface	23
	The Application Interface	24
2	Viewers	27
	Understanding Viewer Options	28
	Installing an X Window Server	28
	Using X Window System Software for MS Windows	28
	Using X Window Server for UNIX Platforms	31
	Installing VNC Viewer	32
	Downloading VNC	32
	Downloading and Installing VNC on Windows	33
	Downloading and Installing VNC on Linux	34
	Installing SVG Plug-In	35
	View System Information	36
	Opening the Client Application	36
	X Windows	36
	VNC	37
3	The Routing Topology Map	39
	Working with Routing Topology Maps	39
	Opening a Routing Topology Map	40
	Symbols and Colors	42
	Links and Peerings	43

Legend Panel	43
Network Summary Panel	45
Main Window Status Bar	47
Main Window Toolbar	49
Main Window Menus	53
Topology	54
View	55
Tools	56
Reports	58
Planning	58
Alerts	60
Administration	60
Help	62
Topology Map Layouts and Background Images	63
Understanding the Topology Hierarchy	64
Viewing Network Anomalies	67
Applying Configuration Options	67
Analysis	69
Visualization Options	69
Algorithmic Analysis Options	69
Node Labels	70
Colors	70
Miscellaneous	71
History Navigator	73
Auto-Hide	74
Working with Router Information and Layout	76
Viewing Node and Link Details	76
Node Information Panel	77
Link Information Panel	79
Hiding Nodes	82
Finding a Router	84
Viewing Exit Routers	84
Creating Custom Filters	85
Assigning Router Names	88
Changing Multiple Router Names	90
Viewing Current Network Inventory	91

Router List	91
Links List	92
Interfaces List	94
Prefix List.	94
OSI Prefixes List	96
VPN Prefixes List	96
Understanding Topology Groups.	97
Creating Groups on the Topology Map	98
Creating Groups Using the Menu	104
Working with Groups	106
Hiding Forwarding Adjacencies in Link Groups	112
Understanding Network Routes	114
Highlighting the IP Route Between Two Points in the Network.	114
Finding a Route By Prefix	116
Finding a VPN Route By Prefix	117
Viewing the Highlighted Path Cost for EIGRP.	118
Diagnosing EIGRP Topology Errors	121
List Topology Errors	122
List Inaccessible Routers.	123
List Mismatched Distances.	125
Find Invisible Links	128
Assigning AS Names	128
Assign and Verify BGP AS Assignments to Routers.	131
4 The History Navigator	133
Understanding the History Navigator	134
Accessing the History Navigator.	135
Working With the History Navigator	136
History Navigator Controls	136
Modes	136
Status Bar	138
Cursor.	138
Buttons.	138
Playback Controls	139
Logarithmic Units	140
Zooming the Time Line	140

History Graphs	141
Analyzing Historical Data	143
Root Cause Analysis	143
Animation Window	146
Playing an Animation	148
Saving an Animation	150
RIB Visualization	151
Generating a Visualization	151
Changing RIB Visualization Thresholds	152
Saving a Visualization	156
RIB Browser	158
IGP Protocols	159
BGP Protocol	161
VPN Protocol	163
OSI ISIS Protocol	163
RIB Comparison	165
IGP Protocols	166
BGP Protocols	167
VPN Protocol	169
OSI ISIS Protocol	169
Trending	169
Event Analysis	171
IGP Protocols	171
BGP Protocol	173
VPN Protocol	174
OSI ISIS Protocol	174
Flow Record Browser	175
Understanding the Events List	177
Events List Controls	179
Event Details	179
Event Operations and Attributes	181
Highlighting Associated Nodes	184
Filtering the Events List	184
Adjusting the Time Range	185
Moving Time and Executing Events	186
Using the History Navigator as a Forensic Tool	187

Correlating Time Series Data	193
Using Filters.....	195
Expression Syntax	199
Examples.....	199
Regular Expression.....	200
Expression Definitions	200
5 Network Planning	219
About the Network Planning Tools.....	220
Planning Menu	221
The Planning Toolbar.....	225
Add Router	226
Adding a Protocol Instance to an Existing Node	227
Add Peering.....	227
Add BGP Peering.....	227
Add IGP Peering	229
Add a Prefix.....	230
Adding a Prefix for BGP or BGP/MPLS-VPN Routers	230
Add prefix for ISIS Routers.....	234
Edit a BGP Prefix	235
Add VRF	235
Add IPv4 Traffic Flow.....	237
Add VPN Traffic Flows.....	239
Add VPN Customer	242
Edit BGP Prefixes.....	244
Edit Traffic Flows	246
Add a Flow Server	247
Add a Traffic Flow	249
Change the Bitrate of a Flow	249
Delete a Flow from a Router	250
Move a Traffic Flow from One Router to Another	250
Edit VPN Traffic Flows	251
Using the VPN Filter.....	252
Edit Node Properties	253
Edit VRFs	254
Bring Down a Router	254

Bring Down Peerings	255
Bring Down a Prefix	257
Bring Down VRF	258
Working with Planning Reports	259
Planning Report Access	260
Navigation Tree	260
Drill-down Function	261
Planning Report Icons	262
Edits	262
Advanced Filtering	264
Understanding Planning Reports	264
Aggregate Reports	264
Links Report	265
CoS Report	266
CoS Links Report	266
Exporters Report	266
Interfaces Report	267
Flow Collectors Report	267
Flows Report	267
IPv4 Planning Reports	268
Links Report	268
CoS Report	269
CoS Links Report	269
Exporters Report	270
Interfaces Report	270
Traffic Groups Report	270
Flows Report	271
BGP Traffic Reports	271
Egress Router Report	272
Neighbor AS Report	272
Transit AS Report	272
Source AS Report	273
Destination AS Report	273
Community Report	274
VPN Traffic Reports	274
VPN Links Report	275

VPN CoS Report	275
VPN CoS Links Report	275
VPN CoS Customers Report	276
VPN Customers Report	276
Ingress PE Report	277
Exporters Report	277
Interfaces Report	277
Egress PE Report	278
VPN Flows Report	278
Working with Capacity Planning Tools	279
Navigation Tree and Report Window Settings	279
Aggregate Capacity Planning Reports	281
Links Report	281
CoS Report	281
CoS Links Report	283
Exporters Report	283
Interfaces Report	284
Flow Collectors Report	284
IPv4 Capacity Planning Reports	284
Links Report	285
CoS Report	285
CoS Links Report	286
Exporters Report	286
Interfaces Report	286
Traffic Groups Report	288
BGP Capacity Planning Reports	288
Egress Router Report	288
Neighbor AS Report	289
Transit AS Report	289
Source AS Report	289
Destination AS Report	290
VPN Capacity Planning Traffic Reports	291
VPN Links Report	291
VPN CoS Report	291
VPN CoS Links Report	293
VPN CoS Customers Report	293

VPN Customers Report	293
Ingress PE Report	295
Exporters Report	295
Interfaces Report	295
Egress PE Report	296
Show Edits	296
6 IGP Reports	299
Understanding IGP Reports	300
Accessing the IGP Report Pages	300
Configuring IGP Reports	301
Understanding IGP Report Contents	303
Network Events Summary	303
Changed Metrics	304
Flapping Links	305
Network Churn	306
New Prefixes	307
New Routers and Links	308
Prefix List	309
Prefix Origination Changes	311
Prefix Origination from Multiple Sources	312
Prefixes Withdrawn	314
7 BGP Reports	317
Understanding BGP Reports	318
Accessing the BGP Report Pages	319
Generating BGP Activity Reports	320
BGP Activity Summary Report	320
BGP Activity by AS Report	321
BGP Activity by Peer Report	322
Route Flap Report	322
Prefix Event Detail	323
Creating BGP Logical Topology Reports	323
Route Distribution Detail Route Distribution Detail Report	324
Route Distribution Detail By RRC Report	325
Route Distribution Detail By Next Hop Report	325

Route Distribution Detail By Next Hop AS Report	325
Route Distribution Detail By Peer Router.	325
Redundancy by Prefix Report.	326
Baseline Redundancy by Prefix Report	326
AS Reachability Report	326
Baseline AS Reachability Report	328
Prefix Reachability Report	328
8 VPN Routing	329
About VPN Routing	330
Understanding the Reachability and Participation Index.	331
Creating Customer and RT Associations	332
Generating XML Customer Reports	335
Viewing VPN Routing Reports	337
Modifying the Report Table	338
VPN Summary Report	339
VPN Prefixes Report.	340
VPN Customers History Report.	341
VPN Reachability History Report	342
VPN Reachability Customers Report	343
VPN PE Participation History Report	345
VPN PE Participation Customers Report	346
Obtaining Detailed Information.	347
Details by PE	348
List Routes	348
Highlight PEs.	348
Show Map.	348
Reachability over Time	348
PE Participation.	349
IPv4 Routers Report	350
IPv4 Links Report.	350
IPv4 Prefixes Report.	350
History Navigator	350
9 Traffic Reports	351
Understanding Traffic Reports	351

Accessing Traffic Reports	353
Navigation Tree	354
Traffic Reports Buttons	355
Working with Traffic Reports	356
Columns Settings	357
Statistics Column Area	358
Difference Column Area	359
Advanced Filtering	359
Minute Data Granularity	359
Drill-Down Capabilities	360
Drill-Down History Option	363
Setting Interface Capacities	364
Understanding Report Types	367
Top Changes Report	369
Aggregate Reports	371
Aggregate – Links	371
Aggregate—CoS	373
Aggregate—CoS Links	373
Aggregate – Exporters	375
Aggregate – Exporters Interfaces	376
Aggregate – Flow Collectors	376
Aggregate – Flows	377
Aggregate – CoS Groups Definition	378
IPv4 Traffic Reports	379
IPv4 Traffic – Links	379
IPv4 Traffic – CoS	380
IPv4 Traffic - CoS Links	381
IPv4 Traffic – Exporters	382
IPv4 Traffic – Interfaces	383
IPv4 Traffic – Traffic Groups	384
IPv4 Traffic – Top Sources	384
IPv4 Traffic – Top Destinations	385
IPv4 Traffic – Protocols	386
IPv4 Traffic – Flows	386
IPv4 Traffic – Traffic Groups Definition	388

BGP Traffic Reports	388
BGP Traffic – Egress Router	389
BGP Traffic – Neighbor AS	390
BGP Traffic – Transit AS	391
BGP Traffic – Source AS	391
BGP Traffic – Destination AS	392
BGP Traffic – Community	393
VPN Traffic Reports	394
VPN Traffic – Links	394
VPN Traffic – Class of Service (CoS)	395
VPN Traffic – Class of Service (CoS) Links	396
VPN Traffic – CoS Customers	397
VPN Traffic – Customers	398
VPN Traffic – Ingress PE	399
VPN Traffic – Exporters	399
VPN Traffic – Interfaces	400
VPN Traffic – Egress PE	401
VPN Traffic – Flows	401
10 Path Reports	403
Understanding Path Reports	404
Accessing the Path Reports Window	404
Using the Path Reports Window	407
Viewing Path Analysis Reports	408
Path Statistics Report	409
Path Statistics by Source	412
Path Statistics by Destination	413
ECMP Paths Analysis	414
Single (Non-ECMP) Path Analysis	415
Asymmetric Paths Analysis	416
Asymmetric Paths by Path	417
Asymmetric Paths by Metric	417
Asymmetric Paths by Source	418
Asymmetric Paths by Destination	418
Network Element Analysis	418
Router Hot Spots	419

Link Hot Spots	420
Unused Links	421
Down Nodes	423
Down Links	423
Asymmetric Link Metrics	424
Failure Analysis	424
Path Failure Analysis	425
Link Failure Analysis	426
Failure-induced ECMP Analysis	427
11 Alerts	429
Understanding Alerts	430
Viewing Alert Types	431
Creating New Alerts	434
Editing, Cloning, and Deleting Alerts	438
Viewing Alert Status	440
Filtering Alerts	441
Acknowledging Alerts	442
Updating Alert Status	443
Creating Dispatch Specifications	443
Editing, Duplicating, and Deleting Dispatch Specifications	447
Creating Suppression Specifications	447
Editing, Duplicating, and Deleting Suppression Specifications	449
A Protocol Compliance	451
Index	453

1 Introduction

This chapter introduces the Route Analytics Management System route analytics tool.

Chapter contents:

- [About Route Analytics Management System](#) on page 18
- [How Route Analytics Management System Operate](#) on page 19
- [Key Components of Route Analytics Management System](#) on page 19
- [Using Route Analytics Management System](#) on page 23

About Route Analytics Management System

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

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

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

The following features are included in this release:

- Support for VPN Traffic
- Capacity Planning
- Network Element Groups
- User authentication

How Route Analytics Management System Operate

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

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

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

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

Key Components of Route Analytics Management System

RAMS includes the following components:

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

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



The Flow Collector is supported only on appliance models with two disk volumes (DL380 G5 FC). See the *HP Route Analytics Management System Administrator Guide* for more information.

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

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

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

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

When there are multiple Route Recorders in a distributed RAMS deployment, you can configure each appliance to record data per protocol or per multiple protocols, per area or per area within a protocol, or in any combination thereof. For a description of recorder configuration, see the “Configuration and Management” chapter in the *HP Route Analytics Management System Administrator Guide*.

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

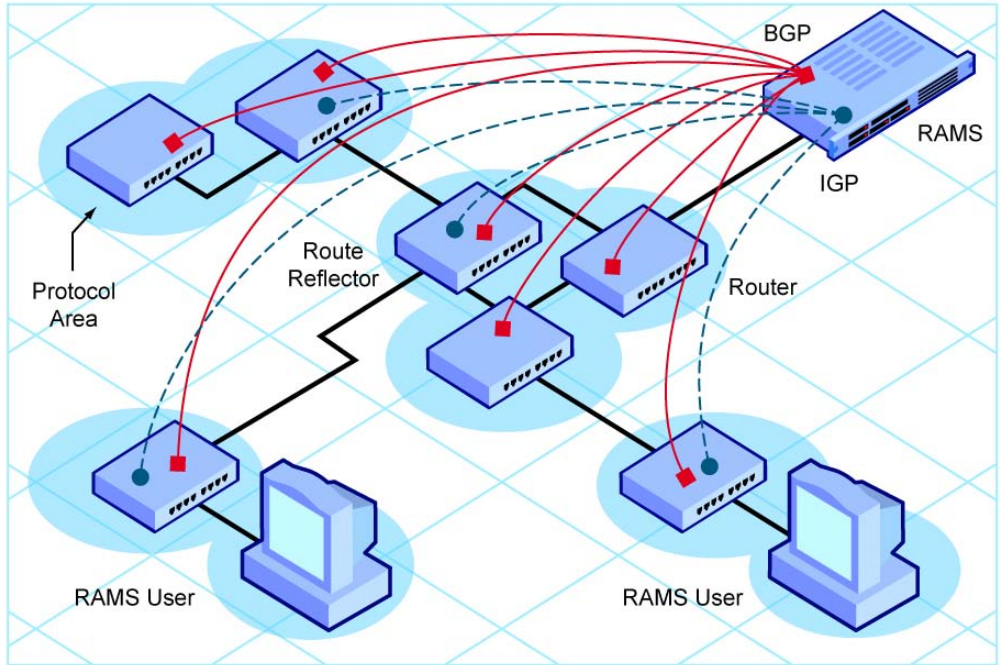


Figure 1 RAMS Data Flow

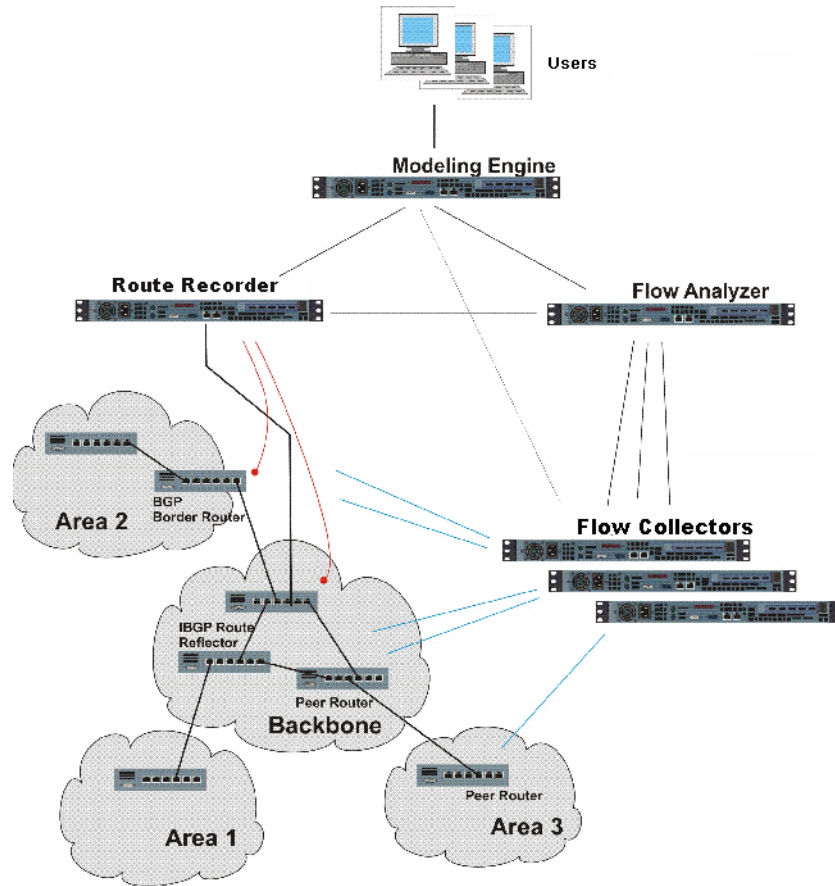


Figure 2 RAMS Traffic Data Flow

In a distributed environment where multiple appliances are installed on the network, one unit in the deployment will have a Master Capability license key. During the configuration process, you designate this unit as the master. The other appliances in the deployment act as clients of the master. For example, the Modeling Engine can be designated the master, while the Route Recorder is designated as a client. (For RAMS, the Route Recorder, Flow Collectors, and Flow Analyzer are client units.) From the master, you view and configure clients for recording. You also manage licenses for the entire configuration from the master.

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

Using Route Analytics Management System

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

- A web browser for accessing the *Administration* web pages. Use the web interface to perform tasks such as database management, report creation, software updates, and recorder configuration.
- A VNC or X Window System client for displaying the Route Analytics Management System application. Network engineers and operators use the VNC or X client interface to view the routing topology map and analyze network activity.

Both types of viewers accommodate remote access, so you can view and manage one or more units from any desktop computer connected to the network, providing that it has a web browser and a VNC or X Window System client installed. Refer to [Chapter 2, “Viewers”](#) for instructions on setting up client access.

The Web Interface

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

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

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

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

The Application Interface

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

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

See [Opening a Routing Topology Map](#) on page 40 for instructions on opening the maps. Monitoring mode is available only with databases that are configured for recording data.

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

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

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

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

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

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

2 Viewers

This chapter describes how to download and install the viewers that are available to access the Route Analytics Management System client application.

Chapter contents:

- [Understanding Viewer Options](#) on page 28
- [Installing an X Window Server](#) on page 28
- [Installing VNC Viewer](#) on page 32
- [Opening the Client Application](#) on page 36

Understanding Viewer Options

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

- The X Window System lets you run an application on a remote computer located anywhere with access to the Internet, and display the application windows on your local computer. Accessing the system 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 the system 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.

Installing an X Window Server

To use the X Window System, your computer must run an X server to receive and display the output of the remote application. For privacy and security, SSH (secure shell) must be used to connect the session.

Using X Window System Software for MS Windows

Several X Window System products with SSH are available for Microsoft Windows:

- Xming
- Xwin-32
- Xmanager

The third-party X software included with the appliance 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 StarNet Communications Corporation.



The X-Win 32 evaluation from StarNet supports anti-aliased fonts, which allow the BGP Root Cause Analysis and RIB visualizations to display correctly.

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

- 1 Using a web browser, go to <http://www.straightrunning.com/XmingNotes>
- 2 Choose **Xming** under the public domain releases option
- 3 Follow the installation steps, selecting **Full Installation**. For efficient operation, choose the options shown in the following figure.

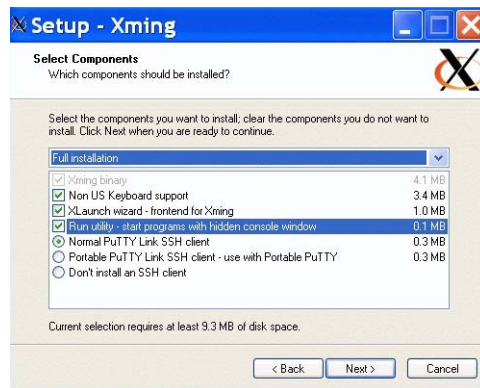


Figure 3 Xming Options

- 4 Include Normal PuTTY Link SSH client in the installation along with the other default selections
- 5 When installation is complete, run **XLaunch**.

For Display settings you can choose multiple windows, one window, full screen, or one window without title bar. The Multiple Window option best fits for most purposes. You can have multiple views of each subset of topology if available under a hierarchical model.

- 6 Choose a display option and click **Next**.
- 7 Choose **Start a program** and click **Next**.

- 8 Choose **Using PuTTY** in the **Run Remote** area. Type the IP address in the Connect to computer field, the user name (admin or op) in the Login as user field, and the password (admin or op) in the Password field. Click **Next**.
- 9 You do not need to enter the parameter settings. Click **Next**.
- 10 To save the configuration for fast subsequent access, click **Save Configuration**. Choose a name for the configuration and click **Save** to save to your desktop or elsewhere.
- 11 Click **Finish**. You will be connected to the appliance.

To download and install X-Win32 for Windows, perform the following steps:

- 1 Using a web browser, connect to the Home page.
- 2 Click **Support** on the top navigation bar.
The Support page appears.
- 3 Click **Link to StarNet Communications Corp. for X-Win32 Evaluation**.
StarNet's Download X-Win32 Evaluation page opens.
- 4 Fill out the form shown on-screen, and click **Send Email**.
After sending the form, in return you will receive a 30-day license key and download instructions for X-Win32.

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

- 1 Using a web browser, connect to the Home page.
- 2 Click **Support** on the top navigation bar
The Support page appears.
- 3 Click **Xmanager 30-Day Evaluation** to download an evaluation copy of X-Win32.
The File download window opens.
- 4 Select **Save this file to disk**, and then click **OK** to save the X-Win32 executable file to the specified local directory.
- 5 Open the downloaded .exe file. The Welcome screen appears.
- 6 Follow the on-screen instructions to install X-Win32.

To start X-Win32, perform the following steps:

- 1 Double-click the X-Win32 icon on the desktop.
- 2 Open the window from the X-Win32 folder.
- 3 Type the connection details in the window that appears:
 - Name: Type a name for the session.
 - Host: Type either the hostname or IP address of the appliance.
 - Protocol: Select SSH; to ensure privacy and security, only SSH connections are accepted.
 - User name and Password: Type your appliance user ID and password.



The first time the SSH connection is initiated, you may see a security warning. Click **Yes** to save the host key and continue.

- 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.

If you would like to view a demo of the Xmanager setup, select the **Xmanager Setup** (ShockWave Demo) link and follow the screens.

Using X Window Server for UNIX Platforms

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



SSH is required to run the system 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 XDE or Gnome is running on the desktop.
- 2 From the shell in a terminal window, open an SSH connection to the appliance. Type the following command:

```
ssh X userid@rex
```

For example:

```
ssh X op@10.0.0.24
```

- 3 Type your appliance user password when prompted.

The 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 the appliance 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 Type your appliance user password when prompted.

The application opens on the desktop.



The system is expected to work with the X Window System on other platforms, but they may not be tested or fully supported.

Installing VNC Viewer

To use VNC, you must install a VNC viewer (client) on your computer. The VNC viewer then connects to the VNC server running on the appliance. Before starting the VNC viewer on the desktop, configure and start the VNC server as described in the Administration chapter of *HP Route Analytics Management System Administrator Guide*.

Downloading VNC

The Support page offers the following versions of the VNC viewer:

- Windows 9x, NT, 2000, XP

- Linux (x86)
- Macintosh (OS9)
- Macintosh (OS X)
- Solaris (sparc)

Downloading and Installing VNC on Windows

To download and install VNC, perform the following steps:

- 1 On the Home page, click **Support** on the top navigation bar.
- 2 On the Support page, click the link for the appropriate version of the VNC viewer.
The File download window opens.
- 3 Select **Save this file to disk**, and then click **OK**.
This saves the VNC viewer to a local directory.
- 4 The downloaded VNC file is compressed. Before installing it, decompress it with an application such as WinZip.
- 5 Run the VNC viewer.exe file to install VNC.

To start VNC, perform the following steps:

- 1 Double-click the VNC icon to open the Connection Details dialog box.
- 2 If this is a first-time installation, click **Options**, adjust options as needed, and then click **OK**:
 - Choose **Tight Encoding** to improve performance.
 - Choose **Full-screen mode** to eliminate scroll bars on the VNC viewer and window frame. This prevents the taskbar and minimized icons on the desktop from being scrolled off-screen.



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.

- 3 Type the appliance IP Address or hostname in the VNC Server text box followed by **:1**.

Example: **192.168.1.5:1**

- 4 Click **OK** to start the VNC viewer.



If a “Failed to connect to server” warning appears, either the VNC server is not running or the system is in single operator mode and another operator is already accessing it. Contact the appliance administrator to resolve the problem.

- 5 Type the VNC authentication password as set in Configuring the VNC Server (refer to the Administration chapter of *HP Route Analytics Management System Administrator Guide*).
- 6 Click **OK**.
This starts the VNC viewer.
- 7 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**, 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 Type 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, type the following command:

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

To start VNC, perform the following steps:

- 1 Type the following command at the command line, where a.b.c.d is the appliance IP address or hostname:

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

or

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



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 administrator to start the VNC Server from the Administration page.

- 2 At the password prompt, type the VNC authentication password as set in Configuring the VNC Server (refer to the Administration chapter of *HP Route Analytics Management System Administrator Guide*).

This starts the VNC viewer.



If the system 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 appliance administrator to resolve the problem. If shared access to the VNC desktop is appropriate, ask the appliance 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**.

Installing SVG Plug-In

Adobe offers a free SVG plug-in which can be downloaded from the following url: <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.

Select **Install SVG Plug-In** and follow the steps provided onscreen to install the plug-in.

View System Information

Selecting this link will display the currently configured settings for your appliance.



To view System Information, you must log-in as the Administrator.

Opening the Client Application

Use the procedures in this section to open the client application in MS Windows using X Window server software or VNC server. For instructions on starting the application in Linux or Solaris, see [Using X Window Server for UNIX Platforms](#) on page 31.

X Windows

Follow these steps only if you have already downloaded, installed, and initially run one of the X Windows options. For instructions on setting up those options, see [Using X Window System Software for MS Windows](#) on page 28.

To open the client application using Xming, perform the following steps:

- 1 Click the shortcut for your saved XLaunch configuration.
- 2 Enter your password, as prompt, and click **Finish**.
- 3 The client application opens.

To open the client application using Xwin-32, perform the following steps:

- 1 Click the Xwin-32 shortcut that you saved.

- 2 Enter your password, as prompt, and click **Finish**.
- 3 The client application opens.

To open the client application using X Manager, perform the following steps:

- 1 Click the X Manager shortcut that you saved.
- 2 Enter your password, as prompt, and click **Finish**.
- 3 The client application opens.

VNC

VNC viewer behavior depends upon on the VNC display that is specified.

For VNC display 1, the application is started when the VNC server is started on the web page. When the first connection is made to the VNC server, the application is already running. If the connection is ended, the session persists. When a new connection is made, the application will be in the state in which it was left at the end of the first session.

If the application is closed using the Quit menu command or by closing the main window, then the next time VNC is opened the desktop appears without the main window. In this case, perform the following steps:

- 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 the product name. The main window opens.

When you start the VNC server, the application is automatically started on the VNC desktop and opens as soon as the VNC viewer connects to the server.

When the VNC viewer makes a connection to one of the VNC displays 2-10, a new instance of the VNC server is started and the application is automatically started on the VNC desktop. If the application is closed using the Quit menu command or by closing the main window, then the session ends. If a new session is connected, a new instance of the application is started.



The size of the VNC window depends upon how the individual VNC display (1-10) has been configured. See the “Administration” chapter in the *HP Route Analytics Management System Administrator Guide*.

3 The Routing Topology Map

This chapter describes how to use the routing topology map to monitor your network.

Chapter contents:

- [Working with Routing Topology Maps](#) on page 39
- [Applying Configuration Options](#) on page 67
- [Working with Router Information and Layout](#) on page 76
- [Understanding Topology Groups](#) on page 97
- [Understanding Network Routes](#) on page 114

Working with Routing Topology Maps

The *Routing Topology Map* window provides an overall view of the network as it is currently running, including any tactical changes made during outage repairs that might not be reflected in network design documents.

Each stored database has a routing topology that you open to view router status and links, spot outages, identify routing failures, and uncover potential configuration errors that may result in service outages following maintenance activities. The routing topology map lets you view the routing events that led to failure and perform forensic analysis. Its accurate, vendor-independent view of the routing network can help you identify implementation or interoperability issues that are not easily isolated using other tools.

[Chapter 2, “Viewers”](#) explains how to start the application in the X Window System or in a VNC viewer. The next step is to select and open a routing topology.

Opening a Routing Topology Map

When a topology initially loads, the appliance uses a randomizing process to place the nodes on the routing topology map. The placement is not geographical. After you save the layout the first time, the database loads more quickly when it is reopened.

To open a routing topology map, perform the following steps:

- 1 Open the client application.



Chapter 2, “Viewers,” describes the options available for running the client application.

- 2 In the main window, select **Topology** → **Open Topology** to display the topology list.

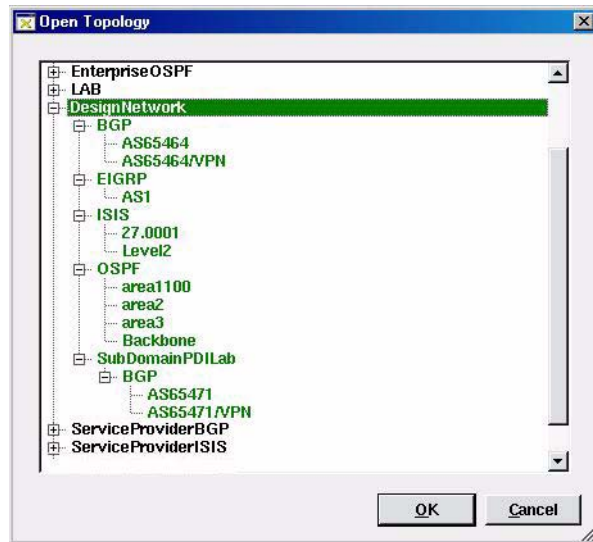


Figure 4 Opening a Topology

Database names shown in green are configured for recording data, and database names shown in black are inactive.

- 3 Select the necessary databases from the list. Selected items are highlighted.

Identify a range by pressing **Shift** as you select names. Choose or remove names by pressing **Ctrl** while clicking on names. Selecting a group name selects all items within the group.



In RAMS, if you plan to perform BGP-specific analysis operations, such as the Root Cause Analysis, deselect any traffic databases in the Open Topology list. Traffic data is not relevant for BGP-specific analysis, and loading traffic information from the database can slow analysis.

4 Click **OK**.

After the database loads, the topology map opens in the main window. The amount of time it takes to render the topology map is based on database size.



In RAMS, any topology that contains traffic data automatically opens in Analysis Mode. This is due to inherent delays in NetFlow aggregation and buffering. If you are interested only in routing data, open the topology in Monitoring Mode by deselecting any topologies that contain traffic in the *Open Topology* dialog box.

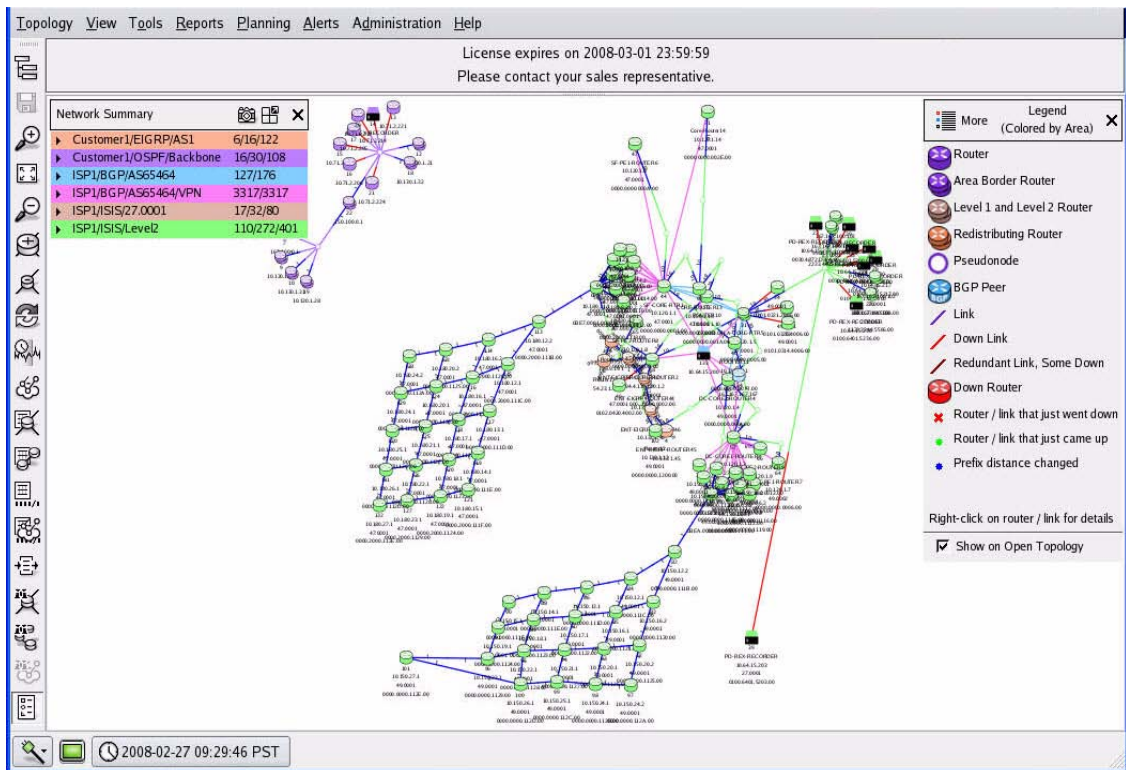


Figure 5 Routing Topology Map Main Window

Symbols and Colors

The routing topology map consists of node symbols connected by links. The symbol used for each node depends on its function. Refer to [Legend Panel](#) on page 43 for the default shape and color associations. The shapes and colors are customizable.

The nodes and links in each routing area of the network are shown in different colors. You can change or turn off element coloring on the map by selecting **View** → **Color Modes** and then choosing one of the following items:

- Color by Area
- Color by Traffic Bitrate (RAMS Traffic only)
- Color by Traffic Utilization (RAMS Traffic only)

- Uncolor
- Color by Metric

When coloring is turned off (uncolor), nodes are black and links are grey. For additional information, refer to [Colors](#) on page 70.

Links and Peerings

Each on the topology map is divided in half to represent the two directions of communication between a pair of nodes. The half adjacent to a node represents the outbound direction from that node. Each half can function separately up or down.

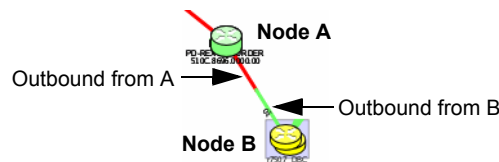


Figure 6 Link Colors

IGP links and BGP peerings are shown as colored lines connecting nodes. By contrast with IGP, peerings between BGP protocol routers and their clients are implied and may not follow physical paths. The system discovers and monitors BGP connections indirectly by receiving routes from BGP protocol routers for which the next hop attribute contains the address of another BGP router.



Because BGP peerings can be too dense on the map to be useful, the default setting is for the peerings not to be displayed. See [Auto-Hide](#) on page 74 for more information.

Legend Panel

The Legend is displayed in the upper-right corner of the routing topology map ([Figure 7](#)). You can move the Legend by placing the cursor in the top area and holding it down while you move. Selecting a symbol in the Legend highlights the symbols on the topology map.





Figure 7 Topology Map Legend

The content in the Legend is dynamic. You can change the colors as described in [Colors](#) on page 70.

Use the options shown in [Table 1](#) to control display of the Legend area.

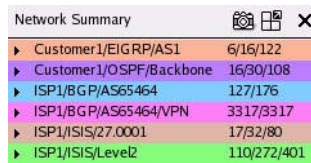
Table 1 Legend Appearance Options

	More/Less button	Toggles between less and more detailed symbol descriptions.
	Close button	Closes the Legend. The next time you open a topology, the Legend will reappear unless you deselect the Show on Open Topology checkbox. You can open the Legend panel at any time from the <i>Help</i> menu or by clicking the Legend button as described in Main Window Toolbar on page 49.
Show on Open Topology checkbox		Determines whether the Legend appears upon opening a topology. The checkbox is enabled by default.

Network Summary Panel

The *Network Summary* panel (Figure 8) allows you to view current network counts and analyze the effects of network changes. By default, the panel is displayed when you open a topology map.

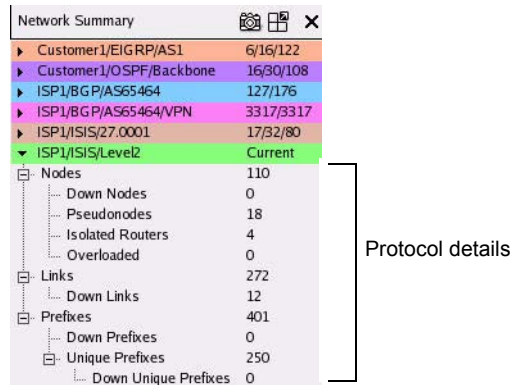
- If you do not want to display the panel when you open a topology map, choose **Administration** → **Options** → **Miscellaneous**, deselect the **Show Network Summary on Open Topology** check box, and click **Close**.
- If you close the Network Summary panel, reopen it by choosing **View** → **Show Network Summary**.



Network Summary	
▶ Customer1/EIGRP/AS1	6/16/122
▶ Customer1/OSPF/Backbone	16/30/108
▶ ISP1/BGP/AS65464	127/176
▶ ISP1/BGP/AS65464/VPN	3317/3317
▶ ISP1/ISIS/27.0001	17/32/80
▶ ISP1/ISIS/Level2	110/272/401

Figure 8 Network Summary Panel

You can expand the detail information for a specific protocol by clicking on the protocol, as shown in Figure 9.



Network Summary	
▶ Customer1/EIGRP/AS1	6/16/122
▶ Customer1/OSPF/Backbone	16/30/108
▶ ISP1/BGP/AS65464	127/176
▶ ISP1/BGP/AS65464/VPN	3317/3317
▶ ISP1/ISIS/27.0001	17/32/80
▼ ISP1/ISIS/Level2	Current
Nodes	110
Down Nodes	0
Pseudonodes	18
Isolated Routers	4
Overloaded	0
Links	272
Down Links	12
Prefixes	401
Down Prefixes	0
Unique Prefixes	250
Down Unique Prefixes	0

Protocol details

Figure 9 Network Summary Panel Expanded Row

The Network Summary panel provides the information listed in Table 2 , depending on the protocol.

Table 2 Network Summary Panel Information




Item	Description	Protocols
Total nodes	Total number of network nodes	IGP, EIGRP, IS-IS, OSPF
Down nodes	Number of nodes that are not operational	IGP, EIGRP, IS-IS, OSPF
Isolated nodes	Number of nodes with no links to other nodes	IGP, EIGRP, IS-IS, OSPF
Total links	Total number of network links	IGP, EIGRP, IS-IS, OSPF
Down links	Number of links that are not operational.	IGP, EIGRP, IS-IS, OSPF
Total prefixes	Total number of network prefixes	IGP, EIGRP, IS-IS, OSPF
Down prefixes	Number of prefixes that are not operational	IGP, EIGRP, IS-IS, OSPF
Unique prefixes	Number of distinct prefixes	IGP, EIGRP, IS-IS, OSPF
Down unique prefixes	Number of distinct prefixes for which all instances are not operational	IGP, EIGRP, IS-IS, OSPF
Active prefixes	Number of prefixes that have at least one operational route	BGP, VPN
Active routes	Number of routes that are operational	BGP, VPN
Baseline up routes	Number of operational routes in the baseline	BGP, VPN
Baseline down routes	Number of non-operational routes in the baseline	BGP, VPN
Next hops	Number of unique BGP next hops for all routes	BGP, VPN
MP Next hops	Number of unique BGP multi-protocol next hops for all routes	BGP, VPN

Table 2 Network Summary Panel Information

Item	Description	Protocols
Neighbor ASs	Number of unique neighbor ASs	BGP, VPN
Pseudo nodes	Number of nodes that are pseudonodes	BGP, IS-IS, OSPF
Overloaded nodes	Number of nodes indicated as overloaded	BGP, IS-IS
Total OSI prefixes	Number of nodes with OSI prefixes	BGP, IS-IS
Down OSI prefixes	Number of OSI prefixes that are not operational	BGP, IS-IS

Table 3 shows the buttons that appear in the *Network Summary* panel.

Table 3 Network Summary Buttons

	Snapshot Statistics	Saves the current Network Summary counts and displays the statistics in a new column.
	Tear Off	Releases the Network Summary panel from the main window so that you can move it around your desktop.
	Put Back	Reattaches the Network Summary panel to its original location in the main window.

Main Window Status Bar

The status bar at the bottom of the main topology map window indicates the current mode, recorder status, and the date and time that you are viewing on the map. When applicable, a status message is shown to the right of the date and time.

To change the date and time, click the field. An **OK** and **Cancel** button are displayed. Make changes and Click **OK**.

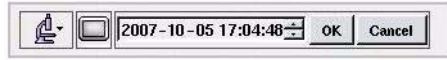


Figure 10 Main Window Status Bar

In Analysis mode, you can click the date/time area to display the playback controls. Choose a date and time and a step size in sections for the playback, and click **OK**. Then click the right-facing arrow to begin the playback.






Figure 11 Main Window Status Bar



In RAMS Traffic, the time in the status bar is based on the time of the traffic data. For current data, there is typically a delay, the length of which depends on network complexity.

Change modes by clicking the icon for the current mode and selecting the desired mode. Table 4 shows the icons.

Table 4 Mode Icons

	Monitoring mode	The topology is currently being recorded and updates to the routing database are shown on the topology map as they occur.
	Analysis mode	Only previously recorded information in the routing database is shown on the topology map.
	Planning mode	Planning features are enabled for the topology map. This mode activates another set of buttons in the main window.


An indicator to the right of the mode button  provides status based on color. Click the status indicator to obtain additional information on the recorder and peers (Table 5).

Table 5 Color Status

Green	<p>Either of the following applies:</p> <ul style="list-style-type: none"> •The system is running and recording to the database, and adjacencies between the system and peer routers in all areas are up. •Discovery is completed.
Blue	<p>Either of the following applies:</p> <ul style="list-style-type: none"> •Data is being recorded, but EIGRP topology exploration is in progress, so changes in the topology will not be shown until completion. The time on the recorder is not synchronized with the time in the appliance. •Discovery is in process.
Yellow	Data is being recorded, but adjacencies to peer routers in some areas are down.
Red	No data is being recorded, either because the system is not running or all adjacencies with peer routers are down.
Gray	This is a historical database to which no new data is being recorded.
Purple	There is a replication-related error.

Main Window Toolbar

The toolbar on the left side of the main routing topology map window containing buttons that control the map display and provide shortcuts to menu options. 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.

Table 6 shows the buttons on the toolbar.

Table 6 Main Window Toolbar Buttons


	Show / Hide Topology Hierarchy	Insert a pane showing a tree view of the routing databases on the map. See Working with Router Information and Layout on page 76 for more information.
---	---------------------------------------	--

Table 6 Main Window Toolbar Buttons (cont'd)


















	Save Layout	Save the current map layout (disabled if no changes). If this is the first time you have saved the layout, the system prompts you to name the layout and specify it as your default layout.
	Zoom In / Zoom Out	Increase or decrease the size of images and text shown in the topology map. When zooming, you can use the scroll wheel on your mouse to scroll up and down within the zoomed topology map.
	Reset View to 1:1	Restore the topology map to the default viewing scale.
	Node Size Up / Node Size Down	Increase or decrease node size and labels.
	Relayout	Generate a new randomized layout of the nodes.
	History Navigator	Open the <i>History Navigator</i> window for the current topology.
	Routing Reports	Open the <i>Routing Reports</i> window. For additional information, see Chapter 9, “Traffic Reports” (RAMS Traffic only)
	List Routers	Open the List of All Routers report to generate a list of all routers in the current topology map. See Router List on page 91 for more information.
	List Links	Open the List of All Links report to generate a list of all links in the current topology map. See Links List on page 92 for more information.
	List Prefixes	Open the List of All Prefixes report to generate a list of all prefixes in the current topology map. See Prefix List on page 94 for more information.
	List VPN Prefixes	Opens the List VPN Prefixes report. See Finding a VPN Route By Prefix on page 117 for more information.
	RIB Browser	Open the <i>Routing Information Base (RIB) browser</i> . See RIB Browser on page 158 for more information.
	Find Router	Open the Find Router or LAN Node search to search for routers by IP address or router name. See Router List on page 91 for more information.

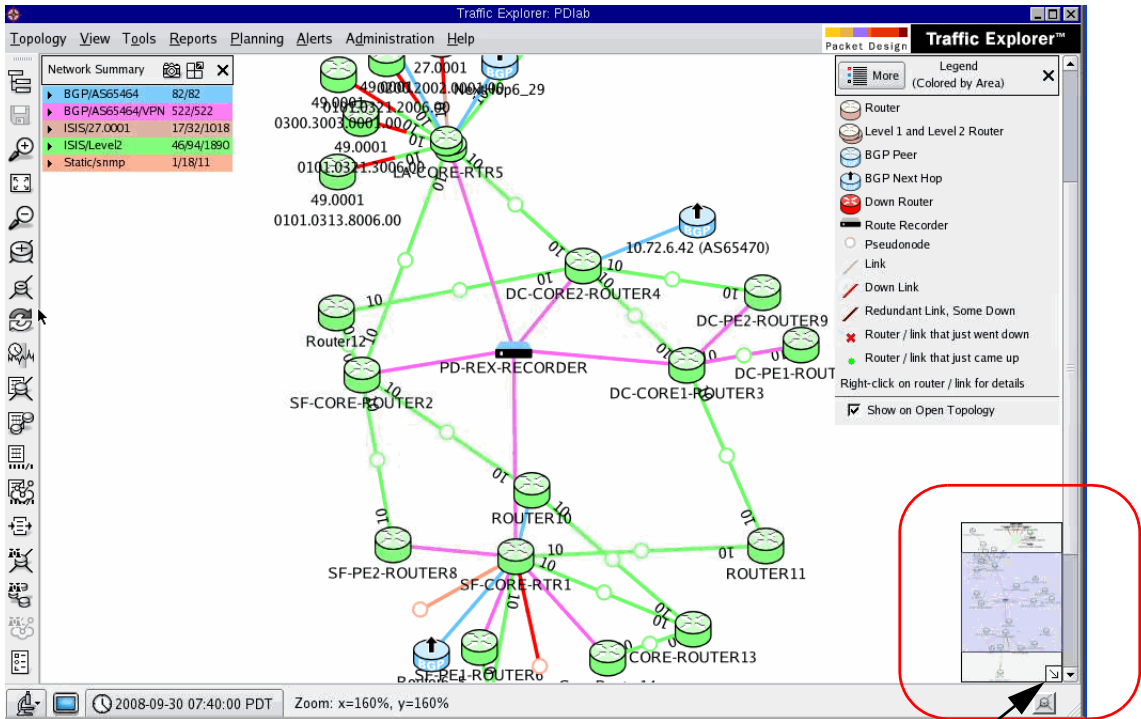
Table 6 Main Window Toolbar Buttons (cont'd)

	List/Find Paths	Open the <i>List or Find Paths</i> window to highlight a path between a router and an Internet prefix or domain name. See Finding a Route By Prefix on page 116 for more information.
	List/Find VPN Paths	Open a window to find VPN paths in the topology.
	Show Legend	Open or close the legend. See Legend Panel on page 43 for more information.



Duplicate functionality is available with some buttons and their associated menu items. The descriptions in this chapter uses the button options, when available.

When you zoom in on the topology map, an overview area opens in the lower right corner of the window to show the zoom area within the context of the full map (see [Figure 12](#)). If you notice that interaction with the map becomes slower when this area is open, click the arrow in the lower right corner to hide the area. Click the modified icon  to reopen the area.



Click to hide overview area











Figure 12 Routing Topology Map Overview Area Shown and Hidden

In Planning mode, a second toolbar is displayed on the right side of the routing topology map window Table 7 shows the buttons on the second toolbar.

Table 7 Main Window Second Toolbar Buttons - Planning Mode Only

	Add Router	Place a new node on the topology map.
	Add IGP Peering	Create IGP peering between two nodes
	Add BGP Peering	Create BGP peering between two nodes

Table 7 Main Window Second Toolbar Buttons - Planning Mode Only (cont'd)

	Add Prefix	Apply prefixes to a router on the topology map. For BGP routers, you can add prefixes manually or by selecting a filtering method for the prefix.
	Add Traffic Flow	Create a new traffic flow. (RAMS Traffic only)
	Edit BGP Prefix	Remove or change the attributes of a prefix on a particular node on the topology map. You can also change multiple prefixes at once by selecting more than one prefix from the table.
	Edit Traffic Flows	Modify a traffic flow. (RAMS Traffic only)
	Edit Router	Change the overload bit for an IS-IS node.
	Down Router	Change the state of a node from up to down to simulate what would happen if the selected router fails.
	Down Peering	Change the state of a peer relationship from up to down to simulate what would happen if the selected peering fails. This action brings down all the peerings in the table or only selected relationships.
	Down Prefix	Change the state of one or more prefixes from up to down on a particular router to simulate what would happen if the selected prefixes fails.
	List/Find VPN Paths	Open a window to find VPN paths in the topology.
	Analyze Edits	Update all traffic and routing edits simultaneously.

Main Window Menus

Use the main menu bar to open routing topology maps and monitor and analyze routing data. This section provides describes the options available with each menu.



Some menu items are for specific protocol families and are shown only if your appliance is licensed for that protocol.

Topology

Table 8 describes the items on the Topology menu.

Table 8 Topology Menu Items

Item	Description
Open Topology	Open a routing topology database, showing the topology map.
Close Topology	Close a routing topology database so that another can be opened.
Analysis Mode Planning Mode Monitoring Mode	List available modes with the exception of the mode you are currently in. Note: When you open only a static database, Planning mode is not available.
Go To Time	View the topology map as it appeared at a particular time in history (Analysis mode only)
Go To Latest Time	Activate the OK and Cancel buttons for the time field at the bottom of the window. This allows you to change the current time.
Load Layout	Load a saved layout to reposition the nodes. If needed, you can save the same layout multiple times under different names.
Reload Layout	Restore the node positions according to the previously loaded layout (disabled if no layout is loaded or no nodes have been moved).
Relayout	Create a new randomized placement of the nodes on the topology map. This can help you find a preferred orientation to name and save.
Delete Layout	Delete a named layout.
Save Layout	Save the current map layout (disabled if no changes). If this is the first time you have saved the layout, the system prompts you to name the layout and allows you to set it as the default.

Table 8 Topology Menu Items (cont'd)

Item	Description
Save Layout As	Open the <i>Save Layout</i> dialog box to save the current layout under a new name. You can also set the new layout as the default.
Select Layout Background	Open the <i>Select Layout Background</i> dialog box. Imported image files are shown in a list of available files.
Quit	Close the client application. The system application continues to run.

View

Table 9 describes the items on the View menu.

Table 9 View Menu Items

Item	Description
Show/Hide Topology Hierarchy	Show or hide a tree view of the routing databases on the left side of the routing topology map window. See Understanding the Topology Hierarchy on page 64 for more information.
Show/Hide Network Summary	Show or hide current counts of network elements. See Network Summary Panel on page 45 for more information.
Show/Hide Toolbar	Show or hide the toolbar on the left edge of the main window.
Color Modes	Modify color characteristics on the routing topology map. The color modes specifying bitrate and utilization are disabled in Monitoring mode. See Symbols and Colors on page 42 for more information.
Node Label Modes	Access the node label options. See Node Labels on page 70 for more information.
Hide Nodes	Specify that nodes matching a pattern will be hidden from view on the routing topology map (see Hiding Nodes on page 82).
Hide Leaf Nodes	Remove nodes that are on the edges of the map and have only a single link. Each time you select Hide Leaf Nodes, additional nodes are removed. See Hiding Nodes on page 82 for additional information.

Table 9 View Menu Items (cont'd)

Item	Description
Show / Hide Failed Nodes	Show or hide failed nodes.
Show / Hide Unconnected Nodes	Show or hide unconnected nodes.
Unhide All Nodes	Show any hidden (trimmed) nodes.
Highlight / Unhighlight All Paths	Turn path highlights on or off.
Zoom In	Increase image and text size.
Rest View to 1:1	Restore the topology map to the default viewing scale.
Zoom Out	Reduce image and text size.
Node Size Up	Increase node and label size. Node placement is saved when you save a layout.
Node Size Down	Decrease node and label size. Node placement is saved when you save a layout.
Node Size Reset	Reset nodes and accompanying text to the default size. This function does not affect zoom level.

Tools

Table 10 describes the items on the Tools menu.

Table 10 Tools Menu Items

Item	Description
Find Router	Search for routers by IP address or router name. See Router List on page 91 for more information.
List/Find Paths	Highlight a path between a router and an Internet prefix or domain name. See Finding a Route By Prefix on page 116 for more information.
List/Find VPN Paths	Find VPN paths in the topology. See Finding a VPN Route By Prefix on page 117 for more information.
Highlight by Exit Router	<p>Find the set of exit routers toward a specified prefix, NSAP Address, IP address or domain name, and color code 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. See Viewing Exit Routers on page 84 for more information.</p> <p>To highlight exit routers, the listed network must include a route to the desired destination.</p>
List Routers	Generate a list of all routers in the current routing topology map. See Router List on page 91 for more information.
List Links	Generate a list of all links in the current routing topology map. See Links List on page 92 for more information.
List Interfaces	Generate a list of interfaces discovered by static protocol. See Interfaces List on page 94 for more information.
List Prefixes	Generate a list of all prefixes in the current topology map. See Prefix List on page 94 for more information.
List VPN Prefixes	Generate a list of all of prefixes that are part of a VPN. See VPN Prefixes List on page 96 for more information.
List Flows	Highlight a specified flow. (RAMS Traffic only)
Topology Diagnostics	Show diagnostic information (for EIGRP topologies only). See Diagnosing EIGRP Topology Errors on page 121 for more information.

Reports

Table 11 describes the items on the Reports menu.



Most report tables support column sorting. You can resort data by clicking any column heading in the report. Click again to change the sort order (descending/ascending).

Table 11 Reports Menu Items

Item	Description
Routing Reports	Open the <i>Routing Reports</i> window. (RAMS Traffic only)
Traffic Reports	Access traffic reports and import interface capacity data. See Chapter 9, “Traffic Reports,” for more information. (RAMS Traffic only)
Path Reports	View computation paths between pairs of routers and generate reports for analysis. See Chapter 10, “Path Reports,” for more information.
History Navigator	Open the <i>History Navigator</i> window to analyze past routing data. See Chapter 4, “The History Navigator,” for more information.
RIB Browser	Open the <i>Routing Information Base (RIB) browser</i> to view link and route information. See RIB Browser on page 158 for more information.
Flow Record Browser	Display aggregated flow information. See Flow Record Browser on page 175 for more information. (RAMS Traffic only)
Events Monitor	Display a detailed list of routing events.
Correlate Time Series	Display a graph of external time series data in correlation with the routing history.

Planning

Table 12 describes the items on the Planning menu. For additional information on *Planning* menu items, refer to [Chapter 10, “Path Reports”](#)

Table 12 Planning Menu Items

Item	Description
Add Router	Place a new node on the topology map.
Add Peering	Create a peering relationship between two nodes on the topology map.
Add Prefix	Apply prefixes to a router on the topology map. For BGP routers, you can add prefixes manually or by selecting a filtering method for the prefix.
Add VRF	Add Virtual Routing and Forwarding, which allows multiple instances of a routing table to co-exist within the same router at the same time.
Add Traffic Flow	Create on the routing topology map. (RAMS Traffic only)
Add VPN Customer	Add a full mesh, or hub and spoke VPN customer to the network, including VRF routes, and traffic flows. (RAMS Traffic only)
Edit BGP Prefix	Change or remove prefix attributes on one or more nodes.
Edit Traffic Flows	Make changes to IPv4 flows or VPN flows. (RAMS Traffic only)
Edit Router	Change the overload bit for an IS-IS node.
Edit VRF	Modify the Virtual Routing and Forwarding router tables.
Down Router	Change the state of a node from up to down, simulating what would happen if the selected router should fail.
Down Peering	Change the state of a peer relationship from up to down, simulating what would happen if the selected peering fails. This action brings down all the peerings in the table or only selected relationships.
Down Prefix	Change the state of one or more prefixes from up to down on a router, simulating what would happen if the selected prefixes fail.
Down VRF	Change the state of one or more customer sites from up to down on a router, simulating what would happen if the selected customer site fails.
Analyze Edits	Updates all traffic and routing edits simultaneously.

Table 12 Planning Menu Items (cont'd)

Item	Description
Reports	Open the Planning Reports window. See Working with Planning Reports on page 259.
Capacity Planning	Open the <i>Capacity Planning</i> window. (Analysis mode only) See Working with Capacity Planning Tools on page 279 for more information. (RAMS Traffic only)
Show Edits	Display recent edits to the topology map. See Show Edits on page 296 for more information (RAMS only).

Alerts

Table 13 describes the items on the Alerts menu. For additional information on *Alerts* menu items, refer to [Chapter 11, “Alerts”](#)

Table 13 Alerts Menu Items

Item	Description
View Alert Status	View the current state of all defined alerts
Configure Alerts	Set up alerts based on alarm and inform criteria.
Dispatch Specifications	Determine the notification method to distribute information about network and traffic status.
Suppression Specifications	Determine the minimum level of activity that is considered typical or recurring and does not require notification.

Administration

Table 14 describes the items on the Administration menu.

Table 14 Administration Menu Items

Item	Description
Router Name	Customize router names and map them to the routers IP address. See Assigning Router Names on page 88 for more information.
Configure Traffic Change	Configure settings for traffic reports. See Top Changes Report on page 369 for more information.
AS Name	Customize Autonomous system (AS) names. See You can highlight invisible links in yellow on the topology map by clicking Highlight. on page 128 for more information.
Saved Filters	View and modify custom filters. See Creating Custom Filters on page 85 for more information.
Router Location Names	View and add router location names for XML customer reports. See Generating XML Customer Reports on page 335 for more information.
VPN Customer Configuration	Import and configure customer configuration mappings. See Creating Customer and RT Associations on page 332 for more information.
Router Groups	Mange <i>router groups</i> . See Creating Groups Using the Menu on page 104 for more information.
Link Groups	Manage link groups. Link groups are used to generate a watchlist on an alert; for example, for adjacency state change. See Creating Groups Using the Menu on page 104” for more information.
Prefix Groups	Manage prefix groups. See Creating Groups Using the Menu on page 104 for more information.
Path Groups	Manage source-destination paths to watch and generate an alert if there is a change. See Creating Groups Using the Menu on page 104 for more information.
VPN Customer Groups	Manage VPN customer groups. See Creating Groups Using the Menu on page 104 for more information.

Table 14 Administration Menu Items (cont'd)

Item	Description
VPN RT Groups	Manage VPN RT groups. See Creating Groups Using the Menu on page 104 for more information.
VPN Prefix Groups	Manage VPN prefix groups. See Creating Groups Using the Menu on page 104 for more information.
Assign BGP ASs to Routers	Assign routers manually to a BGP AS, usually for a BGP confederation. See Assign and Verify BGP AS Assignments to Routers on page 131 for more information.
Set Interface Capacities	Allows you to set the interface capacity (data rate) and save the settings for use in future sessions.
Options	Set preferences. See “ Applying Configuration Options ” on page 67 for more information.

Help

Table 15 describes the items on the Help menu.

Table 15 Help Menu Items

Item	Description
User's Guide	Display the PDF version of the User's Guide in a new window.
Developer's Guide	Display the PDF version of the Developer's Guide in a new window.
Administrator's Guide	Display the PDF version of the Administrator's Guide in a new window.
Show / Hide Legend	Open or close the legend that defines each symbol on the routing topology map.
About ...	Display software version information.

Topology Map Layouts and Background Images

You can customize the appearance of the routing topology map in the following ways:

- Save a topology map under multiple names with different layouts. Changes, such as resizing or hiding/unhiding nodes in a layout, are preserved when you save the layout.
- Customize a layout by changing node placement, topology symbols, and colors. The changes you make are specific to your login name and are view-only for other users. If you load and modify a layout created by another user, your changes are saved under your login name and do not change the other user's layout.
- Apply background images to topology maps. For example, you can use a map that shows the geographic location of network routers and then arrange nodes based on physical or logical groupings, such as per building or per lab. You can import background images in BMP, JPG, PNG, SVG, or XPM format using the *Layout Backgrounds* window. See the “Configuration and Management” chapter in the *HP Route Analytics Management System Administrator Guide*. Image files are stored in a database and are accessible from any device on the network.

To apply a background image to the routing topology map, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Topology** → **Select Layout Background**.
A list of available image files is displayed ([Figure 13](#)).



Figure 13 Available Background Images

- 3 Choose an image and click **OK**.

The image is now displayed as the background for the routing topology map.

To remove a background image from the topology map, perform the following steps:

- 1 Select **Topology** → **Select Layout Background**.
- 2 Choose **<blank>** and click **OK**.

Understanding the Topology Hierarchy

The *topology hierarchy* shows the routing databases in a hierarchical tree view and allows you to work with a subset of the topologies in the *map*. This is useful for large networks that contain numerous IGP areas and BGP ASs.

Next to each branch is a status light. The color of each light indicates the state of the individual recorder. You can hover the cursor over each light for a status message related to the recorder state.

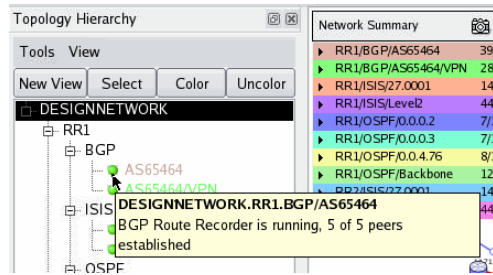


Figure 14 Status Message

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

The system also lets you view each individual area or AS in a separate window. Click **New View** to open a new topology map window that contains only the selected areas.

To display or hide the topology hierarchy, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **View** → **Show Topology Hierarchy**.

The hierarchy is displayed on the left side of the routing topology map.

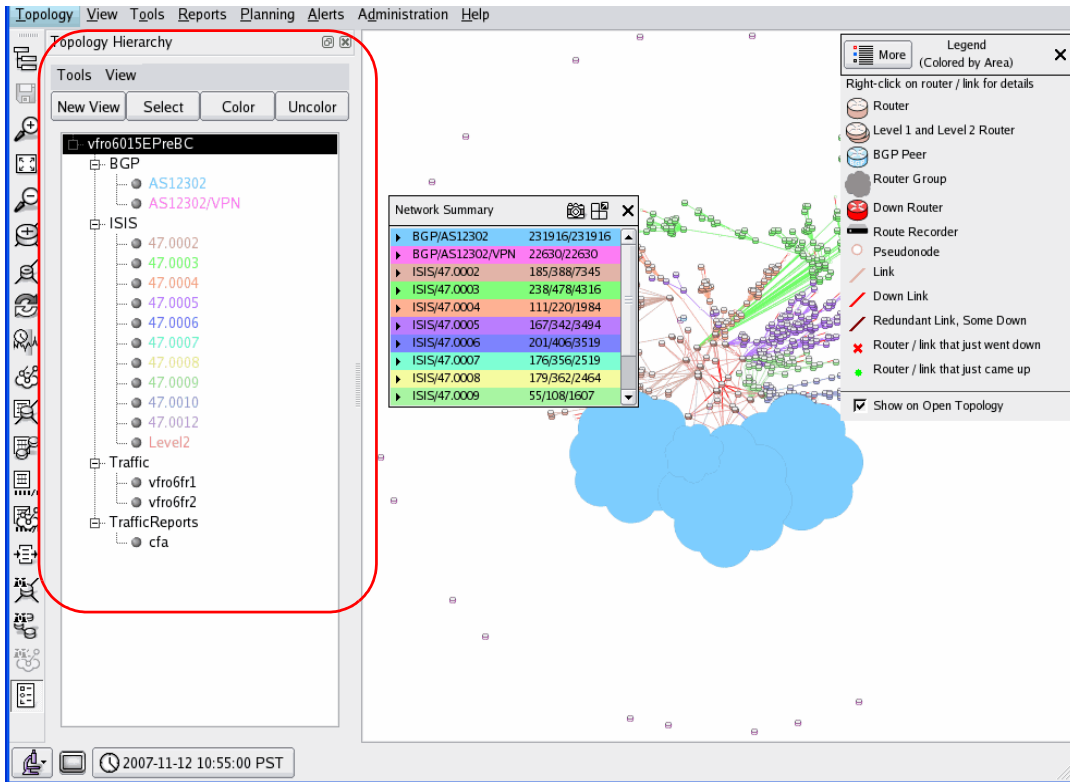


Figure 15 Topology Hierarchy

To view an individual area or AS, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Click **Show Topology Hierarchy**.
- 3 Select the desired areas in the tree structure.
- 4 Click **Select** in the topology hierarchy, and then click **Zoom In** or **Zoom Out** to expand the selected area of the topology map to fill the window. You can also click **New View** in the topology hierarchy pane to open a new window containing just the selected area.

Viewing Network Anomalies

You can use the routing topology map to see possible points of failure, failed links and routers, and other anomalies. For example, when a link goes down, that link turns red.

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

- 1 Open the client application and choose your database to open the routing topology map.
- 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 or LAN.

Applying Configuration Options

Configuration options are available to control the look and feel and behavior of the routing topology map.

To apply configuration options, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** → **Options** to open the configuration options window.

Configuration option categories

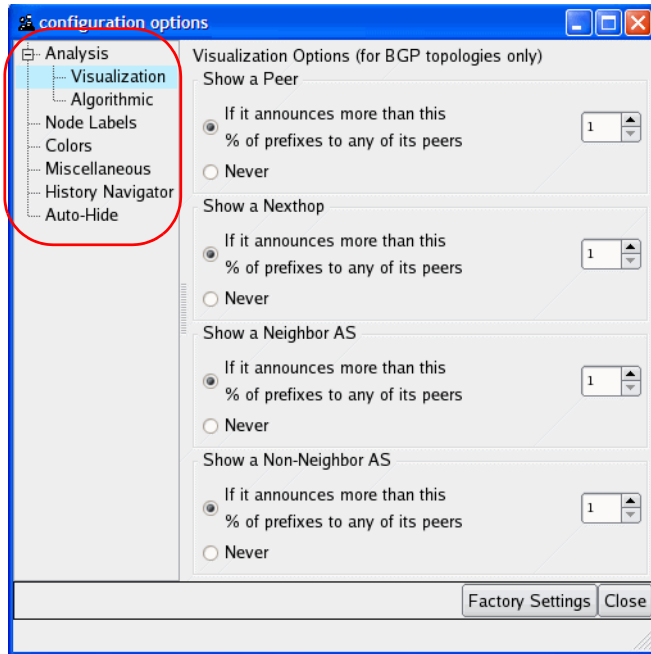


Figure 16 Configuration Options Window

- 3 Choose any of the categories from the left menu and make changes as described in the following sections:
 - [Analysis](#)—see [page 69](#)
 - [Node Labels](#)—see [page 70](#)
 - [Colors](#)—see [page 70](#)
 - [Miscellaneous](#)—see [page 71](#)
 - [History Navigator](#)—see [page 73](#)
 - [Auto-Hide](#)—see [page 74](#)
- 4 To save changes, click **Close**. To restore all options to their default values, click **Factory Settings**.

Analysis

The visualization and algorithmic analysis options control thresholds and level of detail displayed on the map.

Visualization Options

You can customize the level of detail that appears in visualizations and animations of the BGP Routing Information Base (RIB), as described in [RIB Visualization](#) on page 151. Visualization analysis controls whether a network entity appears in a *RIB visualization* window or a *root cause analysis animation* window. For each option, 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 that is too big or crowded to read. The following options are supported:

- **Show a Peer**—Include a peer if it announces 5 percent (default) or more of the total number of prefixes.
- **Show a Nexthop**—Include a nexthop if it announces 5 percent (default) or more of the total number of prefixes.
- **Show a Neighbor AS**—Includes the neighbor AS if it announces 5 percent (default) or more of the total number of prefixes.
- **Show a Non-Neighbor AS**—Includes the non-neighbor AS if it announces 5 percent (default) or more of the total number of prefixes.

Algorithmic Analysis Options

You can set the thresholds that are used in root cause analysis. In each case, a higher value decreases the level of detail and a lower value increases it. See [Root Cause Analysis](#) on page 143 for more information.

The following algorithmic analysis control thresholds are used in root cause analysis:

- Show if more than this percentage of prefixes on an edge is flapping. Default is 10 percent.
- Show if more than this percentage of total prefixes shifted from an edge. Default is 1 percent.

Node Labels

Node Labels determine the node details that are displayed on the routing topology map. The options depend on the protocol family. Each option is displayed only if it applies to currently licensed protocols. For example, router names and system IDs do not appear for an OSPF network.

The following node label options are supported:

- **Automatic**—Automatically chooses a label for the node. For example, if no router name is available for the node, the system uses the DNS Name node label. In automatic mode, node labels are prioritized by router names, DNS names, IP address, and system IDs. Automatic is enabled by default; selecting any of suboptions disables automatic mode.
- **DNS Names**—Includes the router DNS name. If no DNS name resolution is performed, selecting this option initiates DNS name resolution for all routers. In a large network, this can take time.
- **IP Address**—Includes the router IP address.
- **Router Names**—Includes the name of the router obtained from the protocol (if available).
- **System IDs (IS-IS only)**—Includes IS-IS System IDs when IS-IS is present on the routing topology map. If you choose **Show IS-IS NSAP Addresses** from the Miscellaneous options (as described in [Miscellaneous](#) on page 71), the label NSAP Address is used.
- **Area IDs**—Includes IS-IS Area IDs when IS-IS is present on the topology map.
- **Label Routers Only**—Does not label the pseudonodes that represent LANs.
- **ID Numbers**—Includes an internal ID number for the router that may be useful as a shorthand reference.

Colors

The following color options are available for the routing topology map:

- **Color Allocation Order**—Changes the default colors for routers and links when you click and drag color samples in the chart. For example, to make orange the first color for an element on the topology map, click the

orange color sample (by default, in position 5) and drag it to position 1 on the chart. The color formerly in position 1 replaces the color in position 5. Click **Set** to save changes or **Default** to return to the default settings.

- **Color links with metrics greater than**—Assigns colors to links that have metric values greater than the specified value. Use this option to find links with very high metrics.
- **Traffic Coloring Options**—Allows you to enter values to determine how bitrate and utilization are shown in color. (RAMS Traffic only)
- **Default Color Mode**—Allows you to manipulate the colors that are used in Analysis, Planning, and Monitoring modes. The following options appear in a drop-down list for each mode:



Monitoring mode can only use Color by Area and No Color.

- **Color by Area**—The nodes and links of each area appear in distinct colors, which are determined by the Color Allocation Order chart, when a topology is loaded.
- **Color by Traffic Bitrate**—Traffic flows are colored according to bitrate when a topology is loaded. Colors are determined by the Traffic Coloring Options chart. For example, flows with a high bitrate appear in red. (RAMS Traffic only)
- **Color by Traffic Utilization**—Traffic flows are colored according to utilization levels when a topology is loaded. Colors are determined by the Traffic Coloring Options chart. For example, flows with high utilization appear in red. (RAMS Traffic only)
- **No Color**—All areas and traffic flows appear with black nodes and gray links when a topology is loaded.

Miscellaneous

You can set the following miscellaneous preferences, which take effect when you close the Options window:

- **Font size**—Determines the font size for map labels.

- **Default layout on Open Topology**—Specifies the name of the saved layout that is used when loading a topology. This field is empty by default. You can type a name or automatically set one by saving a topology layout using *Save Layout* and enabling the **Use as default layout** checkbox.
- **Show legend on Open Topology**—Automatically shows the Legend panel when you load a topology. See [Legend Panel](#) on page 43 for information about the Legend panel.
- **Show network summary on Open Topology**—Automatically shows the *Network Summary* when you load a topology. See “[Network Summary Panel](#)” on page 45 for more information about this feature.
- **Show link metrics on the map**—Displays metrics for the links on the map.
- **Show BGP Peerings**—If selected, shows all of the BGP peerings. You must reload the topology to view the changes.
- **Show BGP Next Hops**—If selected, shows all of the BGP next hops. You must reload the topology to view the changes.



Because BGP peerings can be too dense on the map to be useful, the default setting is for the peerings not to be displayed. Changes to Show BGP Peerings and Show BGP Next Hops require a topology reload to take effect.

- Hide links in group on the map—Hides the links for the selected group.
- **Show ISIS NSAP Addresses**—Appears only when the loaded topology contains ISIS protocol routers. When this option is enabled, NSAP addresses appear on the topology map rather than the system ID for the IS-IS router. See “[Node Labels](#)” on page 70 for more information.
- **Event panel default time interval**—Sets the time period (default 600 seconds) for 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.
- **Max number of bars in bar chart view**—Sets the maximum number of bars that is displayed in bar chart views.

- **Hide DNS Suffix**—Determines how DNS names appear on the routing topology map. When DNS names of nodes appear, this suffix (if present) is trimmed from the names to reduce crowding of the layout. You can supply multiple DNS suffixes that are separated by a space, a comma, or a comma followed by a space. The default string is mycompany.com.
- **Path Highlight: ECMP degree**—Limits the number of ECMP (Equal Cost Multi-Path) routes to compute and appear 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.
- **Display protocol packet events**—Display events indicating receipt of protocol packets (BGP updates, LSPs, or LSAs).
- **Show RT communities only**—In reports and graphs for MPLS VPN networks, display only the extended communities that are interpreted as Route Targets. See Chapter 8, “VPN Routing.”

History Navigator

You can set the following default options for the *History Navigator* window.

- Choose the graphs that appear in the *History Navigator* window (only the *Events* graph is enabled by default).
 - **Events**—Show the number of routing protocol changes that occurred in the network between recorded snapshots. Examples include a neighbor adjacency going down or a new prefix being announced.
 - **Routers**—Show 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.
 - **Links**—Show the sum of router-to-router links plus the number of router-to-prefix links. Does not apply to BGP protocols.
 - **Prefixes**—Show the cumulative number of prefixes available in the network.
 - **Routes**—Show the number of routes advertised in the network. Does not apply to IGP protocols.
 - **BGP Updates**—Show the number of announced and withdrawn packets found on the network in the preceding 10 minutes. Announced packets are represented by blue lines and re-announced packets are represented in dark yellow lines.

- **EIGRP Activity**—Show updated and inferred activity for EIGRP domains. New activity appears in blue, refreshed activity appears in dark yellow.
- **Interfaces**—Show router interfaces discovered by static protocol.
- **ISIS Activity**—Show LSP activity for ISIS domains. New activity appears in blue, refreshed activity appears in dark yellow. (ISIS only)
- **OSPF Activity**—Show LSA activity for OSPF domains. New activity appears in blue, refreshed activity appears in dark yellow.
- **ES Neighbors**—Show the number of ES neighbors.
- **Prefix Neighbors**—Show the number of prefix neighbors.
- **Traffic**—Include traffic in the graph. (RAMS Traffic only)
- **Value of playback step in seconds**—Set the default value for a single step forward or backward in time during History Navigator playback. Default is 600 seconds.
- **Max number of data points in event graph**—Limit the event graph to the specified number of data points. Default is 25,000 data points.
- **Monitoring mode Update interval**—Sets the number of seconds between updates. Default is 10 seconds.

Auto-Hide

The system cannot determine whether a node or link that goes down has temporarily failed or been decommissioned. Use the following Auto-Hide options to determine when nodes and links that are down should be hidden or removed.

- **Seconds to auto-hide detached nodes**—Determines the number of seconds after which detached nodes will be hidden. A node can become detached from the rest of the network when all of its links are auto-hidden (for example, the node has failed temporarily or is decommissioned).
By default, the value is **-1** (disabled).
- **Seconds to auto-hide pseudonodes with one attachment**—Determines the number of seconds after which pseudonodes will be hidden. This condition may be caused by a problem in the router 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.

When setting this value, consider how many seconds should pass before auto-hiding the pseudonode when the number of attached links is reduced to one. By default, the value is **-1** (disabled).

- **Seconds to auto-hide failed links**—Determines the number of seconds after which a link that fails or is permanently decommissioned from service is removed from the map. These links are normally shown in red.

By default, this option auto-hides failed links in 43,200 seconds (12 hours). To disable this option, change the default value to **-1**. Note that the link will appear again if you use the *History Navigator* window to view a time when the link was up.



Because links between BGP routers and their clients are inferred (as described in [Links and Peerings](#) on page 43), the system cannot conclusively determine if such peering has failed or is simply inactive. If the system does not receive routing information about such peering within a certain amount of time, the peering is marked **inactive** (rather than **down**) and is not removed from the routing topology map.

- **Seconds to auto-hide failed nodes**—Determines the number of seconds after which a node that fails or is permanently decommissioned from service is removed from the map.

By default, this option is set to auto-hide failed nodes after 43,200 seconds (12 hours). To disable this option, change the default value to **-1**.

- **Seconds to auto-hide failed links to pseudonodes**—Determines the number of seconds after which a failed link with one end that is a pseudonode is removed from the map.

By default, the value is zero (hide immediately); the pseudonode for a broadcast network changes whenever a new Designated Router is elected.

- **Seconds to auto-hide failed pseudonodes**—Determines the number of seconds after which a pseudonode that fails is removed from the map.

By default, the value is zero (hide immediately); the pseudonode for a broadcast network changes whenever a new designated router is elected.

Working with Router Information and Layout

This section describes options for viewing and arranging routers (nodes) on the routing topology map:

- [Viewing Node and Link Details](#) on page 76
- [Hiding Nodes](#) on page 82
- [Finding a Router](#) on page 84
- [Viewing Exit Routers](#) on page 84
- [Creating Custom Filters](#) on page 85
- [Assigning Router Names](#) on page 88
- [Viewing Current Network Inventory](#) on page 91



To access these options, open the routing topology map, as described in [Opening a Routing Topology Map](#) on page 40.

Viewing Node and Link Details

In addition to the IP address and name labels, the system stores details about the nodes and links on the topology map. To access the extra detail about a particular node or link, right-click the object to open an information panel.

The title bar of the information panel shows the name of the node or link and the buttons shown in Table 16 .

Table 16 Information Title Bar Buttons

	Tack	Keeps the informational panel open. If you do not click the Tack icon, the current information panel closes when you click anywhere outside the panel.
	Close	Closes the detail panel.

Node Information Panel

Right-click a node in the routing topology map to access the node information panel (Figure 17). If the node is a pseudonode, the corresponding Designated Router (DR) is highlighted on the topology map.

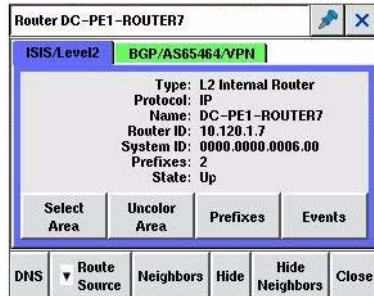


Figure 17 Node Information Panel

Each tab shows 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. If static information collection is configured to include the node, an additional tab is presented to display some of that information.

The details available for a router depend on 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. In the case of IS-IS nodes, the up state (overloaded) appears if the node is overloaded. An overloaded router remains active, but transit use is restricted.

A row of buttons on each tab provides access to functions specific to the particular instance (or routing process) on the node. The list of buttons depends on the current mode. The following buttons appear in all modes:

- **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 appears for another

node. The path between the two nodes highlights if you click the button. For an example, see [Highlighting the IP Route Between Two Points in the Network](#) on page 114. This button is not present for pseudonodes.

- **Neighbors**—Provides a list of neighboring routers and the interface addresses and metrics of the links connecting them.



For IS-IS routers that do not enable Traffic Engineering (TE) extensions, the interface addresses will not be known. If there is a single /30 or /31 prefix in common between the adjacent routers, the prefix appears in place of the source and destination interface addresses.

- **Hide**—Hides the selected node. To view the node, select **View** → **Unhide All Nodes** or click **Unhide All Nodes** in the lower-right corner of the *Routing Topology Map* window. Click the button again to hide the nodes.
- **Hide Neighbors**—Hides the neighbors of the selected node.
- **Close**—Closes the information panel. The panel also closes if you click on the map.

In Monitoring and Analysis modes, the following buttons appear:

- **Select Area**—Selects all of the nodes within the routing area that contains this node and draws a bounding box around those nodes on the topology map.
- **Uncolor/Color Area**—Colors or removes colors from the area of the topology map that contains this node.
- **Prefixes**—Shows a list of the network prefixes announced by this router. The button is disabled when there are zero prefixes.
- **OSI Prefixes**—Shows a list of the OSI prefixes announced by this router. This option appears only when OSI IS-IS is detected.
- **Events**—Shows a list originated by this router or for which this router is the neighbor. It also shows information regarding a neighbor announcing this router, including the parameters of the connection. If a time range has been selected in the *History Navigator* window, the same time range is used for this list; otherwise, events occurring in the last 10 minutes are listed.

In Planning mode, the following additional buttons appear:

- **Down**—Brings down the node for planning purposes.

- **Set Overloaded**—For IS-IS nodes only. The node is up, but not able to send data through the network. The node can receive traffic but routes are not permitted to go through it.

In RAMS Traffic, if there is traffic information for the node, a Traffic tab opens in addition to the protocol tabs, as shown in [Figure 18](#).



Figure 18 Node Traffic Tab

The body of the tab shows the IP address of the router, and information about ingress and egress flows. For example, Egress Flows: 12 indicates that the router is exporting 12 traffic flows. Egress BW (bps): 1.99 indicates that these 12 flows have a total bitrate of 1.99 K.

Click **Ingress Flows** and **Egress Flows** to show a table that lists detailed information for each flow moving into or out of the router.

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 19](#).



Figure 19 Link Information Panel

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.

The link information panel can have one or two tabs. The first tab indicates the instance of the link in a particular topology area (for example, EIGRP area). If there is more than one tab, 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 top-level tab to show the link details corresponding to the protocol instance of that tab. The color of each tab is the same as the color of the nodes and links in that area on the map. The tab label tells the protocol and area identifier.

Inside a top-level tab is an inner level of tabs if the link on the map represents multiple, parallel, physical links between the two routers. The inner tab labels indicate the interface of the router on the left side of the arrow in the title bar (for example, 10.72.4.42/24). The body of the tab provides details about the interfaces on the routers at each end of the link, including the following information:

- **Interface**—Address of the interface for the routers at either end of the link.



For IS-IS routers that do not enable Traffic Engineering (TE) extensions, the interface addresses will not be known. If there is a single /30 or /31 prefix in common between the adjacent routers, the prefix will appear in place of the source and destination interface addresses.

- **Metric**—Metric value for each interface. The link metric value helps determine the best path to take through the network, and is based on bandwidth and delay, among other factors. For EIGRP protocol links, metric is shown as two components calculated from inverse bandwidth and delay.
- **State**—Indication of whether a link is up, down, or inactive. The state Inactive applies to BGP peerings only. Unlike the physical or virtual links that connect link-state routers (OSPF and IS-IS), peerings between BGP protocol routers and their clients are inferred. If the system fails to receive

information about BGP peering within a certain time frame, the link is marked Inactive, as the system cannot determine conclusively if the peering is down.

- **BW** (for EIGRP)—Bandwidth of the data traveling across the link.
- **Delay** (for EIGRP)—Time required to move packets from the source to destination.

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

- **Uncolor/Color AS**—Color or remove color from the AS of the routing topology map that contains this link.
- **Select AS**—Select all of the ASs within the routing area that contains this link. A bounding box is drawn around the ASs.
- **Events**—List routing events related to adjacency changes on this link. If a time range has been selected in the *History Navigator* window, the same time range is used for this list; otherwise, events occurring in the last 10 minutes are listed.
- **Close**—Close the information panel. The panel also closes if you click on the map.

In RAMS Traffic, if there is traffic information for the link, a Traffic tab appears next to the protocol tabs as shown in [Figure 20](#).

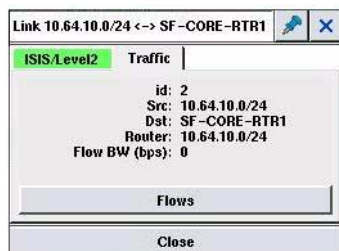


Figure 20 Link Traffic Tab

The Traffic tab provides the IP address of the router (Rtr), the number of flows on the link (Flows), and the total rate of the flows (Flow BW) in kilobits per second (kbps).

You can click Flows to show the Details by Flow table.

Hiding Nodes

You can instruct the system to show a particular class of routers on the 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 Hide Nodes option to show only these routers.

You can also hide nodes through leaf trimming. With this option, 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. Edge nodes with only one link are removed each time you select Hide Leaf Nodes.

To hide the listed nodes, perform the following steps:

- 1 Select **View** → **Hide Nodes** to open the hide *Nodes* window, as shown in Figure 21.

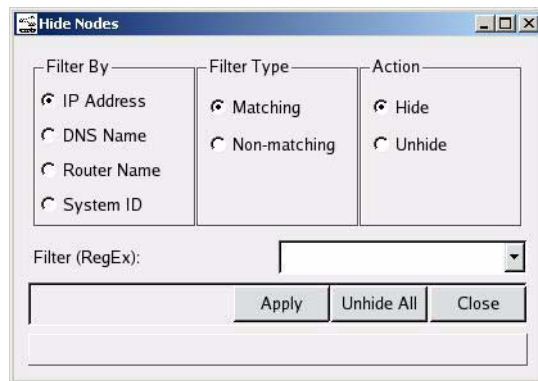


Figure 21 Hide Nodes

- 2 Choose the desired filtering option.
- 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 or click **Unhide** to restore them.

- 5 In the **Filter (RegEx)** field, type a regular expression to select the class of routers to be matched. For example, `-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.



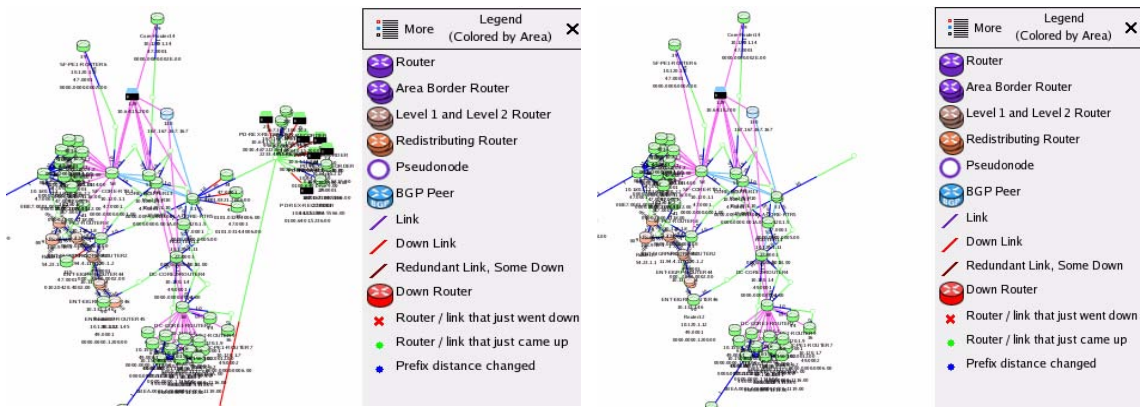
Note that extended regular expression syntax are used. Therefore, the following are metacharacters: `?`, `+`, `{`, `|`, `(`, and `)`. The syntax is not “glob” pattern matching, so use of `*-core-gw` is not correct.

- 6 Click **Apply** to save your changes.
- 7 Click **Close**.

To hide leaf nodes, perform the following steps:

- 1 Open the routing topology map.
- 2 Select **View** → **Hide Leaf Nodes** to hide the nodes on the edge of the network. [Figure 22](#) shows the result of the Hide Leaf Nodes operation performed twice in succession. Hidden nodes are saved with the topology layout.

Figure 22 Hiding Leaf Nodes - Before and After



To restore hidden nodes, click **Unhide All Nodes**.



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

Finding a Router

You can locate a router on the map according to name or address. For instructions on scanning the router list, see [Router List](#) on page 91.

To find a router by name or IP address, perform the following steps:

- 1 Select **Tools** → **Find Router**.
- 2 In the Search For field, enter the IP address, name or system ID of a router, or the prefix of a LAN pseudonode ([Figure 23](#)). If the name entered is the initial portion of multiple router names, then all those routers will be matched.

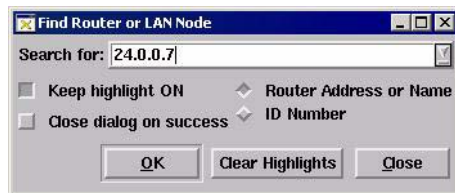


Figure 23 Find Router

- 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 the previous steps.

Viewing Exit Routers

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 balance flows to achieve optimum performance or minimize monthly cost in transit fees and bandwidth costs.

The system 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 116.

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

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **Highlight by Exit Router**.
The Highlight By Exit Router search opens.
- 3 Type the desired internet prefix, NSAP address, or domain name in the Prefix DNS Name field.
- 4 Click **OK**.

Creating Custom Filters

The Custom Filter Repository allows you to create and save custom filters, enabling you to apply them to other filter windows.

In other windows that you use filters, the custom filters you create will appear in the Filter By Expression field.



For additional information about using filters, see [Using Filters](#) on page 195 in [Chapter 4, “The History Navigator”](#)

To access the custom filter repository, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** → **Saved Filters** to open the *Custom Filter Repository* window. ([Figure 24](#)).

Name	Expression	Network Summaries
Filter1	protocol BGP	
Filter2	(eventType add router or eventType drop router)	
Filter3	med 123	DemoISPVPN.BGP/AS59300 DemoISPVPN.BGP/AS59300/VPN

3 entries Delete Edit Add

Figure 24 Custom Filter Repository

The following describes the columns shown in this repository:

- **Name**—Custom filter name
- **Expression**—Filter expression associated with the custom filter name.
- **Network Summaries**—BGP and VPN network summary in which the filter is used. You can filter the active routes in a BGP or VPN topology and view the results in its Network Summary.



Only BGP or VPN-specific filters are intended for showing results in their respective Network Summaries. Using other filters (for example, IGP, planning filters) will result in empty counts in the Network Summary column.

To add a custom filter, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** → **Saved Filters**.
The Custom Filter Repository opens.
- 3 Click **Add** from the Custom Filter Repository.
- 4 In the Name field, enter the name of the filter (Figure 25).



Figure 25 Add Custom Filter

- 5 Choose the type of filter from the drop-down list and then select the desired option from the options that are displayed when you choose the filter type.
- 6 Select the network summaries that you want to include.
- 7 Click **Show** to create a custom filter that accepts all items meeting the filter conditions, or click **Hide** to create a custom filter that rejects all items meeting the filter conditions. Clicking **Show** or **Hide** also saves the filter. Click **Cancel** to stop the operation and close the window.

To edit a custom filter, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 From the **Administration** → **Saved Filters**
The Custom Filter Repository opens.
- 3 Choose the filter you want to edit, and click **Edit**.
- 4 Modify the filter expression in the Filter field.



You can only edit the filter expression, not the filter name.

- 5 Click **Show** to have the filter accept all items meeting the filter conditions, or click **Hide** to have the filter reject all items meeting the filter conditions. Clicking **Show** or **Hide** also saves the filter. Click **Cancel** to stop the operation and close the window.

To delete a custom filter, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.

- 2 Select **Administration** → **Saved Filters**.
The Custom Filter Repository opens.
- 3 Select the filter you want to delete and click **Delete**.
- 4 Click **Yes** to confirm.

Assigning Router Names

Use the Router Name feature to control how the routers in your system are identified. By default, the IP Address of the router is used to identify the router.

To assign router names, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** → **Router Names** to open the Router Names window (Figure 26).

Router IP Address	System ID	Router Name	DNS Name	Configured Name
10.150.38.2				
10.180.38.2				
10.71.6.29				
10.150.35.2				
10.180.35.2				
10.72.6.42				
10.150.32.2				
10.180.32.2				
167.167.100.100				
10.150.29.2				
10.180.29.2				
10.180.26.1	0000.2000.112D.00			
10.150.26.1	0000.0000.112D.00			
10.150.26.2				
10.180.26.2				
10.180.23.1	0000.2000.1129.00			
10.150.23.1	0000.0000.1129.00			
10.150.23.2				
10.180.23.2				
10.180.20.1	0000.2000.1126.00			
10.150.20.1	0000.0000.1126.00			

Figure 26 Router Names Window

The following list describes the columns in this window:

- **IP Address**—IP Address for a particular router.
- **System ID**—System ID received from the router (otherwise, this column will be empty).



The System ID column will appear only if IS-IS is detected.

- **Router Name**—Router name derived from the routing protocol.
- **DNS Name**—Name resolved with the DNS server using the router's IP address.
- **Configured Name**—User-defined name that identifies the router.

The following lists the order in which router names are prioritized:

- 1 **Configured Name** (highest priority)
- 2 DNS Name
- 3 Router Name
- 4 **Router IP Address** (lowest priority)

Use the following Filter by options to determine the which routers are shown or hidden:

- **Any**—Show all rows.
- **Router IP Address**—Enter or choose the IP address of the router. If you select the router's IP address and click **Show**, the system will list only the row with the IP address you entered. If you click **Hide**, the system will show all the router IP addresses except the one you entered.
- **Router Names**—Enter or choose the name of the routers. Choose any of the following options that are displayed:
 - Substring**—Filters the routers with the given string as a substring for either Router Name, DNS Name, or Configured Name.
 - Exact Match**—Filters the routers with the given string as an exact match either of its Router Name, DNS Name, or Configured Name.
 - Begins With**—Filters the routers with the beginning string used for router name, DNS name, or user-specified name.

The following buttons are included in the Router Names window:

- **Show**—Show all router entries you want to view.
- **Hide**—Hide router entries.
- **Save**—Save information you edit. This button will be active only when you have edited information on the screen.
- **Import**—Edit several router names.
- **Close**—Exit the Router Names window.

To change a router name, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** → **Router Name** to open the Router Names window.
- 3 Select the row of the router whose name you want to change.
- 4 Enter the new name in the Configured Name column.
- 5 Click **Save**.

Changing Multiple Router Names

To change the names of multiple routers, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** → **Router Name** to open the Router Names window.
- 3 Click **Import**.
- 4 Enter router names in the format shown in [Figure 27](#).

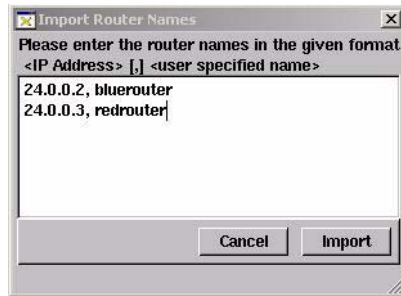


Figure 27 Import Router Names Dialog B

- 5 Click **Import**.



If you attempt to import a router name that is not known or in an incorrect format, the error message “Discarded Invalid Import Entries” will appear at the bottom of the topology window.

Viewing Current Network Inventory

The application can show 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, etc., and each entry in any list can be traced back to the associated router in the topology map with a single click.

Router List

Open the *List of All Routers* window to perform the following tasks:

- 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).
- List 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 of All Routers* window, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **List Routers** to open the *List of All Routers* window.

The screenshot shows a window titled "List of All Routers: vfro6015EPreBC/BGP, [ISIS 47.0002 47.0003], [Traffic vfro6fr1], TrafficReports". At the top, there is a "Filter by:" dropdown menu set to "Any" and "Show" and "Hide" buttons. Below is a table with the following data:

Router	IP Address	Type	Protocol	State	Area ID	System ID	Area or AS
1.1.1.2	1.1.1.2	Originator	IP	Up			vfro6015EPreBC.BG
164_Lilleci	192.168.244.223	L1 Internal Router	IP	Up	47.0003	0164.0244.0223.00	vfro6015EPreBC.ISI
192.168.0.242	192.168.0.242	Originator	IP	Up			vfro6015EPreBC.BG
192.168.1.10	192.168.1.10	Originator	IP	Up			vfro6015EPreBC.BG
192.168.23.210	192.168.23.210	Originator	IP	Up			vfro6015EPreBC.BG
192.168.72.94	192.168.72.94	Originator	IP	Up			vfro6015EPreBC.BG
192.168.110.190	192.168.110.190	Originator	IP	Up			vfro6015EPreBC.BG
192.168.190.58	192.168.190.58	Originator	IP	Up			vfro6015EPreBC.BG

At the bottom of the table, it says "1173 top level entries, 2682 total entries".

Figure 28 List of All Routers

- 3 Use the Filter by drop-down list at the top of the window to filter the list as needed (see [Using Filters](#) on page 195).
- 4 To identify a router on the map, click anywhere in the row corresponding to the router. The row is highlighted in the *List of All Routers* window and the router flashes yellow on the routing topology map.

Links List

Open the *List of All Links* window to display 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.



For IS-IS routers that do not enable Traffic Engineering (TE) extensions, the interface addresses will not be known. If there is a single /30 or /31 prefix in common between the adjacent routers, the prefix will appear in place of the source and destination interface addresses.

To view the list of all links, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **List Links** to open List of All Links window (Figure 29).

NSAP Link	Source Interface	Destination Interface	Bandwidth	Metric	State	Area or AS
IGP Link 27.000	--	LAN Pseudo-Noc	0 Kbps	63	Down	PDLab60.ISIS/Le
27.0001.0030	LAN Pseudo-Noc	--	0 Kbps	0	Up	PDLab60.ISIS/Le
IGP Link 49.000	--	LAN Pseudo-Noc	0 Kbps	10	Up	PDLab60.ISIS/Le
49.0001.0BEA	LAN Pseudo-Noc	--	0 Kbps	0	Up	PDLab60.ISIS/Le
IGP Link 49.000	--	--	0 Kbps	1	Up	PDLab60.ISIS/Le
49.0001.0BEA	--	--	0 Kbps	1	Up	PDLab60.ISIS/Le
IGP Link 49.000	--	--	0 Kbps	1	Up	PDLab60.ISIS/Le
49.0001.0BEA	--	--	0 Kbps	1	Up	PDLab60.ISIS/Le
IGP Link 49.000	--	--	0 Kbps	1	Up	PDLab60.ISIS/Le
49.0001.0BEA	--	--	0 Kbps	1	Up	PDLab60.ISIS/Le

162 top level entries, 494 total entries

Figure 29 List of All Links Window

- 3 Use the Filter by drop-down list at the top of the window to filter the links appearing in the window (see [Using Filters](#) on page 195).
- 4 Perform any of the following operations:
 - Select a link in the list, which causes the link to flash yellow on the map.
 - Copy a single row of the table pressing **Ctrl+C** or the entire table pressing **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 **Export**. 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* window.
- If the routing topology has changed since the report was opened, refresh the contents by clicking **Refresh**.

Interfaces List

Open the Interfaces List to display the router interfaces discovered by static protocol.

To view the interfaces list, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **List Interfaces** to open List of Interfaces window (Figure 29).

Router/Net	Interface	Address	Index	MAC Address	BW (kbps)	Admin Status	Oper Status	Area or AS
Core-Router14.packetdesign.com	Fa0/0	10.64.27.14/24	1	00:02:b9:bc:14:20	100000	Up	Up	PACKETDESIGNLABNETWORKS.RR
Core-Router14.packetdesign.com	Fa0/1	10.77.1.14/24	2	00:02:b9:bc:14:21	10000	Up	Up	PACKETDESIGNLABNETWORKS.RR
Core-Router14.packetdesign.com	Fa1/0	Unassigned	3	00:02:b9:bc:14:31	100000	Down	Down	PACKETDESIGNLABNETWORKS.RR
Core-Router14.packetdesign.com	Fa1/1	Unassigned	4	00:02:b9:bc:14:32	100000	Down	Down	PACKETDESIGNLABNETWORKS.RR
Core-Router14.packetdesign.com	Nu0	Unassigned	6	--	10000000	Up	Up	PACKETDESIGNLABNETWORKS.RR
Core-Router14.packetdesign.com	Lo0	10.120.1.14/32	7	--	8000000	Up	Up	PACKETDESIGNLABNETWORKS.RR
CORE-ROUTER13.packetdesign.com	Fa0/0	10.64.25.13/24	1	00:b0:8e:96:cc:00	100000	Up	Up	PACKETDESIGNLABNETWORKS.RR
CORE-ROUTER13.packetdesign.com	Fa1/0	10.64.26.13/24	2	00:b0:8e:96:cc:1c	100000	Up	Up	PACKETDESIGNLABNETWORKS.RR
CORE-ROUTER13.packetdesign.com	Fa2/0	10.64.27.13/24	3	00:b0:8e:96:cc:38	100000	Up	Up	PACKETDESIGNLABNETWORKS.RR
CORE-ROUTER13.packetdesign.com	Nu0	Unassigned	5	--	10000000	Up	Up	PACKETDESIGNLABNETWORKS.RR

Figure 30 List of Interfaces Window

- 3 Use the Filter by drop-down list at the top of the window to filter the links appearing in the window (see [Using Filters](#) on page 195).

Prefix List

Open the List of Prefixes window to obtain the following information:

- 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.

- View the routers in a network that are advertising default routes.
- List the advertised BGP prefixes and the list of attributes associated with each BGP prefix.

To view the list of prefixes, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **List Prefixes** to open List of All Links window (Figure 31).

Prefix	Router/Net	Attributes	State	Area or AS
0.0.0.0/0	Router23	Metric: bw=256000 dly=2560 (External)	Up	trunk4062.RA148.EIGRP/AS1
0.0.0.0/0	24.0.0.12	Metric: 1 (AS External) Forward Addr: 192.168.0.254	Up	trunk4062.RA148.OSPF/0.0.0.1
0.0.0.0/0	24.0.0.12	Metric: 1 (AS External) Forward Addr: 192.168.0.254	Up	trunk4062.RA148.OSPF/0.0.0.3
0.0.0.0/0	24.0.0.12	Metric: 1 (AS External) Forward Addr: 192.168.0.254	Up	trunk4062.RA148.OSPF/Backbone
10.23.89.0/30				
10.23.89.0/30	24.0.0.5	Metric: 11112 (Area External)	Up	trunk4062.RA148.OSPF/0.0.0.1
10.23.89.0/30	24.0.0.11	Metric: 11113 (Area External)	Up	trunk4062.RA148.OSPF/0.0.0.1
10.23.89.0/30	24.0.0.7	Metric: 15207 (Area External)	Up	trunk4062.RA148.OSPF/0.0.0.3
10.23.89.0/30	24.0.0.11	Metric: 11113 (Area External)	Up	trunk4062.RA148.OSPF/0.0.0.3
10.23.89.0/30	24.0.0.23	Metric: 11111	Up	trunk4062.RA148.OSPF/Backbone
10.23.89.0/30	Router23	Metric: bw=256000 dly=2560 (External)	Up	trunk4062.RA148.EIGRP/AS1
74.74.74.0/24				

147 top level entries, 865 total entries

Figure 31 List of Prefixes Window

- 3 Use the Filter by drop-down list at the top of the report to filter the prefixes appearing in the window (see [Using Filters](#) on page 195).
- 4 Perform any of the following operations:
 - Select a router in the list, and the node will flash yellow on the map.
 - If the routing topology has changed since the report was opened, refresh the contents by clicking **Reload**.

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

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Locate the node on the map.
- 3 Right-click on the node to open the node information panel.

4 Click **Prefixes**.

The List of Prefixes window opens to show all prefixes that are advertised by the node you selected. For each prefix, all nodes that advertise the prefix are listed.



The names and addresses in the Router/Net column are the routers that are advertising the prefix. The way that the routers are listed 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.

OSI Prefixes List

Open the List of OSI Prefixes window to obtain the following information:

- Determine if a prefix is currently advertised or not, and by which routers.
- See what metric is advertised with each prefix.

To view the List of OSI Prefixes/ES Neighbors, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map
- 2 Choose **Tools** → **List of OSI Prefixes** to open the List of OSI Prefixes window.
- 3 Use the Filter by drop-down list at the top of the report to filter the OSI Prefixes and ES Neighbors.

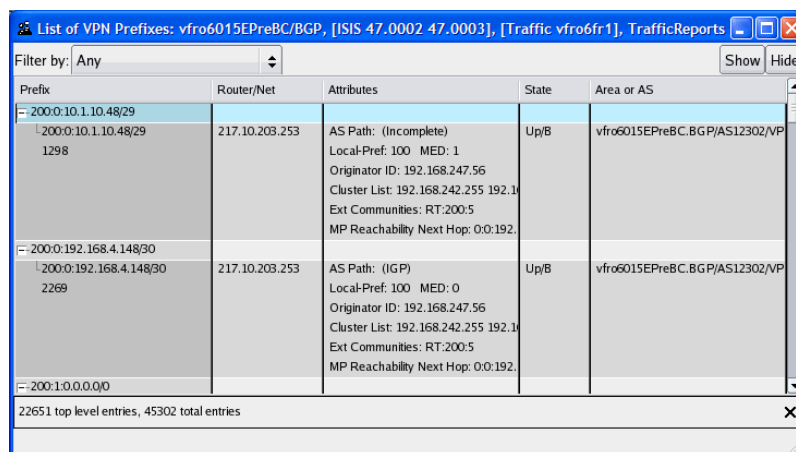
VPN Prefixes List

Open the *List of VPN Prefixes* window to obtain the following information:

- *Determine if a prefix is currently advertised or not, and by which routers.*
- *See what metric is advertised with each prefix.*
- *List the VPN routers in a network. (To list the routers, sort on the Router/Net column, right-click the column header and choose **Group**, and then right-click and choose **Collapse all**).*

To view the list of VPN prefixes, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **List VPN Prefixes** to open the List of VPN Prefixes window.



The screenshot shows a window titled "List of VPN Prefixes: vfro6015EPreBC/BGP, [ISIS 47.0002 47.0003], [Traffic vfro6fr1], TrafficReports". The window has a "Filter by:" dropdown menu set to "Any" and "Show" and "Hide" buttons. The main content is a table with the following columns: Prefix, Router/Net, Attributes, State, and Area or AS. The table contains three rows of data, each with a collapsed tree view of prefixes. The first row shows a prefix tree for 200.0.10.1.10.48/29 with 1298 entries, associated with Router/Net 217.10.203.253. The second row shows a prefix tree for 200.0.192.168.4.148/30 with 2269 entries, also associated with Router/Net 217.10.203.253. The third row shows a prefix tree for 200.1.0.0.0/0. The "Attributes" column contains detailed BGP information such as "AS Path: (Incomplete)", "Local-Pref: 100 MED: 1", "Originator ID: 192.168.247.56", "Cluster List: 192.168.242.255 192.168.242.255 192.168.242.255", "Ext Communities: RT:200:5", and "MP Reachability Next Hop: 0.0:192.". The "State" column shows "Up/B" for all entries. The "Area or AS" column shows "vfro6015EPreBC.BGP/AS12302/VP". At the bottom of the table, it states "22651 top level entries, 45302 total entries".

Prefix	Router/Net	Attributes	State	Area or AS
200.0.10.1.10.48/29 1298	217.10.203.253	AS Path: (Incomplete) Local-Pref: 100 MED: 1 Originator ID: 192.168.247.56 Cluster List: 192.168.242.255 192.168.242.255 192.168.242.255 Ext Communities: RT:200:5 MP Reachability Next Hop: 0.0:192.	Up/B	vfro6015EPreBC.BGP/AS12302/VP
200.0.192.168.4.148/30 2269	217.10.203.253	AS Path: (IGP) Local-Pref: 100 MED: 0 Originator ID: 192.168.247.56 Cluster List: 192.168.242.255 192.168.242.255 192.168.242.255 Ext Communities: RT:200:5 MP Reachability Next Hop: 0.0:192.	Up/B	vfro6015EPreBC.BGP/AS12302/VP
200.1.0.0.0/0				

Figure 32 List of Prefixes Window

- 3 Use the Filter by drop-down list at the top of the report to filter the list.

Understanding Topology Groups

Topology groups are collections of network elements that are treated as a single unit for use in alert watchlists. A watchlist is a set of routers associated with a specific alert (see [Creating New Alerts](#) on page 434).

In addition to their role in alert watchlists, router groups allow you to simplify the topology map display by showing the routers in a group as a cloud, which you can operate on as a single entity or expand to display the individual routers.

Child groups are groups that are nested within another group.



See [Administration](#) on page 60 for a list of the group types that you can create from the Administration menu.

Example: The router group NewYork is created with routers A, B, and C, and the router group California is created with routers D, E, and F. With these groups in place, you can define alert watchlists that focus on each of these areas. If you want to create another watchlist that includes both of these groups, you can define the group UnitedStates and add NewYork and California as child groups.

Creating Groups on the Topology Map

You can include network elements in a group to increase the ability to analyze information.



Be sure to save the routing layout before making any changes to the layout.

To create a router group directly on the topology map, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Click, hold, and drag the cursor diagonally from an open area that encompasses the routers you want to group. Release the mouse button.

A bounding box appears around the routers and the selected routers change color, as shown in the following figure.

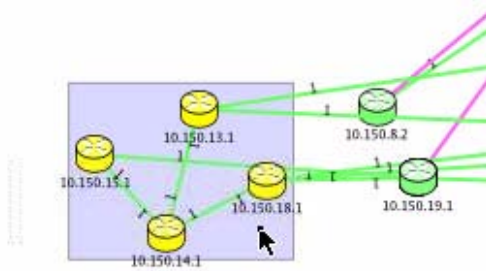


Figure 33 Router Group Bounding Box on the Topology Map



Only the routers 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.

- 3 With the cursor placed within the bounding box, right-click to open the Selection panel (Figure 34).

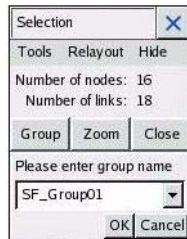


Figure 34 Selection Panel

- 4 Click **Group**.

The Selection panel expands to display a field for creating a group name.

- 5 Type a name and click **OK**.

You can resize a group cloud that is open. Double-click on the cloud, if necessary, to show the routers in the group. by (Figure 36). Click once to display a blue bounding box with a small rectangle in the lower right corner. Drag the rectangle to expand or shrink the cloud.

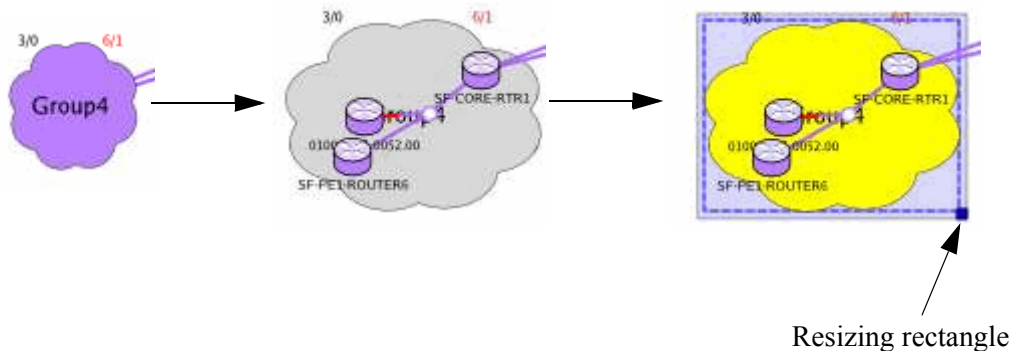


Figure 35 Enlarging a Group Cloud

In addition to creating a single group on the topology map, you can:

- Create multiple router groups.
- Nest a group a within another group.
- Include a router in multiple groups.
- View the routers within a group.

You can also create a group that contains individual elements that are not close to each and using a bounding box will not work.

To group individual nodes on the routing topology map, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Click any node on the map.
A bounding box is created around the node.
- 3 Press and hold the **Ctrl** key and then click on other node.
The bounding box expands to contain the additional nodes.
With the elements selected, right-click and choose **Group**.
- 4 Type a name and click **OK**.
The selected area changes to a cloud. Links and element locations will change on the topology map to accommodate the disparate nodes.

To view the routers within a group on the topology map, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Double-click on a grouping cloud.

The cloud expands to show its contents, as shown in the following figure.

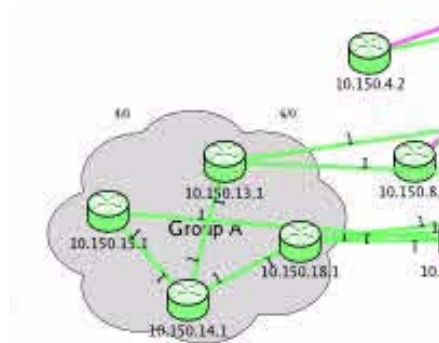


Figure 36 Viewing Elements Within a Cloud

With the cloud expanded, you can:

- Move elements to different positions within the cloud by clicking and dragging elements within the cloud.
- Drag elements out of the cloud to remove them from the group or drag routers in to extend the group.

Right-clicking on the cloud opens the cloud panel, as shown in (Figure 37):

SF_Group01			
Number of routers: 13			
Number of nodes: 14			
Number of links: 24			
Number of prefixes: 56			
Number of VPN prefixes: 3761			
Routers	Links	Prefixes	List VPN Prefixes
Ungroup	Show Contents	Close	

Figure 37 Cloud Panel

The general status of network elements within a cloud is indicated by the numbers appearing above it. By gliding the cursor over a cloud you can also obtain pop-up statistics that include the group name and a breakdown of the included elements with the up or down status (Figure 38).

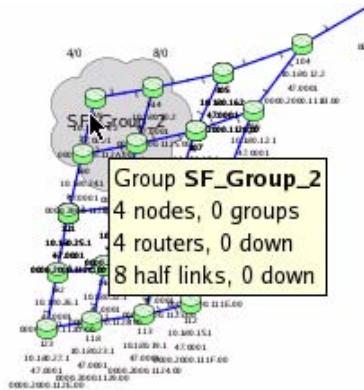


Figure 38 Status in Cloud

- 3 Perform any of the following operations on the cloud:
 - **Routers**—Click the **Routers** button to open the List of Routers in Group report (Figure 39).

Router	IP Address	Type	Protocol	State	Area ID	System ID	Area or AS
- 10.64.10.0/24							
10.64.10.0/24	9/10.64.10.0	LAN Pseudo-Node	IP	Up	47.0001	0000.0000.0001.03	PDLab60.ISIS/Level2
- 10.180.1.2							
10.180.1.2	67/10.180.1.2	L2 Internal Router	IP + OSI (Dual)	Up	47.0001	0000.2000.1111.00	PDLab60.ISIS/Level2
10.180.1.2	14/10.180.1.2	Originator	IP	Up			PDLab60.BGP/AS65464/VPN
+ 10.180.2.2							
+ 10.180.3.2							

14 top level entries, 41 total entries

Figure 39 List of Routers in a Group

- **Links**—Click the **Links** button to open the List of Links in Router Group report (Figure 40).

Link	NSAP Link	Source Interface	Destination Interface	Bandwidth	Metric	State	Area or AS
- IGP Link 10.180.1.2 <> 10.180.1.1							
└ 10.180.1.2 -> 10.180.11.1	47.0001.0000.2000.1111.00 ->	--	--	0 Kbps	1	Up	PDLab60.ISIS/Level2
└ 10.180.1.2 <- 10.180.11.1	47.0001.0000.2000.1111.00 <-	--	--	0 Kbps	1	Up	PDLab60.ISIS/Level2
- IGP Link 10.180.2.2 <> 10.180.1.1							
└ 10.180.2.2 -> 10.180.11.1	47.0001.0000.2000.1112.00 ->	--	--	0 Kbps	1	Up	PDLab60.ISIS/Level2
└ 10.180.2.2 <- 10.180.11.1	47.0001.0000.2000.1112.00 <-	--	--	0 Kbps	1	Up	PDLab60.ISIS/Level2
+ IGP Link 10.180.3.2 <> 10.180.1.1							
+ IGP Link 10.180.4.2 <> 10.180.1.1							
+ IGP Link 10.180.5.2 <> 10.180.1.1							

12 top level entries, 36 total entries

Figure 40 List of Links in a Group

- **Prefixes**—Click the **Prefixes** button to open the List of Prefixes in Router Groups report (Figure 41).

Prefix	Router/Net	Attributes	State	Area or AS
- 10.120.1.1/32				
└ 10.120.1.1/32	SF-CORE-RTR1	Metric: 10	Up	PDLab60.ISIS/Level2
- 10.120.1.6/32				
└ 10.120.1.6/32	SF-PE1-ROUTER6	Metric: 10	Up	PDLab60.ISIS/Level2
+ 10.73.6.0/24				
+ 10.73.0.0/16				

37 top level entries, 93 total entries

Figure 41 List of Prefixes in Router Groups

- **List VPN Prefixes**—Click the **VPN Prefixes** button to open the List of VPN Prefixes for Router Group report (Figure 42).

Prefix	Router/Net	Attributes	State	Area or AS
- 100:1.122.122.1.0/24				
└ 100:1.122.122.1.0/24	10.120.1.1	AS Path: (IGP) Local-Pref: 0 Originator ID: 10.180.1.2 Cluster List: 10.120.1.1 Ext Communities: RT:100:1 MP Reachability Next Hop: 0:0:10	Up/B	PDLab60.BGP/AS65464/VPN
├ 100:1.122.122.2.0/24				
├ 100:1.122.122.3.0/24				
└ 100:1.122.122.4.0/24				
2209 top level entries, 4418 total entries				

Figure 42 List of VPN Prefixes for Router Group

- **Ungroup**—Ungroup on the map or delete (destroy) the group. By ungrouping the cloud on the map, the elements retain a group identity in the Router Groups report but the cloud does not appear on the topology map. Deleting the group removes it from the Router Groups report and the topology map.
- **Show Contents**—View the routers within the cloud. This is the same as double-click the cloud.
- **Close**—Close the cloud panel. Double-click the expanded cloud to close the panel.
- **Hide Contents**—Close the information panel for the opened group.

Creating Groups Using the Menu

You can create router groups, link groups, path, or prefix groups from the Administration menu. Groups are useful in configuring alerts, applying filters, and focusing in on specific areas within the topology map.

The following group types are accessible from the Administration menu in the client application:

- Router Groups
- Link Groups
- Prefix Groups

- Path Groups
- VPN Customer Groups
- VPN RT Groups
- VPN Prefix Groups



Any router that belongs to multiple groups can only appear in one group on the topology map. Any other groups to which that element belongs are disabled from being displayed.

The following options are supported for most of the group types (see [Working with Groups](#) on page 106):

- New Group—Create a new group.
- Edit Group—Modify an existing group.
- Copy—Make a copy of the group or group element to use in another group.
- Move—Move the group or group element to another group.
- Delete—Remove a group or group element.
- Group by Areas (router groups only)—Create a router group with a structure that matches the topology hierarchy. See [Understanding the Topology Hierarchy](#) on page 64 for information on the topology hierarchy.
- Tooltips—Move the cursor over a group name to view details about the group ([Figure 43](#)). Tooltips are available in the group window and in the dialog box that opens when you move a group or group element.

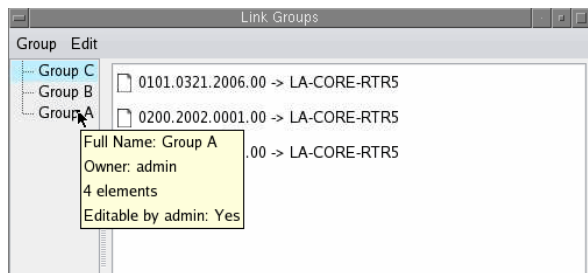


Figure 43 Group Tooltip

- Router group checkbox (route groups only, see [Figure 44](#))—Select the checkbox for a router group to display that group on the map.

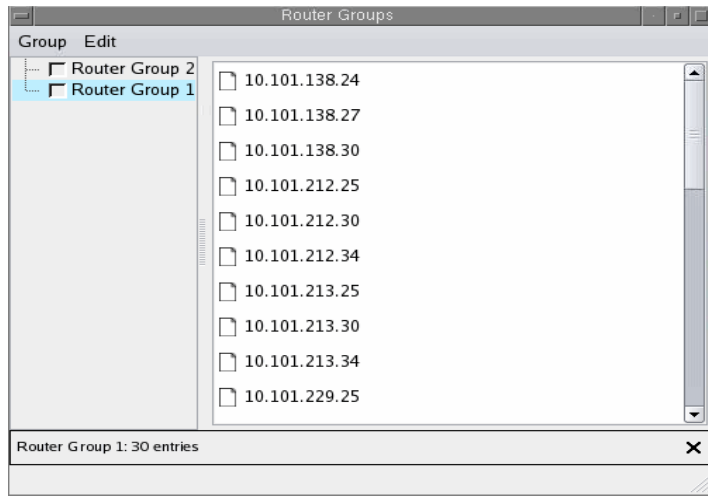


Figure 44 Router Groups

Working with Groups

You can create, edit, copy, move, or delete groups.



Changes that you make to groups are reflected immediately on the routing topology map. The system prevents you from making changes if you do not have permission to do so.

To create a new group, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** and select one of the Groups menu items. If a group does not exist, a pop-up window indicates how to create a new group. Click **OK** to close the pop-up.
- 3 If a group of this type does not already exist, a pop-up window indicates how to create a new group. Click **OK** to close the pop-up.
- 4 Choose **Group** → **New Group**.
- 5 Enter a group name, as shown in [Figure 45](#).

- For most of the group types, the first tab that opens shows a list of IP addresses or names on the left. Highlight the items that you want to add to the group, and click -> to move them to the selection area on the right (Figure 45).

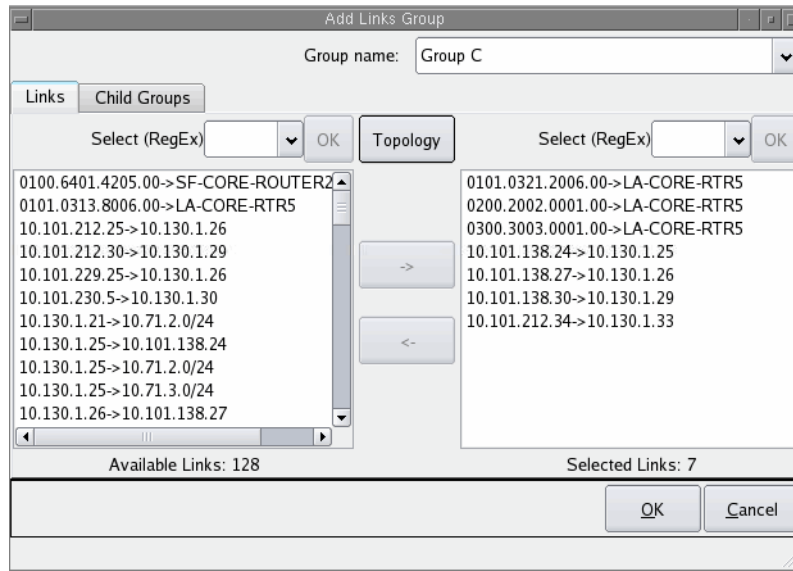


Figure 45 Creating a New Group

For path groups, enter the starting and terminating IP addresses for each path, and click **Save** to add the path to the group (Figure 46).

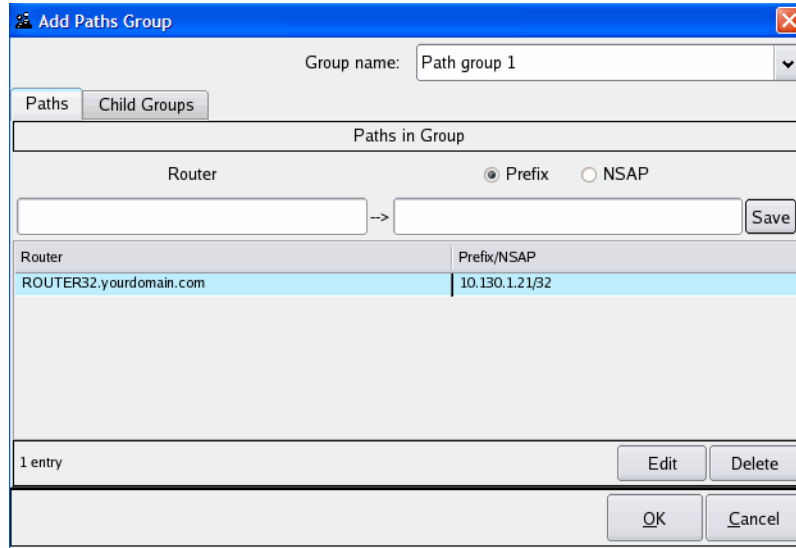


Figure 46 Creating a New Path Group

- 7 If you want to select only specific members of the list, type the common characters in the Select (RegEx) field and click OK by the field. For example, if you only want IP addresses starting with 192, type 192 in the Select (RegEx) field, click OK by the field, and then click the arrow to move the selected IP addresses from the Available Items field to the Selected Items field.
- 8 Click the **Child Groups** tab.

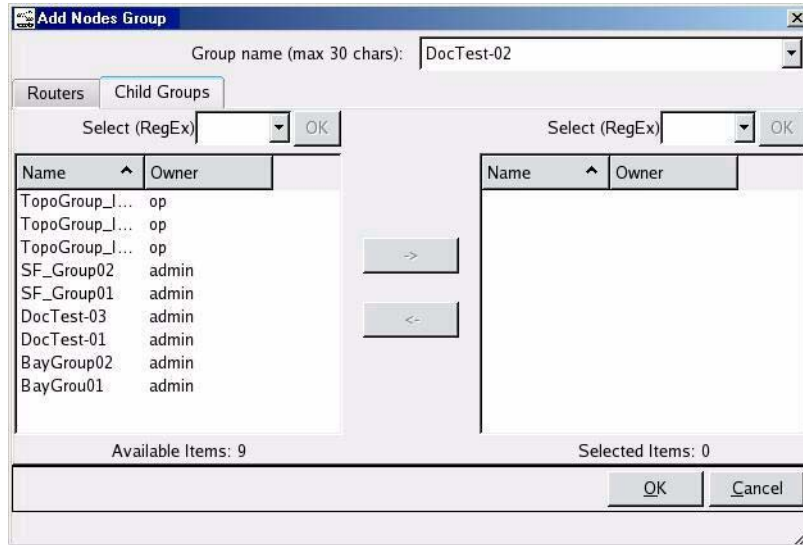


Figure 47 Child Groups

- 9 The Child Groups tab lists items associated with the group type. If you want to select only specific members of the list, type the common characters in the Select (RegEx) field and click **OK** by the field.

For example, if you only want IP addresses starting with 192, type **192** in the Select (RegEx) field, click **OK** by the field, and then click the arrow to move the selected IP addresses from the Available Items field to the Selected Items field.

- 10 After adding the appropriate child groups, click **OK** to save your settings.

To edit a group, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** and select the Group menu item to open the group window
- 3 Right-click the group name and choose **Edit Group**.
- 4 Set up the group elements as you would when adding a new group. See [Creating Groups Using the Menu](#) on page 104.
- 5 Click **OK**.

To move or copy a group within the group hierarchy, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** and select the Group menu item to open the group window.
- 3 Use one of these options to move the group:
 - Right-click the group you want to move and choose **Move** or **Copy**. In the dialog box that opens, choose the group that will include the selected group as a subgroup or choose **Top Level**, and click **OK**. The group is moved or copied to the new location (Figure 48).

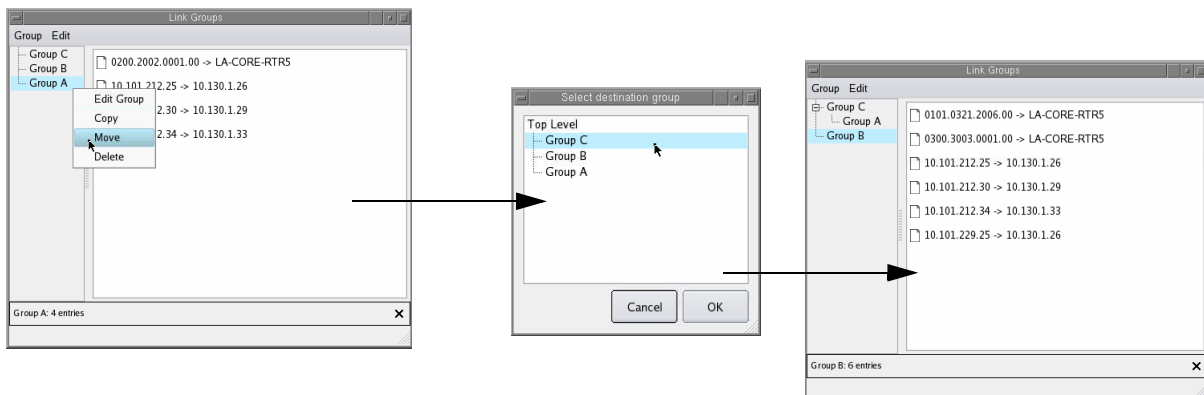


Figure 48 Moving Groups

- Drag and drop the group to a new location in the hierarchy.



The system prevents you from dragging and dropping an item if you do not have permission to do so.

To copy or move a group element within the group hierarchy, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** and select the Group menu item to open the group window.
- 3 Choose one of these options to copy or move an individual group member (such as an IP address) to another location:
 - Right-click the item you want to move and choose **Move** or **Copy**. In the dialog box that opens, choose the group that will include the selected item, and click **OK**. The item is copied or moved to the new group.
 - Drag and drop the item to a different location in the hierarchy.

To delete a group or group element, perform the following steps:



Only the group owner or an administrator can delete a group.

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** and select the Group menu item to open the group window.
- 3 Select the element or group, right-click, and choose **Delete**.
- 4 Click **OK** to confirm.



Removing a router from a group does not delete the router from your topology. You can add a router

To create a single router group that matches the structure of the topology hierarchy, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** → **Router Groups**.

- 3 Choose **Group** → **Group by Area**.
- 4 Type a name and click **Apply**.

A new router group is created with a structure that matches the topology hierarchy.

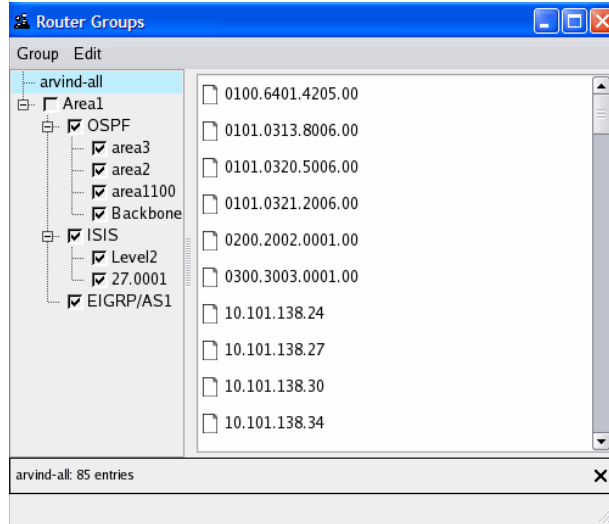


Figure 49 Grouping by Area

Hiding Forwarding Adjacencies in Link Groups

Some networks contain routers include forwarding adjacency (FA) configuration. FAs allow administrators specify label-switched path (LSP) tunnels as links in the IGP network. A forwarding adjacency can be created between routers regardless of their location in the network, and routers with forwarding adjacency can be multiple hops apart.

FAs can crowd the routing topology map, making it more difficult to focus on other areas of interest. To simplify the routing topology display, you can add all the FAs to a single link group and then hide the group containing the forwarding adjacencies in your network and then hide the group when you want to focus on other areas of interest.

To create a link group containing all the FAs in the network, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Administration** → **Link Groups**.
- 3 Choose **Group** → **New Group**.
- 4 Enter a name for the group.
- 5 Click **Select FA** to highlight all of the FAs in the Links list.

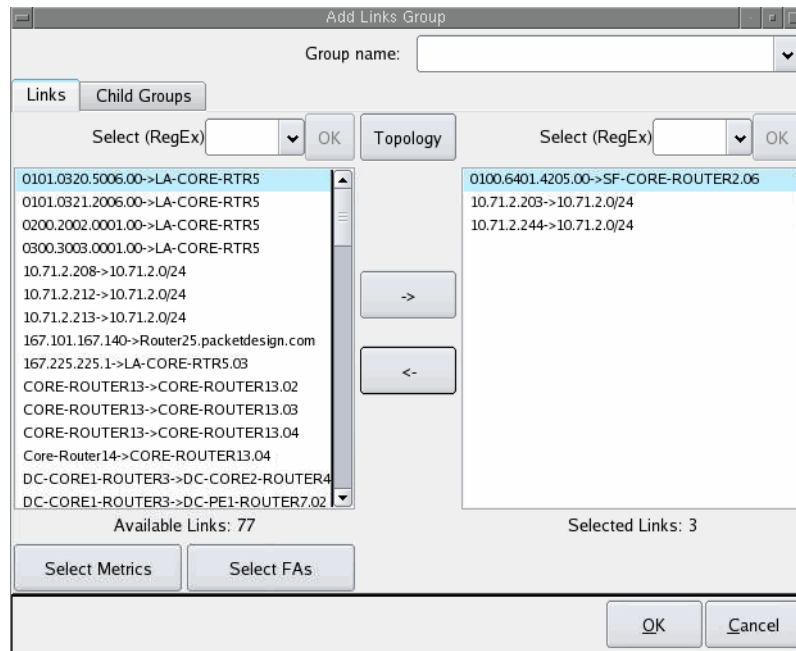


Figure 50 Link Group - Select FA Option

- 6 Click the right facing arrow to move the highlighted link to the selection area.
- 7 Click **OK**.

A new group is now created containing all the FAs. You can now hide the group on the routing topology map.

Understanding Network Routes

This section describes client application supports for viewing and managing routes through the network:

- [Highlighting the IP Route Between Two Points in the Network](#) on page 114
- [Finding a Route By Prefix](#) on page 116
- [Finding a VPN Route By Prefix](#) on page 117
- [Viewing the Highlighted Path Cost for EIGRP](#) on page 118
- [Diagnosing EIGRP Topology Errors](#) on page 121
- [Assigning AS Names](#) on page 128
- [Assign and Verify BGP AS Assignments to Routers](#) on page 131

Highlighting the IP Route Between Two Points in the Network

Viewing the IP paths taken by traffic from a source router to a destination router in a multidomain network is useful for network planning. You can identify paths for which it is critical to avoid delays that are caused by rerouting due to router failures, for example a VoIP service path between an IP PBX and a PSTN media gateway.

The system can quickly show the path resolved between two nodes in a network at the current time or at any point in recorded topology history.

Paths are shown in the following colors:

- Forward path: Green
- Reverse path: Orange

Nodes are shown in the following colors:

- Unidirectional: source: Green, destination: Yellow
- Bidirectional: source: Green, destination: Orange

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 *Find or List Paths* window described in [Finding a Route By Prefix](#) on page 116.

The path is selected using the information panels for the source and destination nodes on the routing topology map. Figure 51 shows the node information panels for the source and destination of a route.

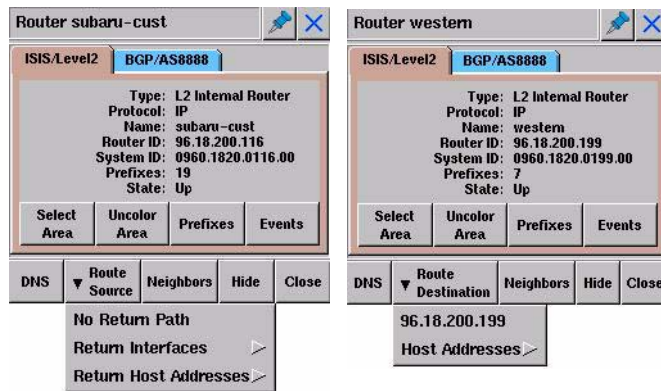


Figure 51 Source and Destination Node Information Panels

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

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Right-click the source node on the map to open the node information panel.
- 3 Click **Route Source**, and one of the following choices from the drop-down list:
 - **No Return Path**—Provides route source only.
 - **Return Interfaces**—Specifies return interface for route source.
 - **Return Host Addresses**—Provides the host address.

The route from one router toward another router is highlighted in yellow on the routing topology map. The return route highlights in orange.

- 4 Right-click on the destination node on the routing topology map.
- 5 Click **Route Destination** in the node information panel that opens, and then select an interface from the drop-down list, or select **Host Addresses**.

The route from one router toward another router is highlighted in yellow on the routing topology map. The return path is highlighted in orange.

- 6 To see the path details, click **List/Find Paths**.



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 system, 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, the system 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, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **List/Find Paths** to open the *The Find or List Paths* window.

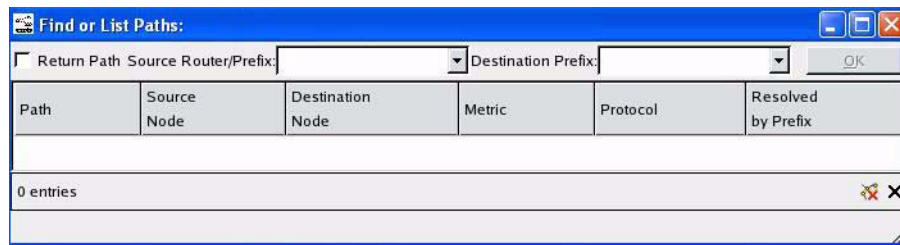


Figure 52 Find or List Paths

- 3 Enter the IP address or System ID of the source router or name in the Source Router field.
- 4 Enter the destination IP address, Internet prefix or domain name in the Destination Prefix field.
- 5 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 listed in the lower section of the *Find or List Paths* window, including the link metric and the prefix by which each next hop was resolved. The forward path highlights in yellow on the routing topology map and the return path appears orange.



A path flashes momentarily on the topology map when its corresponding entry in the *Find or List Paths* window is selected.

Multiple paths are shown for equal-cost multipath routes.



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.

Finding a VPN Route By Prefix

In Planning mode, you can find VPN paths in the topology.

To find VPN paths, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **List/Find VPN Paths** to open the *Find or List VPN Paths* window.

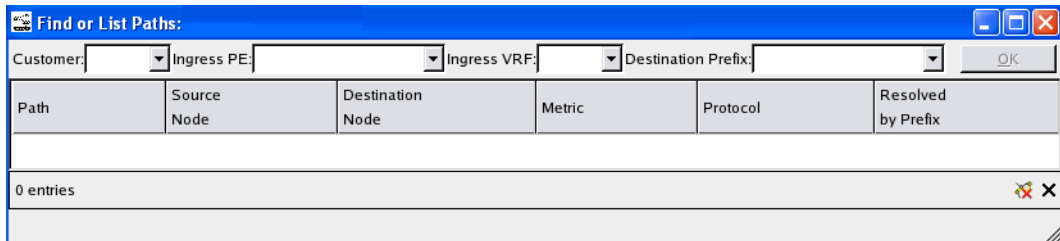


Figure 53 Find or List VPN Paths

- 3 Enter the customer name in the Customer field. The customer name should be an existing Customer to route target (RT) mapping (as defined by **Administration** → **VPN Customer -RT Mapping Configuration**). The customer name is case-sensitive.

- 4 Enter the IP address of the ingress PE in the Ingress PE field.
- 5 Select the desired Ingress VRFs.

This step lists all existing VRFs on the selected Ingress PE belonging to the selected Customer. If the Ingress VRF field remains empty after the fields Customer and Ingress PE are populated, there are no VRFs on the Ingress PE belonging to that customer.

- 6 Enter the desired prefix of the selected VPN in the Destination Prefix field in IP4 format.
- 7 Click **OK**.



During route resolution only VPN routes with RTs matching the RT import policy of the Ingress VRF are considered. If a path is found, the segments of the path are listed in the lower section of the *Find or List VPN Paths* window, including the link metric and the prefix by which each hop was resolved. The forward path highlights in yellow on the routing topology. The paths will flash momentarily on the topology map when its corresponding entry in the Find or List Paths is selected.

Viewing the Highlighted Path Cost for EIGRP

You can view the details of a highlighted path, select **Tools** → **List/Find Paths**. An example for the EIGRP protocol is shown in [Figure 54](#).

To find the highlighted path cost for IEGRP, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **List/Find Paths** to open the *Find or List Paths* window.

The Metric (bw) and Metric (delay) columns for EIGRP show the cost in EIGRP metric units for the bandwidth and delay values that are configured for the link. The Metric column lists the amount that each link contributes to the overall path distance, or cost. The total path cost for EIGRP is the sum of the *delay* values for each hop plus the maximum of the *bw* values.

Applications Places System Mon Mar 17, 2:16 PM

Find or List Paths: LabNetworksBGP

Return Path Source Router: Core-Router14 Destination Prefix: 10.150.30.2/32 OK

Path	Source Node	Destination Node	Metric	Metric (bw)	Metric (delay)	Protocol	Resolved by Prefix
Core-Router14 -> 10.150.30.2/32							
Path 1			68				
Hop 1	Core-Router14	CORE-ROUTER13.04	10			ISIS	10.150.30.2/32
Hop 2	CORE-ROUTER13.04	CORE-ROUTER13	0			ISIS	10.150.30.2/32
Hop 3	CORE-ROUTER13	CORE-ROUTER13.03	10			ISIS	10.150.30.2/32
Hop 4	CORE-ROUTER13.03	SF-CORE-RTR1	0			ISIS	10.150.30.2/32
Hop 5	SF-CORE-RTR1	SF-CORE-RTR1.02	10			ISIS	10.150.30.2/32
Hop 6	SF-CORE-RTR1.02	ROUTER11	0			ISIS	10.150.30.2/32
Hop 7	ROUTER11	ROUTER11.05	10			ISIS	10.150.30.2/32
Hop 8	ROUTER11.05	DC-CORE1-ROUTER3	0			ISIS	10.150.30.2/32
Hop 9	DC-CORE1-ROUTER3	DC-CORE2-ROUTER4.03	10			ISIS	10.150.30.2/32
Hop 10	DC-CORE2-ROUTER4.03	DC-CORE2-ROUTER4	0			ISIS	10.150.30.2/32
Hop 11	DC-CORE2-ROUTER4	DC-PE2-ROUTER9.01	10			ISIS	10.150.30.2/32
Hop 12	DC-PE2-ROUTER9.01	10.150.11.1	0			ISIS	10.150.30.2/32
Hop 13	10.150.11.1	10.150.12.2	1			ISIS	10.150.30.2/32
Hop 14	10.150.12.2	10.150.16.2	1			ISIS	10.150.30.2/32
Hop 15	10.150.16.2	10.150.16.1	1			ISIS	10.150.30.2/32
Hop 16	10.150.16.1	10.150.17.1	1			ISIS	10.150.30.2/32
Hop 17	10.150.17.1	10.150.18.1	1			ISIS	10.150.30.2/32
Hop 18	10.150.18.1	10.150.19.1	1			ISIS	10.150.30.2/32
Hop 19	10.150.19.1	10.150.23.1	1			ISIS	10.150.30.2/32
Hop 20	10.150.23.1	10.150.27.1	1			ISIS	10.150.30.2/32
Hop 21	10.150.27.1	10.150.27.1	0			ISIS	10.150.30.2/32
Path 2	Core-Router14	10.150.27.1	68				
Path 3	Core-Router14	10.150.27.1	68				
Path 4	Core-Router14	10.150.27.1	68				
Path 5	Core-Router14	10.150.27.1	68				
Path 6	Core-Router14	10.150.27.1	68				
Path 7	Core-Router14	10.150.27.1	68				
Path 8	Core-Router14	10.150.27.1	68				
Path 9	Core-Router14	10.150.27.1	68				
Path 10	Core-Router14	10.150.27.1	68				
Path 11	Core-Router14	10.150.27.1	68				
Path 12	Core-Router14	10.150.27.1	68				
Path 13	Core-Router14	10.150.27.1	68				
Path 14	Core-Router14	10.150.27.1	68				
Path 15	Core-Router14	10.150.27.1	68				
Path 16	Core-Router14	10.150.27.1	68				
Path 17	Core-Router14	10.150.27.1	68				
Path 18	Core-Router14	10.150.27.1	68				
Path 19	Core-Router14	10.150.27.1	68				
Path 20	Core-Router14	10.150.27.1	68				
Path 21	Core-Router14	10.150.27.1	68				
Path 22	Core-Router14	10.150.27.1	68				
Path 23	Core-Router14	10.150.27.1	68				
Path 24	Core-Router14	10.150.27.1	68				

1 top level entry, 2311 total entries

Cost of path from Core-Router14 to 10.150.30.2/32: 68

Figure 55 Highlighted Path Details for EIGRP

Because 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 *Find or List Paths* window and in the status bar of the *Routing Topology Map* 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.

Diagnosing EIGRP Topology Errors

Topology Diagnostics are available EIGRP topologies only. They allow you to study problems found in the network configuration or in the topology modeling.

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **Topology Diagnostics** and select one of the following options:
 - **List Topology Errors**—Open a list of messages describing anomalies that were discovered during exploration of the EIGRP topology. Click an entry in the list to highlight the affected routers and links. See [List Topology Errors](#) on page 122.
 - **List Inaccessible Routers**—Open a list of routers that were not accessible through Telnet during exploration of the EIGRP topology, including a reason such as authentication failure. Click an entry in the list to highlight the last accessible router on the path toward the inaccessible router. Inaccessible routers are not shown on the topology map. They can cause incorrect routes to appear and reduce the ability of t to track changes in the network topology. See [List Inaccessible Routers](#) on page 123.
 - **List Mismatched Distances**—Open a list of prefixes for which the distance to the prefix reported by a router that peers with the appliance does not match the distance that the system calculates across its model of the topology. This list also shows when the periodic topology explorations start and end, along with summary statistics. See [List Mismatched Distances](#) on page 125.
 - **Find Invisible Links**—Run a simulation on the topology model to determine if there are any links where a failure will not be immediately detected because the routers that peer with the system will not report an EIGRP distance change. The simulation can take several hours to run on a large network topology. You can cancel it at any time. See [Find Invisible Links](#) on page 128.

List Topology Errors

The Route Recorder detects 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 and shown in the List of Topology Errors report. The report shows only the anomalies that were detected since the start of the last full exploration. These anomalies can indicate router configuration errors that should be corrected.

Figure 56 shows an example of the List of Topology Errors report.

Time	Message	AS
2006-06-12 12:00:21	Duplicate interface address 10.148.148.1 on 192.168.109.11 and 24.0.0.23	Lab58.EIGRP/AS1
2006-06-12 12:00:21	2 duplicate interface addresses 192.168.118.23 ... on 24.0.0.23 and 24.0.0.23	Lab58.EIGRP/AS1
2006-06-12 12:00:46	Duplicate interface address 10.115.115.1 on 198.99.99.1 and 24.0.0.23	Lab58.EIGRP/AS1

3 entries

Figure 56 List of Topology Errors Report

The report contains the following columns:

- **Time**—the time when the anomaly was detected.
- **Message**—a description of the problem. The following anomalies are included:
 - **Interface mask length mismatch**—Indicates that the address mask length is not the same for the interfaces on the two ends of a link.
 - **Duplicate router ID**—Indicates that 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**—Indicates that the router ID on one router is the same as an interface address on another router. Because the router ID is normally derived from an interface address on the router and interface addresses are normally unique to one router, this is an anomaly.
 - **Duplicate interface address**—Indicates that 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**—Indicates that the prefix is configured for redistribution but the metric has not been configured. Applies to the case where an external prefix is advertised by a router but is unreachable from that router.
- **Variance not supported by the system**—Indicates that the router is configured for equal-cost multi-path routing with a variance value other than one. Only the paths with the lowest metric are included.
- **Router ID unroutable in this AS**—Indicates that the router ID of the indicated router is not an address within any routable prefix in the AS. If the router-to-router path highlighting function is used with this router as the destination, the path will be incomplete.
- **Prefix with delay of 0**—Indicates that 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**—Indicates that the Route Recorder can discover a routing loop 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 show 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 the peer routers to that prefix.
- **AS**—Includes the AS where the anomaly was detected, for topologies with multiple ASs.

Clicking the table row for an error message highlights the associated routers and links, assuming that those objects are present in the topology at the current time. The *History Navigator* window 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.

List Inaccessible Routers

During the EIGRP topology exploration, the system 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, the system cannot include that router in the topology, nor can it learn about other routers connected beyond that router. If a path between two

accessible routers passes through an inaccessible router, the system will not be able to find that path. It is important to fix router accessibility problems so that the topology is correct.

Figure 57 shows an example of the List of Inaccessible Routers report.

Time	Inaccessible Router	Last Accessible Router on Path	First-Hop Gateway	Reason	AS
2006-06-12 12:00:10	192.168.116.19	54.23.1.1	192.168.118.17	Authentication failure	Lab58 EIGRP/AS1
2006-06-12 12:07:22	10.115.115.2	24.0.0.23	192.168.118.17	Connection timeout	Lab58 EIGRP/AS1

Figure 57 List of Inaccessible Routers Report

The report contains the following columns:

- **Time**—Indicates the time when the problem was detected.
- **Inaccessible Router**—Identifies the inaccessible router
- **Last Accessible Router On Path**—Indicates the address of the last router on the path to the inaccessible one. Clicking on the entry in this column highlights that router on the topology map.
- **First-Hop Gateway**—Indicates the gateway (first-hop router) used in attempting the connection if the solution is to specify a different default gateway
- **Reason**—Indicates a possible reason for failure to access the router:
 - **Authentication failure**—Occurs if the router does not accept the login password or user name/password configured in for the AS.
 - **Invalid input (unauthorized command?)**—Occurs if the TACACS account used by the system 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?)**—Occurs if too many other Telnet sessions are open at the time the system attempts its connection. No free virtual terminal is available on the router, and the connection is refused. The system attempts several connections with exponentially increasing delay. This error can also occur if the connection is blocked by a firewall or other appliance.

- **Connection timeout**—Indicates that the router is unreachable and timed out, for example, if the path to the router hits a black hole.
- **Telnet open failed**—Presents additional details, if provided by Telnet.
- **CLI parsing error**—Indicates that the output of the commands issued to the router in a query was not formatted as expected. Report this problem to technical support.
- **Problem in recorder**—Indicates that the system was unable to issue the query for some reason. Please report this problem to technical support.
- **AS**—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 Mismatched Distances

The List of Mismatched Distances report lists the prefixes whose reported distance (or metric) between the prefix and a peer does not match the calculated distance. When the system calculates metrics across the topology model, those metric values are compared to the metrics reported by appliance peers. If the distance does not match, the prefixes are listed in the List of Mismatched Distances report.

Route Recorder compares these distances at the end of each full topology exploration to provide a measure of the accuracy of the topology model. Ideally, this report 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 report is shown in [Figure 58](#).

Time	Source	Destination	Router's Metric (bw+dfly)	Model's Metric (bw+dfly)	Reason / Message	AS
2006-06-12 04:11:40	192.168.118.23	10.127.1.0/24	256000+2760	0+4261412865	Unreachable router 192.168.118.23 hides a	Lab58.EIGRP
2006-06-12 12:00:02					Start of periodic topology exploration	Lab58.EIGRP
2006-06-12 04:00:02					Start of full topology exploration	Lab58.EIGRP
2006-06-12 04:11:04	192.168.118.18	192.168.133.0/30	1666560+4294967295	1666560+4262462465	Prefix 192.168.133.0/30 not converged at 1	Lab58.EIGRP
2006-06-12 04:11:19	192.168.118.18	24.0.0.12/32	0+4294967295	256000+28160	Path to internal prefix hidden by external a	Lab58.EIGRP
2006-06-12 04:11:24	192.168.118.18	192.168.101.0/24	0+4294967295	256000+28160	Path to internal prefix hidden by external a	Lab58.EIGRP
2006-06-12 04:11:28	192.168.118.18	13.13.13.0/24	0+4294967295	256000+28160	Path to internal prefix hidden by external a	Lab58.EIGRP
2006-06-12 04:11:35	192.168.118.18	15.15.15.1/32	0+4294967295	256000+28160	Path to internal prefix hidden by external a	Lab58.EIGRP
2006-06-12 04:11:39	192.168.118.18	144.144.144.0/24	0+4294967295	256000+28160	Path to internal prefix hidden by external a	Lab58.EIGRP
2006-06-12 04:11:42	192.168.118.18	192.168.104.0/24	0+4294967295	256000+28160	Path to internal prefix hidden by external a	Lab58.EIGRP
2006-06-12 04:11:45	192.168.118.18	192.168.0.0/24	0+4294967295	256000+28160	Path to internal prefix hidden by external a	Lab58.EIGRP
2006-06-12 04:11:47	192.168.118.18	10.10.0.0/16	0+4294967295	256000+4261441025	Path to internal prefix hidden by external a	Lab58.EIGRP
2006-06-12 04:11:08	192.168.118.23	24.1.7.0/24	25600+130810	0+4261412865	Model and router behavior don't match	Lab58.EIGRP
2006-06-12 04:11:09	192.168.118.23	10.0.106.4/30	256000+2760	0+4261412865	Model and router behavior don't match	Lab58.EIGRP
2006-06-12 04:11:11	192.168.118.23	196.99.99.0/24	256000+2760	0+4261412865	Model and router behavior don't match	Lab58.EIGRP
2006-06-12 04:11:11	192.168.118.23	26.0.0.0/8	1280000+130810	0+4261412865	Model and router behavior don't match	Lab58.EIGRP
2006-06-12 04:11:13	192.168.118.23	192.168.244.0/24	256000+2760	0+4261412865	Model and router behavior don't match	Lab58.EIGRP
2006-06-12 04:11:14	192.168.118.23	25.0.0.4/32	256000+2760	0+4261412865	Model and router behavior don't match	Lab58.EIGRP
2006-06-12 04:11:15	192.168.118.23	24.1.9.0/24	25600+130810	0+4261412865	Model and router behavior don't match	Lab58.EIGRP

210 entries

Figure 58 List Mismatched Distances Report

The report contains the following columns:

- **Time**—Indicates the time when the anomaly was detected.
- **Source**—Indicates the source IP address involved in the mismatched distance.
- **Destination**—Indicates the source IP address involved in the mismatched distance.
- **Router's Metric**—Indicates the metric for highlighted path cost. See [Viewing the Highlighted Path Cost for EIGRP](#) on page 118 for more information.
- **Model's Metric**—Indicates the metric for the topology model. See [Viewing the Highlighted Path Cost for EIGRP](#) on page 118 for more information.
- **Reason/Message**—Indicates the reason that the mismatch may have occurred:
 - **Unreachable router hides actual path**—Indicates that the path goes through a router that the system cannot access. The actual links traversed and their metrics are unknown.
 - **Different equal-cost path chosen by model**—Indicates that a different path with equal cost was taken. If there are multiple paths whose total costs are equal, but which have different bandwidth and

delay components of the metric, then the system might choose a different path than the routers actually use. The algorithm of the router is not always deterministic.

- **Prefix not converged**—Indicates that the system has traced the actual path taken by the routers, and that one of the routers has no route to the prefix in question. This condition usually indicates that EIGRP routing to the prefix has not converged so the distance of the peer router is not valid.
- **Network has routing loop**—Indicates that the system encountered a routing loop when attempting to trace the actual path taken by the routers. This means EIGRP routing to the prefix has not converged and the distance given by the peer router is not valid.
- **Model and router behavior do not match**—Indicates that the system modeling of recorder behavior is not exact. This message may also indicate that a router has become confused and reports inconsistent metric information (perhaps due to a bug in the router software). Some router configuration changes, such as changing an access control list (ACL) used in a route filter, do not take effect until the routing process is restarted. The system will see the new value but the router will not be using it, causing a distance mismatch. Report this message to technical support if it persists across multiple full explorations.
- **Failed to query**—Indicates a possible bug. Report this problem to technical support.

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

The system 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 or due to limitations in tracking network dynamics. The period is set as part of 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* window describing the number of links and prefix attachments that were corrected during the last periodic topology exploration. Ideally, these numbers should 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, the system 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 the system will not report an EIGRP distance change. During the simulation, the system 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, the system will be able to detect a failure of the real interface. If not, the system can only detect the interface failure during the next periodic topology exploration (the default is 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 coverage.

The simulation can take several hours to run on a large network topology, but it can be canceled at any time by clicking **Cancel**. 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 **Reload** in the *Invisible EIGRP Interfaces* window to re-run the simulation.

You can highlight invisible links in yellow on the topology map by clicking **Highlight**.

Assigning AS Names

The AS Name feature allows you to assign a name to the AS. This name will take priority over the AS name received from the Whois server. You have the option of keeping the Whois server name as the assigned AS name, or you can enter a new name.

To access the AS Name feature, perform the following steps:

- 1 Open the client application.
- 2 Choose **Administration** → **AS Names**.

The AS Names window opens ([Figure 59](#)).

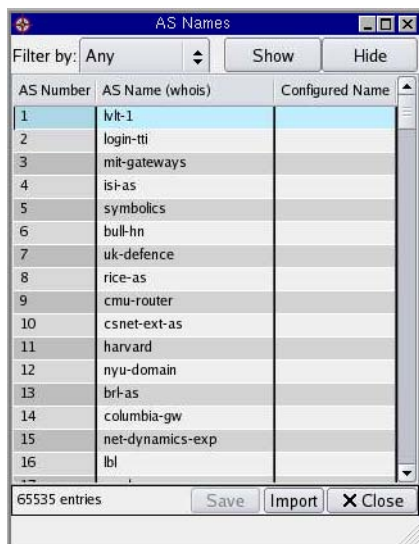


Figure 59 AS Names Window

This window includes the following columns:

- **AS Number**—Provides the number identifying the AS number.
- **AS Name**—Provides the name of the AS derived from the Whois server. (lowest priority)
- **Configured Name**—Enter a unique AS name in this column. (highest priority)

You can use the following filter options and buttons on this page:

- **Filter By**—Choose which AS name and number entries you want to show and/or hide in the table with the following choices:
 - **Any**—Selecting this shows all rows.
 - **AS Number**—Selecting this choice shows a drop-down list, which allows you to filter by entering the AS Number, while also showing previously used AS Numbers. Simultaneously, an **Options** drop-down list also opens, which allows you to filter with the following choices:
 - Greater Than:** Provides AS numbers with a greater number than the one entered in the text field.
 - Exact Match:** Provides only exact matches typed in the text field.

Begins With: Provides matches that begin with numbers entered in the text field.

- **AS Names**—Select this choice and a text field opens where you can enter AS names. Simultaneously, an **Options** drop-down list also appears, allowing you to filter with the following choices:

Substring: Filters the AS Names with the given string as a substring for its name.

Exact Match: Filters the AS names with the given string as an exact match of its name.

Begins With: Filters the AS names with the beginning string used for the AS name.

- **Show**—Select this to show all AS name entries that you want listed.
- **Hide**—Select this to hide router entries.
- **Save**—Select this to save information you edit. This button is active only when you have edited information on the screen.
- **Import**—Select this when you want to edit several AS names.
- **Close**—Select this to exit the AS Names window.

To change the AS name, perform the following steps, perform the following steps:

- 1 Select **Tools** → **AS Name**.
The AS Names window opens.
- 2 Select the row of the AS name you want to change.
- 3 Enter the new AS name in the Configured Name field.
- 4 Click **Save**.

To change the name of multiple AS names, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Tools** → **AS Name**.
- 3 Click **Import**.

The *Import AS Names* dialog box opens, as shown in [Figure 60](#).

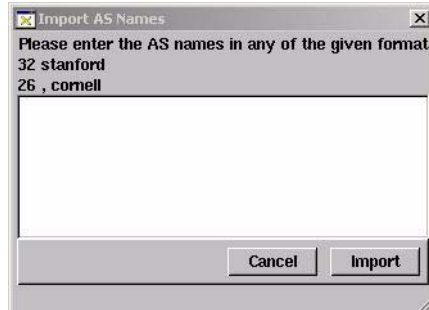


Figure 60 Import AS Names

- 4 Type the names of the ASs you want to rename in the format.
- 5 Click **Import**.

The new AS names now appear in the Configured Name column.

Assign and Verify BGP AS Assignments to Routers

The system can show the path resolved between two points in a network, as described in the next section. For network configurations that include BGP, correct BGP AS assignments to routers are required 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, The system 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 AS for Routers* window.

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, the system 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 Open the client application and choose your database to open the routing topology map.

- 2 Choose **Administration** → **Assign BGP AS to Routers** to open the *BGP AS for Routers* window as shown in [Figure 61](#). Some routers may have AS numbers already assigned to them as detected by BGP peering or computed from network topology.
- 3 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.
- 4 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.
- 5 Click **Assign**.
- 6 Repeat Steps 3-5 to manually assign other routers.
- 7 Click **Save User Input**.
- 8 Click **Close**.



Figure 61 BGP AS to Routers

4 The History Navigator

This chapter describes how to use the History Navigator to analyze the detailed routing history of the network.

Chapter contents:

- [Understanding the History Navigator](#) on page 134
- [Accessing the History Navigator](#) on page 135
- [Working With the History Navigator](#) on page 136
- [Analyzing Historical Data](#) on page 143
- [Understanding the Events List](#) on page 177
- [Using the History Navigator as a Forensic Tool](#) on page 187
- [Correlating Time Series Data](#) on page 193
- [Using Filters](#) on page 195

Understanding the History Navigator

The History Navigator allows you to display the detailed routing history of a network. The Route Recorder obtains the routing history by monitoring the routing protocols and recording all protocol events in a database.

Every ten minutes the Route Recorder saves a complete, time-stamped snapshot of the routing topology. During each interval between snapshots, all routing announcements are recorded with timestamps. This data enables the system to display a precise routing map of the network at any point in time.

The History Navigator includes numerous options for viewing and analyzing the recorded data:

- View summaries of recorded data in graphical format to understand changes in vital network statistics over time.
- View the number of events between snapshots.
- For each snapshot, view the number of routers, routing adjacencies, and prefixes.
- Display detailed lists of routing events for a specified time period to aid in diagnosing a network outage or performing forensic analysis after an outage.
- 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.
- View a real-time graph of events as they occur.
- 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.
- Perform a before-and-after comparison of the state of the network at different times.

Accessing the History Navigator

You can access the History Navigator from the client application.

To access the History Navigator, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator**.

The History Navigator window opens to show a graph of recorded network routing events ([Figure 62](#)).

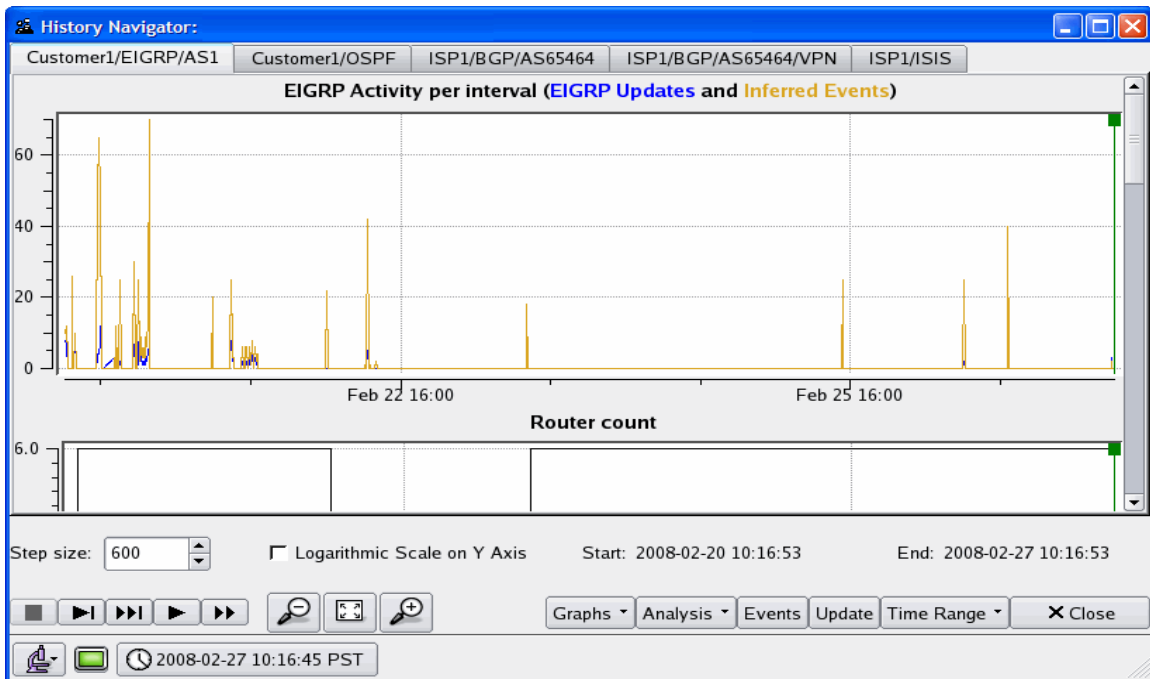


Figure 62 History Navigator Window (Analysis Mode)

- 2 Perform operations as described in the next section, [Working With the History Navigator](#) on page 136.

Working With the History Navigator

This section describes the options available for working with the History Navigator:

- [History Navigator Controls](#) on page 136
- [History Graphs](#) on page 141



If a database contains multiple protocols, the History Navigator window displays multiple tabs, one for each protocol. As in the example shown in [Figure 62](#), a database containing BGP, EIGRP, and OSPF protocols has tabs for BGP, EIGRP, and OSPF.

History Navigator Controls

The History Navigator window controls allow you to navigate through the routing database and customize the presentation of data. The controls are available in the main History Navigator window (see [Accessing the History Navigator](#) on page 135).

Modes

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

The following modes are available in the History Navigator window:

Monitoring 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. Traffic data is not displayed in this mode. In this mode, the History Navigator window displays routing events as they occur. In RAMS, traffic events are delayed by 30 minutes in real time.

Analysis 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.

Planning mode—A network icon indicates that planning features are enabled for the topology map.

The controls for the window in Monitoring mode are the same as those present when the window is in Analysis mode or Planning mode. However, options that do not apply in Monitoring mode and Planning mode are disabled, such as playback controls.

To switch modes in the History Navigator, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Reports** → **History Navigator** to open the main History Navigator window.
- 3 Click the mode icon in the lower left corner of the window and choose the desired mode.

This has the effect of changing the Time Range shown on the graph from Online to One Week (see [Buttons](#) on page 138 for information about the values that can be set with the Time Range button).



When switching from Analysis to Monitoring mode, a pop-up box will open, alerting you that if the amount of events exceeds a certain threshold, the analysis of the events could take a few minutes. You can restart Monitoring mode without this analysis, however the event history graph will show no data for that period.

Status Bar

The tool bar at the bottom of the History Navigator window is the same as the status bar on the Topology Map window. See [Main Window Toolbar](#) on page 49 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:

- Use the mouse to drag the cursor to a different point on the time line. The routing topology map immediately displays the routing topology as it existed at that time. Note that in RAMS Traffic, traffic data is delayed by 30 minutes.
- Right-click on a point in the time line. A pop-up asks whether you want to move time to that point. Click **Yes**. The topology map immediately displays the routing topology as it existed at that time. If the time is within the last 30 minutes, traffic data is not displayed in RAMS Traffic.
- Move the cursor through time by stepping or animating (automated stepping) using the playback controls as described in [Playback Controls](#) on page 139. Any paths highlighted on the routing topology map are recomputed and redisplayed at each step of the replay.



The routing topology database does not store nodes and links that are down; therefore, objects that are down when the topology is first opened are not 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 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](#) on page 74 for information about node/link timeout intervals).

Buttons

Use the panel of buttons in the lower right-hand corner of the window to access graphs, data analysis tools, and events lists, and to specify the time range for display:

- **Graphs**—Choose which graphs are displayed. See [History Graphs](#) on page 141 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.
- **Analysis**—Choose from a list of data analysis tools. See [Analyzing Historical Data](#) on page 143 for information about these tools.
- **Events**—Display a detailed list of routing events. See [Understanding the Events List](#) on page 177 for information about the Events list.
- **Update**—Update the display. This button is enabled only 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.
- **Time Range**—Choose the data range to include in the History Navigator window. By default, the time range is set to **Online** when in Monitoring mode and to **One Week** when in Analysis mode. You can set the time range to one hour, one day, one week, or one month. In RAMS Traffic, traffic data does not appear in Monitoring mode and is delayed by 30 minutes in all other modes.
- **Close** button—Close 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:



Stop—Stops animated playback. This button is enabled only in animated playback mode.



Step—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.



Fast Step—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.



Animate—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 **Stop** to stop the animated playback.



Fast Animate—Starts animated playback in fast mode, automatically advancing the cursor by 10 times the number of seconds specified in the Step size text box. Click **Stop** to stop the animated playback.



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 [Understanding the Events List](#) on page 177, includes all routing changes.

Logarithmic Units

To display the Y axis of the graph in logarithmic units, select the **Logarithmic Scale on Y Axis** check box. The graph is redisplayed with logarithmic Y values.

Zooming the Time Line

You can 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.



The zoom buttons zoom only the values on the X axis.

The panel of buttons toward the bottom center of the screen control zooming functions. From left to right, the buttons are:



The **Zoom In** button allows you to zoom into a subsection of the History Navigator graph.



The **Zoom Out** button allows you to zoom out of a subsection of the History Navigator graph



The **Reset Zoom** button resets the view back to the standard viewer setting.

To zoom the time line, perform the following steps:

- 1 While holding the **Ctrl** key down, right-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.

History Graphs

The primary feature of the History Navigator window is the Events graph that is shown in the default window. Several additional graphs can be selected to show a wide range of statistics about the state of the network.



In RAMS, open the Traffic tab to display additional traffic-related graphs.

To access history graphs, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Click **Graphs**, and then choose the desired graph.



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

The following graphs may be available, depending upon the selected protocol:

- **Routers**—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**—Displays the number of routes advertised in the network. This graph does not appear if the topology currently selected in the History Navigator window is an IGP area or AS.

- **Links**—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 is a BGP AS.
- **Prefixes**—Displays the number of prefixes available in the entire network.
- **BGP Updates**—Displays the number of how many announced and withdrawn packets received in the preceding 10 minutes. Announced packets are represented by blue lines and re-announced packets are represented in dark yellow lines.
- **ISIS Activity**—Displays LSP activity for ISIS domains. New activity displays in blue, refreshed activity displays in dark yellow. (option is shown only for ISIS)
- **ES Neighbors**—Displays activity between the router and end systems and routers.
- **Prefix Neighbors**—Displays activity between neighboring routers.
- **OSPF Activity**—Displays LSA activity for OSPF domains. New activity displays in blue, refreshed activity displays in dark yellow.
- **EIGRP Activity**—Displays updated and inferred activity for EIGRP domains. New activity displays in blue, refreshed activity displays in dark yellow.
- **Events**—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.
- **Interfaces**—Displays the number of interfaces discovered by static protocol.

You can configure the system to include any or all of the graphs in the default window. See [Applying Configuration Options](#) on page 67 for more information.



In Monitoring mode, the update interval is refreshed every 10 seconds, by default. In Analysis mode, the update interval is every 600 seconds, by default.

Analyzing Historical Data

The History Navigator supports the following tools for detailed analysis of historical data:

- [Root Cause Analysis](#) on page 143
- [RIB Visualization](#) on page 151
- [RIB Comparison](#) on page 165
- [Trending](#) on page 169
- [Event Analysis](#) on page 171
- [Flow Record Browser](#) on page 175

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.



Traffic data in RAMS Traffic is not relevant for this type of analysis, and that loading traffic information from the database may slow the analysis process. When you open a topology for BGP-specific analysis, it is recommended that you deselect any traffic databases from the tree in the Open Topology dialog box as described in [Chapter 3, “The Routing Topology Map”](#)

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

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Use one of these options to open the root cause analysis window:
 - Choose **Reports** → **History Navigator** to open the main History Navigator window. Choose **Analysis** → **Root Cause Analysis**.
 - If your topology has BGP data, choose **Reports** → **Root Cause Analysis**.



You cannot perform root cause analysis if more than one BGP database is open.

- 3 Left-click in the graph just before the events occurred.
- 4 Left-click in the graph just after the events occurred.
- 5 (Optional) If you have more than 500k events, a window prompts you to **Continue**, **Abort**, or **Prefilter** the events.
- 6 (Optional) If you select **Prefilter**, the Event Prefiltering window opens. From here, you can select from a list of filters from the drop-down menu, decreasing the time it takes to generate the event list. For more information on using filters, see [Using Filters](#) on page 195.

If no significant incidents occurred during the time you specify, a message indicates that the Root Cause Analysis algorithm did not find any major BGP problems. Adjusting the analysis options as described in [Chapter 3, “The Routing Topology Map,”](#) may increase the number of incidents the algorithm will find.

If incidents are found, the Root Cause Analysis Results window opens. [Figure 63](#) shows an example.

Description	View Details
Recording restarts First event: 2006-04-05 11:21:38 Last event: 2006-04-13 21:50:43 Time elapsed: 202 h 29 m 5 s	Animation 296 Events 26 Prefixes
Router 24.0.0.3 has re-established peerings First event: 2006-04-05 11:25:12 Last event: 2006-04-14 03:58:38 Time elapsed: 208 h 33 m 26 s	Animation 73481 Events 18 Prefixes
Peering to 24.0.0.5 has flapped First event: 2006-04-05 11:25:20 Last event: 2006-04-14 03:58:55 Time elapsed: 208 h 33 m 35 s	Animation 14664 Events 1 Prefixes
Peering to 24.0.0.12 has flapped First event: 2006-04-06 15:43:15 Last event: 2006-04-14 03:58:36 Time elapsed: 180 h 15 m 21 s	Animation 40485 Events 8 Prefixes
Peering to 24.0.0.16 has flapped First event: 2006-04-12 13:32:16 Last event: 2006-04-14 03:57:44 Time elapsed: 36 h 25 m 28 s	Animation 4640 Events 1 Prefixes
5 entries	

Figure 63 Root Cause Analysis Results

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. For each group, the inferred root cause will be one of the following:

- **Prefixes shifted**—When the event messages of a group indicate that prefixes have shifted, the number of prefixes that have shifted on a specified link is listed. “Shifted” refers to the total number of prefixes that have either left or joined the link. The count is approximated because the same prefixes may join and leave the link more than once, or different prefixes may be joining and leaving. Therefore, the system calculates a maximum shift size or change in count. For example, if 2 prefixes left and 3 prefixes joined, the maximum shift size is 4. The total number of prefixes to traverse the link is at least 4, but can be any number between 4 and 9, hence the approximation.
- **Prefixes are flapping**—When the event message of a group indicates that prefixes are flapping, the prefixes are being announced and withdrawn, possibly over and over. The corresponding message takes one of two forms:
 - 192.168.103.0/24 is flapping on 128.32.0.66 > 11423.calre_2
In this case, one prefix (192.168.103.0/24) is flapping on the specified link (128.32.0.66 > ...).
 - 3435 prefixes are flapping on 128.32.0.66 > 11423.calre_2
In this case, 3435 prefixes are flapping on the specified link (128.32.0.66 > ...).
- **Peering established** — Each time the system establishes a BGP peering, the peer router sends all of its BGP routes. At the end of this sequence, the system writes a synchronized event.
- **Peering lost**—When a peering is lost, the connection between the system and the peer router has closed. The Animation window will continue to show the effect of associated prefix withdrawals, but the withdrawn prefixes are not listed in the Prefixes table.
- **Peering has flapped**—When a peering is both established and lost, the peering has flapped. If the peer router has several established and lost events during the selected interval, all of these events are combined into a single incident.

- **Router has lost peerings**—When the system loses its connection to a peer router, it may detect that other routers have also lost contact with the peer. As a result, the system infers that the router has lost peerings. This message might indicate, for example, that the router is rebooting.
- **Router has established peerings, or re-established peerings**—When a peering is established, all prefixes are added at once, which creates an artificial spike in activity.
- **Recording stopped, started, or restarted**—Recorders write to the database when they start recording and when they shut down. Any peerings that are established within five minutes of the start of recording are included in this event message. Multiple stops, starts, and restarts within the selected interval are combined into a single event.

To the right of each group of event messages 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

The routes of a BGP router 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 system appears at the left side of the tree. The time range of the animation is indicated in the rectangle. To the right of the rectangle are its BGP peers; to their right are its BGP next hops; to their right are the AS the next hops serve; to the right of each AS is the downstream AS, if any; to the right of the downstream AS are the prefixes it advertises.

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 64 shows an example of the Animation window.

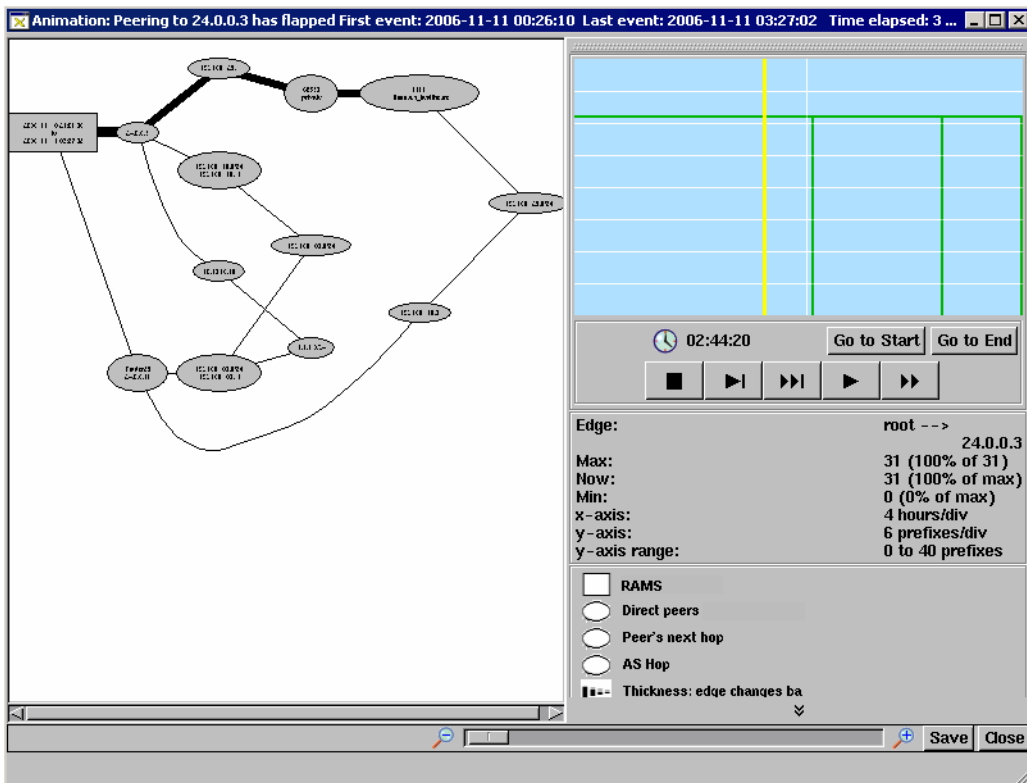


Figure 64 Animation Window

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.

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 139).

- **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 left 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 gray 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 Open the client application and choose your database to open the routing topology map.

- 2 Choose **Reports** → **History Navigator** to open the main History Navigator window.
- 3 Choose a time period (see [Cursor](#) on page 138).
- 4 Choose a playback option (see [Figure 65](#)):

- 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 10 steps.
- 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.
- Stop  halts the playback of an animation.

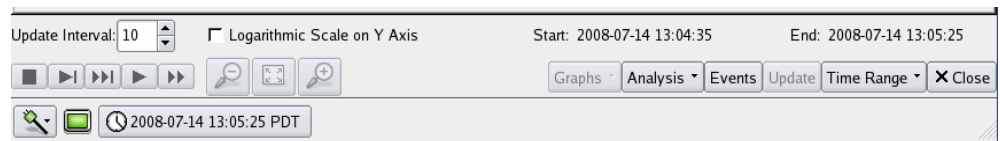


Figure 65 Playback Controls

- 5 Click the corresponding playback button to begin the animation.



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

Saving an Animation

You can save an animation for later viewing by clicking Save in the lower right corner of the Animation window. The animation is saved in Scalable Vector Graphic (SVG) format (file extension .svg) on the appliance 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 which can be downloaded from <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 may require more CPU usage than the Adobe viewer.

To view a saved animation, perform the following steps:

- 1 Open the web application on a Route Recorder and choose **Home**.



Administrator privileges are not required to view a saved animation.

- 2 Choose **Reports Portal** on the top navigation bar.
- 3 Click **BGP Animations** on the left navigation bar.

The BGP Animations page displays a list of all saved SVG files, and contains a link to the installation page for the Adobe plug-in.

- 4 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 window cursor position. Visualizations can help you identify difficult-to-diagnose problems such as prefix load-balancing issues.

Generating a Visualization

To generate a RIB visualization, perform the following steps:

- 1 Open the client application.
- 2 Use one of these options to open the RIB visualization window:
 - Choose **Reports** → **History Navigator** to open the main History Navigator window. Move the History Navigator cursor to the time desired, and choose **Analysis** → **RIB Visualization**.
 - If your topology has BGP data, choose **Reports** → **RIB Visualization**.

The RIB Visualization window opens, as shown in [Figure 67](#).



You cannot perform RIB visualization if more than one BGP database is open.

The routes of a BGP router 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 appliance appears at the left side of the tree. The appliance 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. You can create visualizations filtered to include only a subset of the routes from the RIB Browser as described on [page 162](#).

To the right of the rectangle are its BGP Peers, followed by its BGP next hops; to their right are the ASs that the next hops 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.

The bottom of this screen has a zoom slider which allows you to zoom in on any portion of the window by moving the zoom slider to the right. You can also pan across the screen by holding down the space bar while left-clicking on the mouse.

Changing RIB Visualization Thresholds

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 following entities are included on the Options panel of the RIB Visualization window:

- **Show a Peer.** The default is to include a peer if it announces 5% or more of the total number of prefixes.
- **Show a Nexthop.** The default is to include a nexthop if it announces 5% or more of the total number of prefixes.

- **Show a Neighbor AS.** The default is to include the neighbor AS if it announces 5% or more of the total number of prefixes.
- **Show a Non-Nighbor AS.** The default is to include the non-neighbor AS if it announces 5% or more of the total number of prefixes.
- **Show an Edge to a Prefix.** Select **Always** to show an ellipse for the prefix on the visualization and connect that ellipse to the other elements. For example, [Figure 66](#) shows a visualization without the **Never Show an Edge to a Prefix** option selected. [Figure 67](#) shows the same visualization with **Always** option selected.

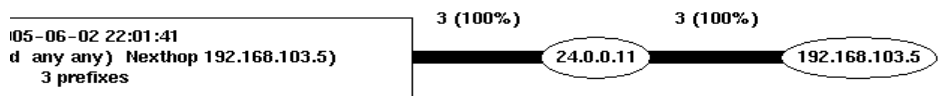


Figure 66 RIB Visualization without Show an Edge to a Prefix Option

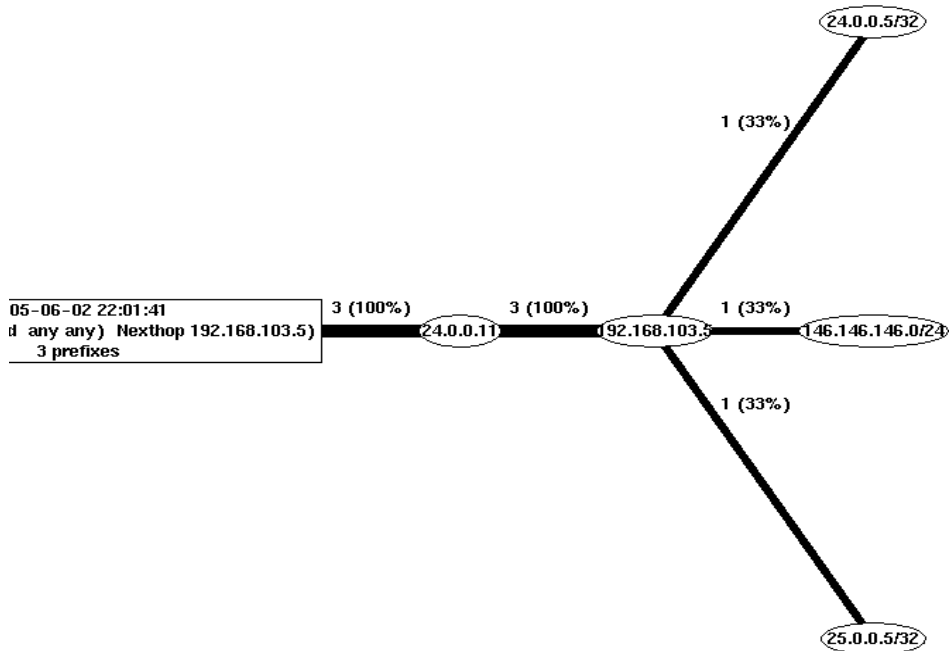


Figure 67 RIB Visualization with Show an Edge to a Prefix Option

To change RIB visualization thresholds, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Move the History Navigator cursor to the time desired.
- 3 Choose **Analysis** → **RIB Visualization**.
- 4 Click **Options**.

The Visualization options are displayed in the left pane of the window.

- 5 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.



If choosing one of the Always options would create a visualization too big or crowded to read, that option is disabled.

- 6 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 Visualization window. The visualization is saved in SVG format (file extension `.svg`) on the 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 150 for available plug-ins.

To view a saved visualization, perform the following steps:

- 1 Open the web application on a Route Recorder and choose **Home**.



Administrator privileges are not required to view a saved animation.

- 2 Choose **Reports Portal** on the top navigation bar.
- 3 Click **BGP Animations** on the left navigation bar.

The BGP Animations page displays a list of all saved SVG files, and contains a link to the installation page for the Adobe plug-in.

- 4 Click the title of the visualization you wish to view to open a window for that visualization. All of the information and controls present in the original animation are available in the saved animation.

RIB Browser

Use the Routing Information Base (RIB) Browser to display the following types of information:

- For IGP, links and prefixes that are currently down.
- For BGP, distribution of routes based on attributes such as Peer, Nexthop, MED, and so on.
- For OSI ISIS, in addition to the fields displayed for IGP, additional fields are available if the OSI network is present.

To open the RIB browser, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Move the History Navigator cursor to the time desired.
- 3 Choose **Analysis** → **RIB Browser**.

The RIB browser opens (Figure 68).

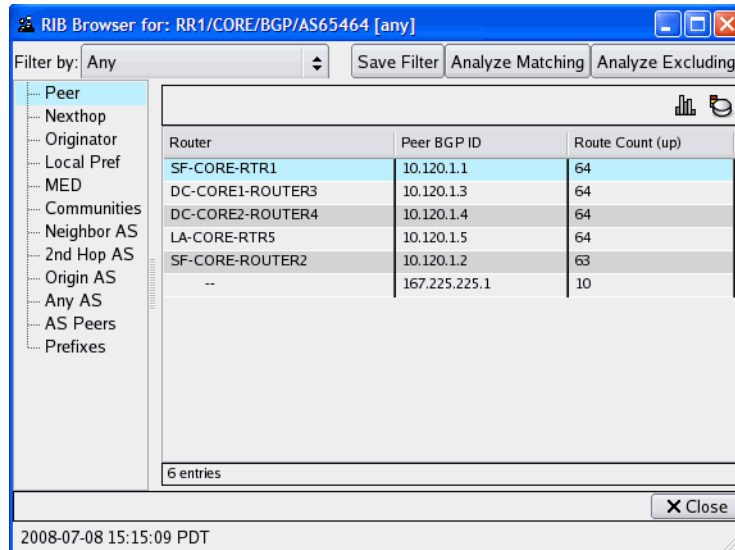

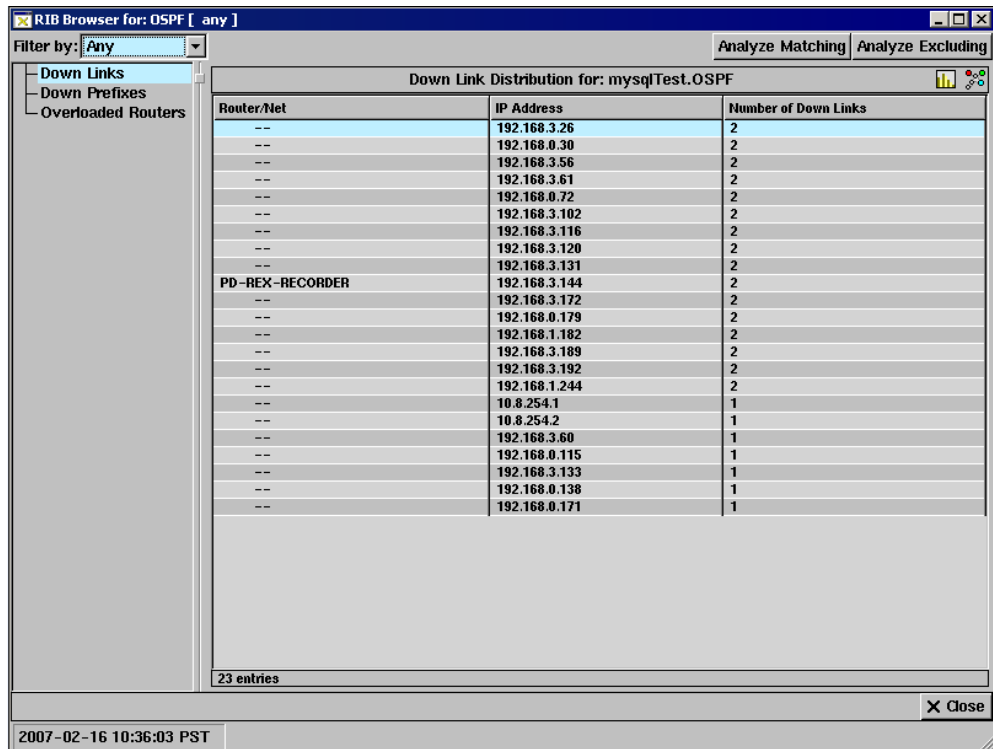


Figure 68 RIB Browser

IGP Protocols

For IGP protocols, the RIB Browser displays a list of links and prefixes that are currently down at the bottom of the History Navigator window. [Figure 69](#) shows an example of the RIB browser with IGP link data.


On the left side of the RIB browser, click **Down Links** or **Down Prefixes** to view the list of links or prefixes, respectively, that are currently down. For ISIS networks, **Overloaded Routers** displays all the routers that currently have their overload bit set. The **Router** column identifies the router that corresponds to each link or prefix, while the **Number of Down Links** column displays the number of times the link or prefix that are down. To view the list of links or prefixes as a bar chart, click  **View as Bar Chart** in the upper right corner of the window.



The screenshot shows the 'RIB Browser for: OSPF [any]' window. The left sidebar has 'Down Links' selected. The main area displays a table titled 'Down Link Distribution for: mysqlTest.OSPF'. The table has three columns: 'Router/Net', 'IP Address', and 'Number of Down Links'. There are 23 entries in the table. The bottom status bar shows the date and time: '2007-02-16 10:36:03 PST'.

Router/Net	IP Address	Number of Down Links
--	192.168.3.26	2
--	192.168.0.30	2
--	192.168.3.56	2
--	192.168.3.61	2
--	192.168.0.72	2
--	192.168.3.102	2
--	192.168.3.116	2
--	192.168.3.120	2
--	192.168.3.131	2
PD-REX-RECORDER	192.168.3.144	2
--	192.168.3.172	2
--	192.168.0.179	2
--	192.168.1.182	2
--	192.168.3.189	2
--	192.168.3.192	2
--	192.168.1.244	2
--	10.8.254.1	1
--	10.8.254.2	1
--	192.168.3.60	1
--	192.168.0.115	1
--	192.168.3.133	1
--	192.168.0.138	1
--	192.168.0.171	1

Figure 69 RIB Browser 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 are 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 70 shows an example of the RIB Browser with BGP peer data.



Router	Peer BGP ID	Route Count (up)
LA-CORE-RTR5	10.120.1.5	77
--	167.167.167.167	50
SF-CORE-RTR1	10.120.1.1	19
DC-CORE2-ROUTER4	10.120.1.4	15
DC-CORE1-ROUTER3	10.120.1.3	10
CORE-ROUTER13	10.120.1.13	5

Figure 70 RIB Browser for BGP

For BGP protocol, the RIB Browser displays distributions of the advertised prefixes according to their attributes. A tree structure on the left side of the window presents the following attribute options:

- **Peer**—Displays the number of routes advertised by the peer.
- **Nexthop**—Displays the number of routes that list that Nexthop router among their attributes.
- **Originator**—Displays the number of routes that list that Originator among their attributes.
- **Local Pref**—Displays the number of routes that list that Local Pref among their attributes.

- **MED**—Displays the number of routes that list that MED among their attributes.
- **Communities**—Displays the number of routes that list that community among their attributes.
- **Neighbor AS**—Displays the number of routes that list that neighbor AS among their attributes.
- **2nd Hop AS**—Displays the number of routes that list that 2ndHopAS among their attributes.
- **Origin AS**—Displays the number of routes that list that origin AS among their attributes.
- **Any AS**—Displays the number of routes that list that AS among their attributes.
- **AS Peers**—Displays the number of routes that list that peer-pairing among their attributes.
- **Prefixes**—Displays a count of routes for that prefix 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. 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 that are down. 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 151).
- **Filter Analysis**—Displays a new RIB Browser window with data for the selected entity only.

VPN Protocol

For VPN protocols, the RIB Browser displays distributions of the advertised prefixes their attributes. A tree structure on the left side of the window presents the following attribute options:

- **Peer**—For each peer, displays the number of routes advertised by that peer.
- **MP Nexthop**—For each MP NextHop, displays a count of routes that list that MP NextHop router 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.
- **Ext. Communities**—For each Extended Community, displays a count of routes that list that Extended Community among their attributes.
- **VPN Customer**—For each VPN Customer, displays a count of routes that list the RTs associated with that VPN Customer among their attributes.
- **Prefixes**—For each prefix, displays a count of routes for that prefix.
- **Route Distinguishers**—For each route distinguisher, displays a count of routes that list that Route Distinguisher among their attributes.
- **VPN Prefixes**—For each VPN prefix, displays a count of routes for that VPN prefix.

OSI ISIS Protocol

For OSI ISIS protocol, the RIB browser displays a tree structure on the left side of the window and presents the following attribute options:



If OSI ISIS is not detected by the system, this window will not display.

- **Down Links**—Provides details of the number of links between the routers that are down.
- **Down Prefixes**—Displays the number of prefixes that are down in the topologies that are loaded.

- **Overloaded Routers**—Displays the routers that have their overload bit set.
- **Down ES Neighbors**—Displays the number of ES Neighbors that are down.
- **Down Prefix Neighbors**—Displays the number of Prefix Neighbors that are down.

Use the **Filter By** drop-down list to select the filter parameters and the **Analyze Matching** or **Analyze Excluding** buttons to list only those links that match the filter criteria, or exclude those events that match the filter criteria, respectively.

For more information on using filters, see [Using Filters](#) on page 195.

RIB 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 71](#) provides an example of one such instance.

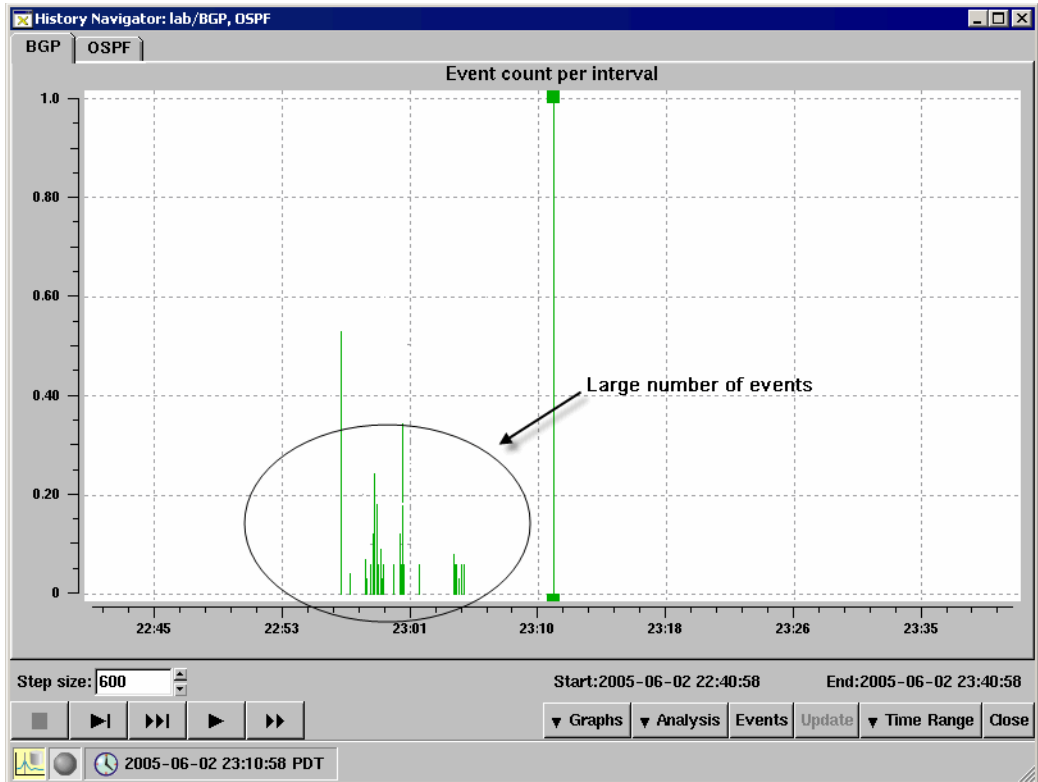


Figure 71 Large Number of Events in Short Space of Time

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 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose **Analysis** → **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 window opens. It is similar to the RIB browser window.

IGP Protocols

For IGP protocols, the RIB Before-N-After Comparison window includes columns for the link and prefix counts before and after the events, and also a column for the difference between the two. Figure 72 show an example of the RIB Comparison window with IGP link data.

Router/Net	System ID	Down Link Count Delta	Before Count	After Count
PD-REX-RECORDER	0100.6401.5203.00	2	0	2
LA-CORE-RTRS	0000.0000.0005.00	2	0	2
PD-REX-RECORDER	0100.6401.5200.00	1	3	4
--	0101.0321.2006.00	1	3	4
--	0101.0314.4006.00	1	2	3
--	0101.0320.4006.00	1	3	4
--	0101.0312.5006.00	1	3	4
PD-REX-RECORDER	0100.6401.5217.00	1	3	4
PD-REX-RECORDER	0100.6401.5223.00	-1	3	2
PD-REX-RECORDER	0100.6401.5229.00	1	3	4
PD-REX-RECORDER	0100.6401.5236.00	1	3	4
PD-REX-RECORDER	0030.4888.2756.00	-1	3	2
PD-REX-RECORDER	0030.4886.A3D3.00	1	3	4
PD-REX-RECORDER	0030.4872.D3F4.00	1	3	4


14 entries


2008-02-22 00:35:43 - 2008-02-27 03:07:42 PST

Close

Figure 72 RIB Comparison for IGP

Click the **Down Link** and **Down Prefix** options to view information about the down links and prefixes, respectively. **Overloaded Routers** shows all the routers that have had their overload bit change between the two set time frames, along with what states the bits were at the beginning and end time frames. **Changed Metrics** shows all the links whose metric values have changed between the

time frames, along with what the values were at in the beginning and end time frames. To view the list of links or prefixes as a bar chart, click  **View as Bar Chart**.

Click a router in the list and the corresponding node 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 times the link or prefix that are 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 [Understanding the Events List](#) on page 177.
- **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 window as those that appear in the RIB browser. In addition, **Before**, **After**, and **Delta** columns display the route count before and after the specified events, and the difference between the two counts.

[Figure 73](#) displays the RIB Comparison window.

For the Peer, Nexthop and Originator options, click any entry in the list, and the corresponding node flashes yellow on the 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 any of the lists as a bar chart, click  **View as Bar Chart**.

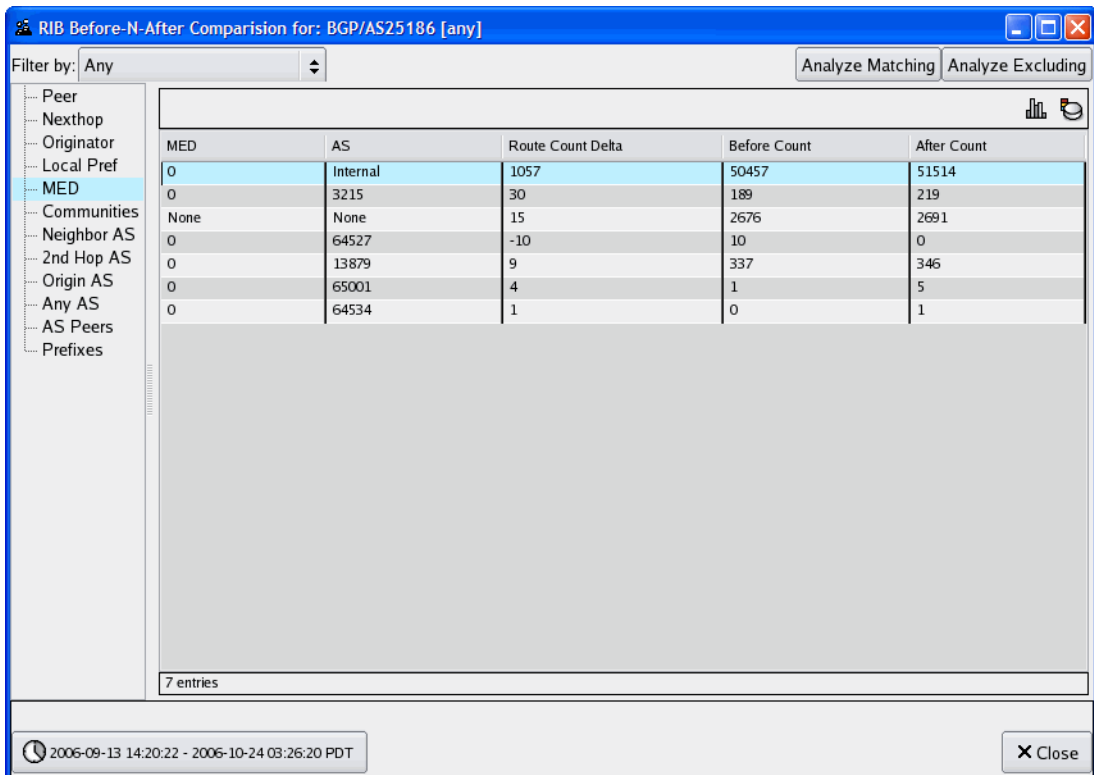


Figure 73 RIB Comparison for BGP

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 window. See [Figure 74](#) for an example of the display.
- **Filter Analysis**—Displays a new RIB Browser window with data for the selected entity only.

Router Name	Peer BGP ID	Prefix	Before Attributes	After Attributes
--	24.0.0.3	192.168.120.0/24	--	Next Hop: 192.168.129.1 AS Path: 65533 11111 (IGP) Local-Pref: 100 MED: 222 Next Hop: 192.168.129.1
--	24.0.0.3	25.0.0.1/32	--	AS Path: (INCOMPLETE) Local-Pref: 100 MED: 0 Next Hop: 192.168.129.1
--	24.0.0.3	192.168.122.90/32	--	AS Path: (INCOMPLETE) Local-Pref: 100 MED: 0 Next Hop: 192.168.103.11
--	24.0.0.3	27.27.27.0/29	--	AS Path: 65533 11111 (INCOMPLETE) Local-Pref: 100 MED: 222 Next Hop: 192.168.129.1
--	24.0.0.3	192.168.103.0/24	--	AS Path: (IGP) Local-Pref: 100 MED: 2 Next Hop: 192.168.110.11

17 entries

Figure 74 Show Differences Display

VPN Protocol

In addition to the options found for BGP, RIB Browser Before-N-After Comparison for VPN includes the following options: MP Nexthop, Ext. Communities, VPN Customers, Route Distinguishers, and VPN Prefixes. These options are described in the RIB Browser section for VPN Protocol on [page 163](#).

The functions for RIB Browser Before-N-After Comparison for VPN protocol are the same as for BGP protocol (described on [page 167](#)) with the exception of the Animation feature, which is not included for VPN.

OSI ISIS Protocol

As in IGP protocols, similar columns appear in the RIB Before-N-After Comparison window for OSI ISIS.



If OSI ISIS is not detected by the system, this window will not display.

Trending

Use this option to view aggregate event counts over an extended period of time. [Figure 75](#) provides an example of one such instance.

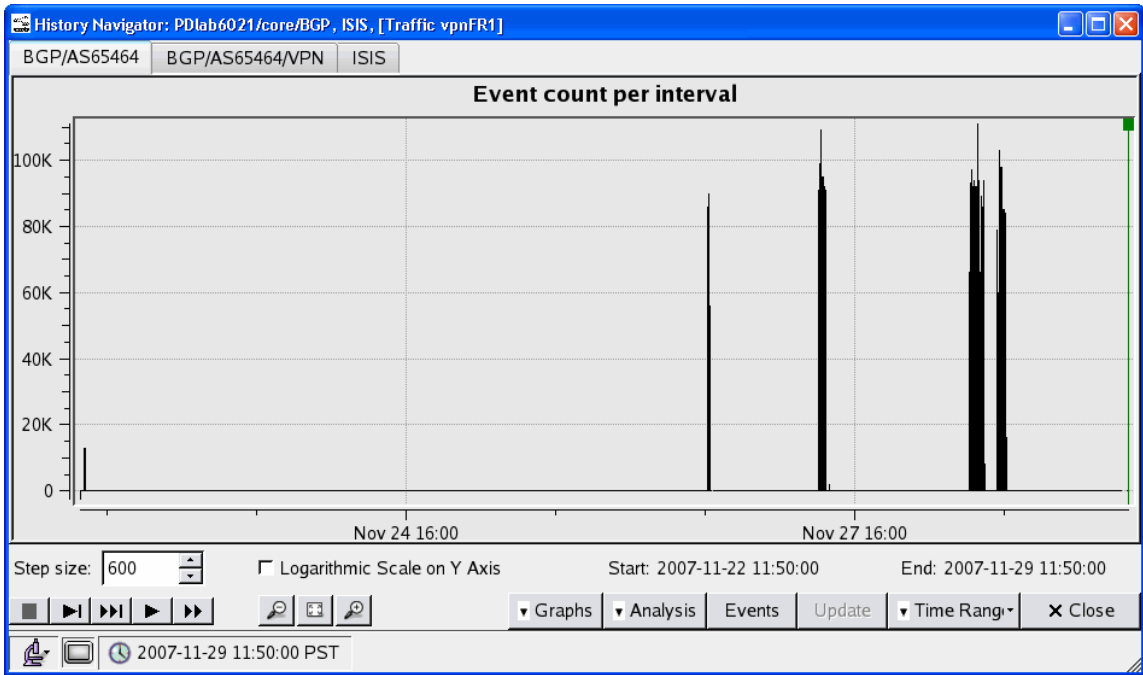


Figure 75 Event Trending

To display a trending graph, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose **Analysis** → **Trending**.
- 3 Select whether to display the trending graph in linear or exponential format, and choose the desired end date. You can enter values directly or click on a component of the date and use the up and down arrows (Figure 76).

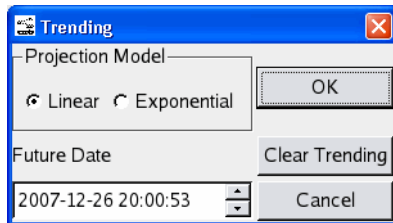


Figure 76 Trending

- 4 Click **OK** to display the graph.

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. The system 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.

In Monitoring mode, the update interval is refreshed every 10 seconds, by default. If any events are generated during this time frame, a spike corresponding to the number of events is drawn on the graph.

In Analysis mode, the data points for the events graph is updated every 600 seconds, by default.


To analyze a series of events, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose **Analysis** → **Event Analysis**.
- 3 Click in the Events graph just before the events occurred.
- 4 Click in the Events graph just after the events occurred.
- 5 (Optional) If you have more than 500k events, a window prompts you to **Continue**, **Abort**, or **Prefilter** the events.
- 6 (Optional) If you select **Prefilter**, the Event Prefiltering window opens. From here, you can select from a list of filters from the drop-down menu, decreasing the time it takes to generate the event list. For more information on using filters, see [Using Filters](#) on page 195.

The Event Analysis window appears.

IGP Protocols

For IGP protocols, this window displays the number of routing events that occurred in the specified time interval for each involved initiator, router, link, or prefix. [Figure 77](#) shows an example Event Analysis window.

To locate a router on the routing topology map, click 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, right-click the corresponding row in the table, 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 179 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.

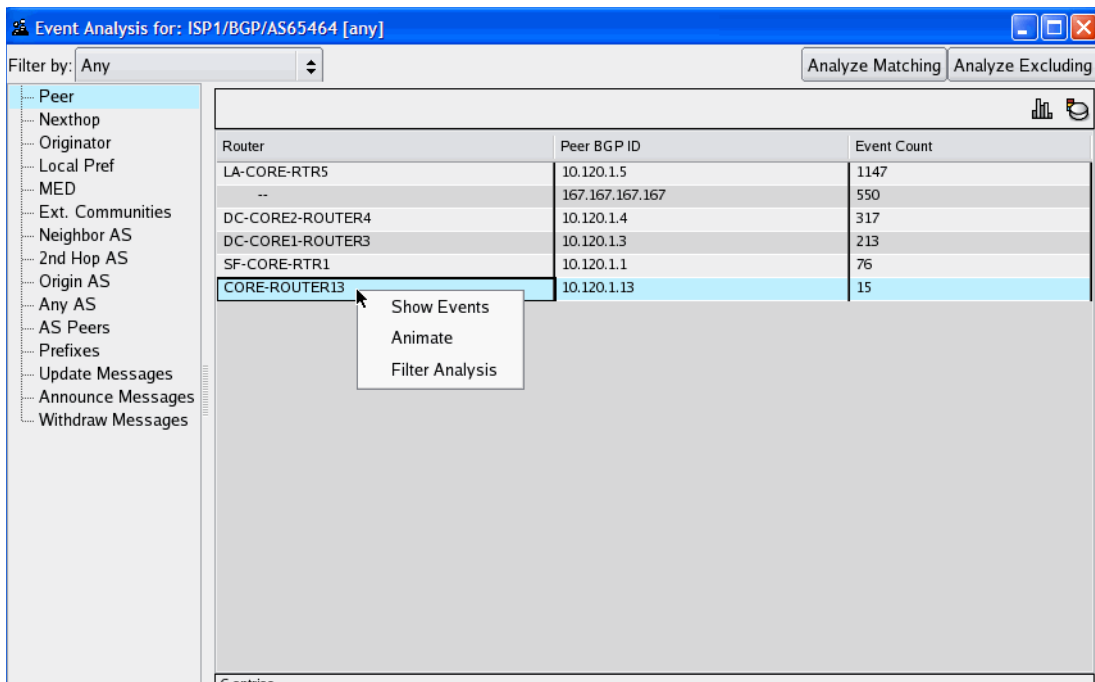


Figure 77 Event Analysis

BGP Protocol

For BGP, the Event Analysis window 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, right-click the corresponding row in the table, 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 [Understanding the Events List](#) on page 177 for information about this window.
- **Animate**—Displays an Animation window that animates the events reported by the selected entity. No Root Cause Analysis is performed. See [Root Cause Analysis](#) on page 143 for information about the controls that appear in this window.
- **Filter Analysis**—Displays a window with event data for the selected entity only.

[Figure 78](#) shows an example of the Event Analysis window for BGP, and includes the pop-up menu that appears when you right-click an entry in the list.

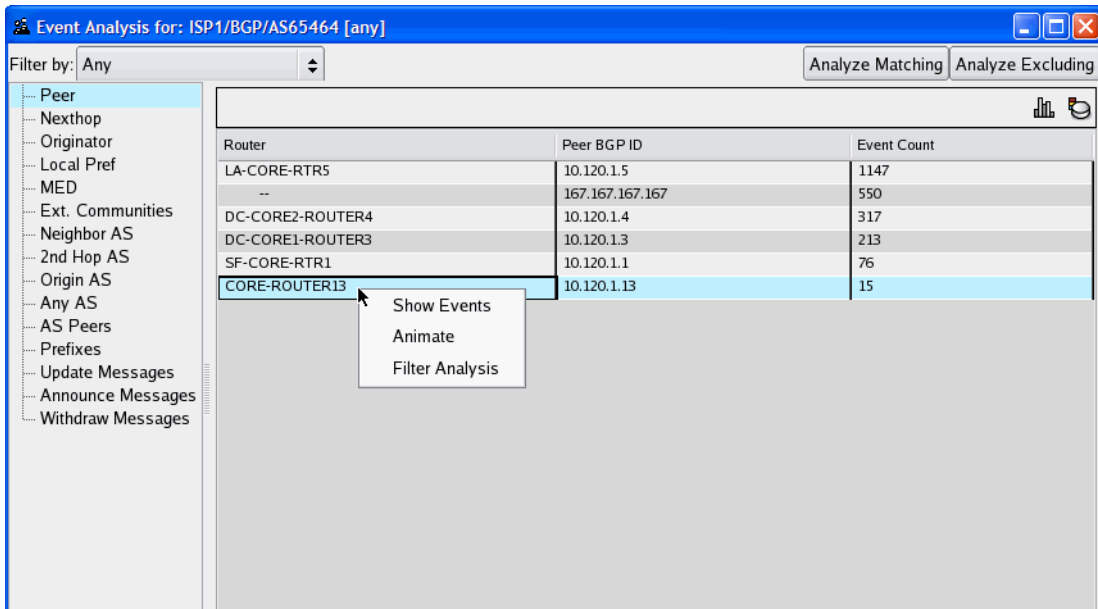


Figure 78 Event Analysis for BGP

VPN Protocol

In addition to the options found for BGP, Event Analysis window for VPN includes the following options: MP Nexthop, Ext. Communities, VPN Customers, Route Distinguishers, and VPN Prefixes. These options are described in the RIB Browser section for VPN Protocol on [page 163](#).

The functionality for Event Analysis for VPN is the same as the Event Analysis for BGP, described on [page 173](#).

OSI ISIS Protocol

For OSI ISIS protocol, the Events Analysis window displays the number of routing events that occurred in a specified time interval with particular values for the Initiator, Router, Link, Prefix, ES Neighbor, and Prefix Neighbor.



If OSI ISIS is not detected by the system, this window will not display.

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, right-click the corresponding row in the table, 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 [Understanding the Events List](#) on page 177 for information about this window.
- **Animate**—Displays an Animation window that animates the events reported by the selected entity. No Root Cause Analysis is performed. See [Root Cause Analysis](#) on page 143 for information about the controls that appear in this window.
- **Filter Analysis**—Displays a window with event data for the selected entity only.

Flow Record Browser



This section applies to RAMS Traffic only.

Use the Flow Record Browser to display aggregated flow information.

The columns of information vary according to the type of aggregation chosen on the left side of the window. Choose a type from the side to display the flow information.

Aggregated by Source Address		
Source Address	Bytes	Packets
10.64.12.9	581.45M	578.00K
10.64.10.14	88.65M	87.66K
10.64.10.13	88.63M	87.68K
10.64.10.15	75.19M	74.32K
10.64.10.10	66.45M	65.68K
10.64.10.11	66.41M	65.64K
10.64.10.19	44.47M	44.20K
10.64.10.28	44.36M	44.09K
10.64.10.26	44.32M	44.05K
10.64.10.18	44.32M	44.05K
10.64.10.12	44.30M	43.81K
10.64.10.23	44.28M	44.02K
10.64.10.27	44.28M	44.01K
10.64.10.17	44.27M	44.00K
10.64.14.9	44.16M	43.90K
10.64.10.25	39.85M	39.61K
10.64.10.20	37.55M	37.32K
10.64.10.16	37.55M	37.32K
10.64.10.21	33.12M	32.92K
10.64.10.24	22.14M	22.00K
10.64.14.8	22.08M	21.95K
3757 entries		

Figure 79 Flow Record Browser with Source Address Aggregation

To use the flow record browser, perform the following step:

- 1 Open the client application and choose **Reports** → **Flow Record Browser** to open the Flow Record Browser window.

The following aggregation choices are available:

- **Protocols**– Aggregation by protocols involved in the flow. Select **Protocols** and then expand or contract the listing as needed.
- **Exporters**– Aggregation by IP addresses of exporters
- **Source Address**– Aggregation by source IP addresses
- **Destination Address**– Aggregation by destination IP addresses
- **Multicast Group**– Aggregation by groups configured as multicast groups
- **Egress PE**– Aggregation by IP addresses of egress PEs
- **Traffic Groups**– Aggregation by groups configured as traffic groups
- **CoS**– Aggregation by class of service levels

- **Conversations**– Aggregation by active connections, indicated by source > destination IP address pairs
- **Outgoing**– Choices include:
 - Egress Hop– Aggregation by IP address for the egress hop
 - Neighbor AS– Aggregation by IP address of the neighboring AS
 - Destination AS– Aggregation by IP address of the destination AS
- **Incoming**–
 - Ingress Hop– Aggregation by IP address for the ingress hop
 - Neighbor AS– Aggregation by IP address of the neighboring AS
 - Destination AS– Aggregation by IP address of the destination AS

Understanding the 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 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Click **Events**.
- 3 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.
- 4 Move the mouse cursor to the ending time and left-click again to mark that time.
- 5 (Optional) If you have more than 500k events, a window prompts you to **Continue**, **Abort**, or **Prefilter** the events.

- 6 (Optional) If you select **Prefilter**, the Event Prefiltering window opens. From here, you can select from a list of filters from the drop-down menu, decreasing the time it takes to generate the event list. For more information on using filters, see [Using Filters](#) on page 195.

The All Events window opens displaying details of the events that occurred within the selected time period, as shown in [Figure 80](#).



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
2006-04-04 17:36:25.1488	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 2 (Area External)	LabTestDomain.RouteRecorder
2006-04-04 17:36:25.1830	24.0.0.11	Change Prefix	10.88.88.0/24	Metric: 11113 (Area External)	LabTestDomain.RouteRecorder
2006-04-04 17:36:25.1830	24.0.0.11	Change Prefix	10.79.79.0/24	Metric: 11113 (Area External)	LabTestDomain.RouteRecorder
2006-04-04 17:36:30.0798	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 1 (Area External)	LabTestDomain.RouteRecorder
2006-04-04 17:36:30.1150	24.0.0.11	Change Prefix	10.88.88.0/24	Metric: 11112 (Area External)	LabTestDomain.RouteRecorder
2006-04-04 17:36:30.1150	24.0.0.11	Change Prefix	10.79.79.0/24	Metric: 11112 (Area External)	LabTestDomain.RouteRecorder
2006-04-04 17:46:04.6575	192.168.0.171	Add Router		Type: Internal Router	LabTestDomain.RouteRecorder
2006-04-04 17:46:04.6888	10.88.88.2	Add Router		Type: Internal Router	LabTestDomain.RouteRecorder
2006-04-04 17:46:13.4894	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 2 (Area External)	LabTestDomain.RouteRecorder
2006-04-04 17:46:13.5212	24.0.0.11	Change Prefix	10.88.88.0/24	Metric: 11113 (Area External)	LabTestDomain.RouteRecorder
2006-04-04 17:46:13.5212	24.0.0.11	Change Prefix	10.79.79.0/24	Metric: 11113 (Area External)	LabTestDomain.RouteRecorder
2006-04-04 17:46:18.8811	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 1 (Area External)	LabTestDomain.RouteRecorder
2006-04-05 09:43:25.7056	192.168.0.72	Add Router		Type: Internal Router	LabTestDomain.RouteRecorder
2006-04-05 09:55:47.5291	192.168.0.2 DR	Add Neighbor	192.168.0.127	Metric: 0	LabTestDomain.RouteRecorder
2006-04-05 09:44:51.3011	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 2 (Area External)	LabTestDomain.RouteRecorder
2006-04-05 09:44:56.5149	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 1 (Area External)	LabTestDomain.RouteRecorder
2006-04-05 09:52:34.5317	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 2 (Area External)	LabTestDomain.RouteRecorder
2006-04-05 09:52:40.3927	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 1 (Area External)	LabTestDomain.RouteRecorder
2006-04-05 09:55:42.4624	192.168.127.2	Add Router		Type: Internal Router	LabTestDomain.RouteRecorder
2006-04-05 09:55:47.4941	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 2 (Area External)	LabTestDomain.RouteRecorder
2006-04-05 09:55:47.5291	192.168.0.127	Add Router		Type: Internal Router	LabTestDomain.RouteRecorder
2006-04-05 09:55:52.9060	24.0.0.11	Change Prefix	192.168.116.0/24	Metric: 1 (Area External)	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	24.0.0.2	Add Router		Type: ASBR	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	192.168.101.2 DR	Add Router		Type: LAN Pseudo-Node	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	192.168.103.11 DR	Add Router		Type: LAN Pseudo-Node	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	24.0.0.5	Add Router		Type: Area BR, ASBR	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	24.0.0.11	Add Router		Type: Area BR, ASBR	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	24.0.0.12	Add Router		Type: ASBR	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	192.168.0.2 DR	Add Router		Type: LAN Pseudo-Node	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	192.168.0.179	Add Router		Type: Internal Router	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	192.168.0.176	Add Router		Type: Internal Router	LabTestDomain.RouteRecorder
2006-04-05 10:01:27.2618	192.168.0.171	Add Router		Type: Internal Router	LabTestDomain.RouteRecorder









574 entries | 2006-04-04 11:56:17 - 2006-04-07 02:18:57 PDT

Figure 80 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 184).

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 window, 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, with the exception of traffic data in RAMS Traffic, which is delayed by 30 minutes. This button is disabled when the History Navigator window is in Analysis mode.
-  **Show Current Event**,  **Stop Execution**,  **Execute One Event**, and  **Start Execution** buttons—See [Moving Time and Executing Events](#) on page 186 for information about using these buttons.
-  **Clear** button—Clears all events from the Events window. This button is only functional in Monitoring 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 OSI ISIS Link State Packets (LSP). EIGRP is a distance-vector protocol, so it does not communicate link-state changes directly. However, the system 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, reannouncements, and withdrawals. In addition to the events indicating network state changes, entries are inserted in to the events list when the peering between the appliance and 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 17 .

Table 17 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 OSI ISIS, 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 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, Reannounce 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. This includes node isolation for ISIS domains. A corresponding alert will occur once this isolation is detected.
Area or AS	The OSPF area, OSI ISIS 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 80](#), 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 192.168.0.72 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 192.168.0.127 as a neighbor with metric 0. (The metric from a pseudonode to a router is always 0). About 20 minutes later, the adjacency was dropped and the router along with it.

If the Router Isolated alert is enabled, an alert is sent when all of the adjacencies in a specific area attached to a router are down. This action isolates the node from the rest of its area, and the router is no longer accessible from the connected area where the peering resides.

The following information is included in the isolated router alert:

- Time and date the router was isolated.
- Specific area in which the router isolation occurs.
- Information on the router that was isolated

When a Router Isolated alert is received, open the routing topology map to view the effect of the isolation. The History Navigator window is also useful for bringing up the Events List for the network, which will display information about adjacency losses that cause router isolations in the **Attributes** column.

To configure router isolated alerts, see [Creating New Alerts](#) on page 434.

Event Operations and Attributes

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 prefix advertisement of the router 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 [Appendix A](#), “Protocol Compliance.”

- OSI ISIS: Since OSI ISIS 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.” The system labels an OSI ISIS 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 [Appendix A](#), “Protocol Compliance.”
- 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 the 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

The system 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 OSI ISIS 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. The system cannot infer the link change in this case.
- Not on old path; new path broken—If the internal routing topology model provided by the system 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, The system will not be able to infer a link failure that partitions some nodes from the viewpoint of the appliance.
- Query failed—A query by the system 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 the system 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.

- BGP: The set of event operations for BGP is small: Open or Close of a peering, or announce, reannounce, 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 [Appendix A](#), “Protocol Compliance.”

In addition to the protocol-specific events outlined above, there are Add Peering and Drop Peering events that indicate when the system 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 Add Router event at 09:43:25 in [Figure 80](#), 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.

If you have more than 500k events, the system will display a window prompting you to prefilter. If you select Prefilter, you can select from an array of filters to help cut down processing time. See Step 5 in [Understanding the Events List](#) on page 177 for more information.

Some parameters require that you type a value in a text box (for example, if you filter by router, you must type 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 195 explains how to combine filter parameters using the **Expressions** option on the filter drop-down list.

See [Using Filters](#) on page 195 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 ([Node Information Panel](#) on page 77 and [Link Information Panel](#) on page 79, 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 3 and 4 in [Understanding the Events List](#) on page 177. You can adjust the time range as needed.

In Analysis mode, you can double-click the date/time area to display the playback controls. Choose a date and time and a step size in sections for the playback, and click **OK**. Then click the right-facing arrow to begin the playback.



Figure 81 Main Window Status Bar

To adjust the start and end of the time range, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Adjust the time range in any of the following ways:
 - Click **Time Range** → **Online** to view current data in a moving 1-hour window.
 - Click **Time Range** → **Custom**. Type new values into the **From** and **To** fields, or adjust the values with the up and down triangle buttons. Click **OK**.
 - Choose **Time Range** and select a pre-set interval: one hour, day, week or month. The time range will be centered around the currently displayed point in time.
 - Choose **Time Range** → **Recent** to display a drop-down list of recently used time ranges from which you can select.
 - Choose **Time Range** → **All** to include all events recorded in the database.



In RAMS Traffic, Traffic data is delayed by 30 minutes.

- 3 Click **OK** to accept the adjusted time range.






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 box 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 80](#), the next event is the Add Router event at 09:43:25.

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 (X), 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.

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. The [RIB Comparison](#) on page 165 showed how the History Navigator window 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 narrow down the event churn to its root cause.

In the example shown in [Figure 82](#), a period of instability (a high level of churn) lasts for more than an hour. Using the History Navigator Event Analysis tool, you can focus on a small part of the total churn period.

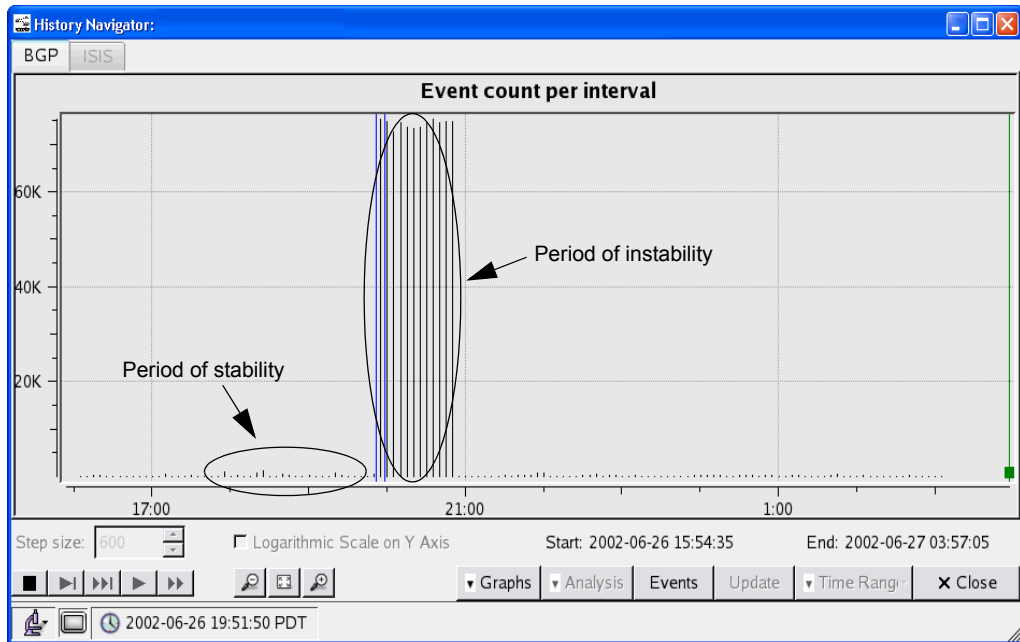


Figure 82 Stability and Instability

To perform an events analysis, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose **Analysis** → **Event Analysis**.
- 3 Mark the start and end time for the analysis using the blue cross-hairs.
The Event Analysis window appears, as shown in [Figure 83](#).

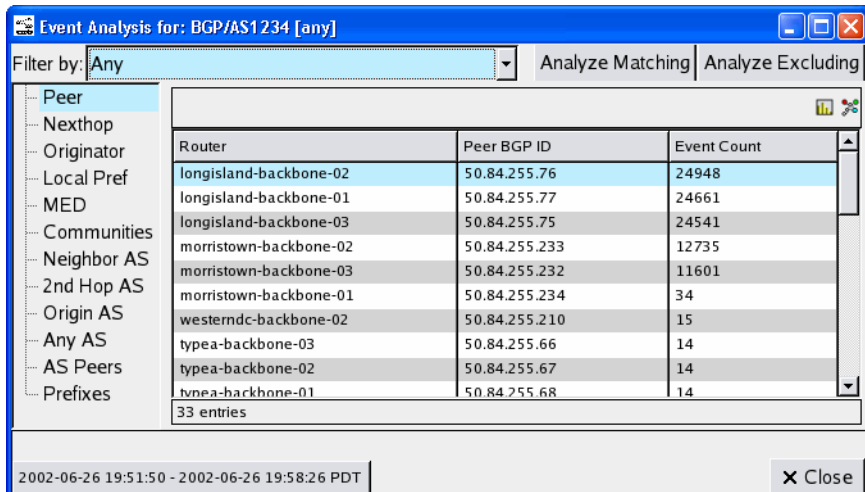


Figure 83 Event Analysis Window

The Event Analysis table can be filtered, sorted by column heading, or viewed as a bar chart.

When the **MED** option is selected, as shown in Figure 84, a small number of MEDs may have a large number of events associated with them. This could represent a MED oscillation.

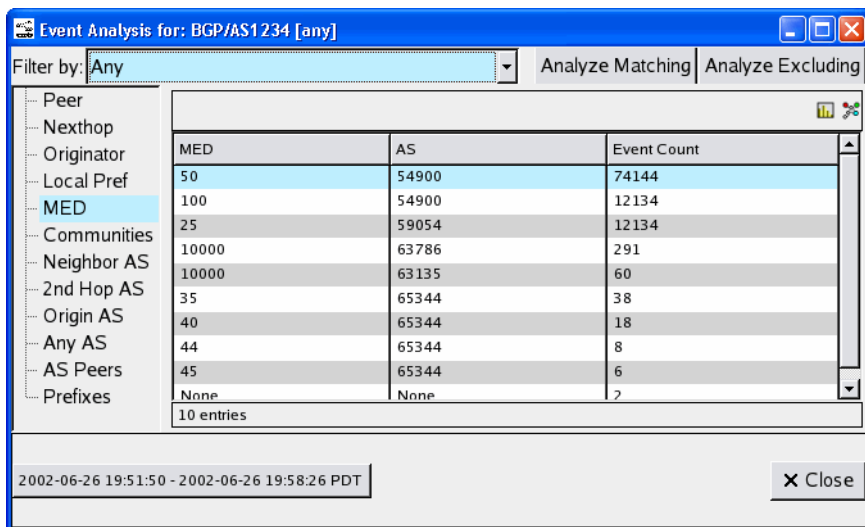
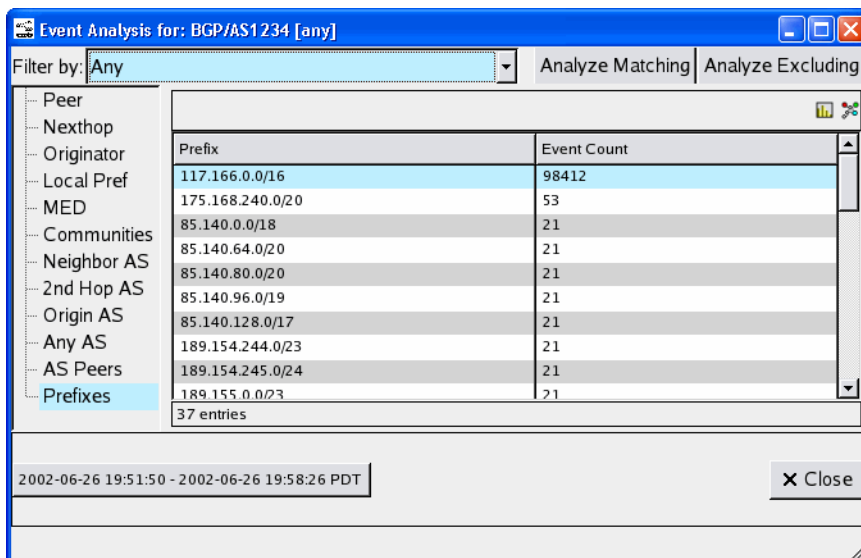


Figure 84 MEDs

To identify the prefixes affected by this possible MED oscillation, select the **Prefixes** tab as shown in [Figure 85](#).



Prefix	Event Count
117.166.0.0/16	98412
175.168.240.0/20	53
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

37 entries

2002-06-26 19:51:50 - 2002-06-26 19:58:26 PDT

Close

Figure 85 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 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose **Analysis** → **Event Analysis**.
- 3 Select a time range (see [Adjusting the Time Range](#) on page 185).
- 4 Right-click the desired prefix.
- 5 Click **Filter Analysis** in the pop-up window that appears.

[Figure 86](#) displays the results of the drill-down filter analysis.

The screenshot shows a window titled "Event Analysis for: BGP/AS1 234 [(any and prefix 175.168.240.0/20)]". The "Filter by:" dropdown is set to "Any". The table displays event counts for various routers and their associated Peer BGP IDs. The data is as follows:

Router	Peer BGP ID	Event Count
westerndc-backbone-02	50.84.255.210	12
westerndc-backbone-01	50.84.255.211	12
westerndc-backbone-03	50.84.255.209	11
richardson-backbone-03	50.84.255.84	6
richardson-backbone-02	50.84.255.85	6
richardson-backbone-01	50.84.255.86	6

The interface also includes a left-hand navigation menu with categories like Peer, Nexthop, Originator, Local Pref, MED, Communities, Neighbor AS, 2nd Hop AS, Origin AS, Any AS, AS Peers, and Prefixes. At the bottom, a date range "2002-06-26 19:51:50 - 2002-06-26 19:58:26 PDT" and a "Close" button are visible.

Figure 86 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.

The RIB analysis identified the possibility of a MED oscillation, and the 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 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose **Analysis** → **Event Analysis**.
- 3 Select the desired start and end times with the blue cross-hairs.

- 4 To view the events associated with an individual table entry, right-click the entry, and then select **Show Events** in the pop-up menu.

The Filtered Events window appears, as shown in [Figure 87](#). This window lists all of the events associated with the selected table entry.

Time	Router	Operation	Neighbor/Prefix	Attributes	Area or AS
2002-06-26 19:51:50.009063	50.84.255.77	Withdraw	117.166.0.0/16	AS Path: 54900 (IGP) Local-Pref: 100 MED: 50 Communities: 65326:65326 65326:4 Next Hop: 50.84.217.213 Originator Cluster List: 255.255.172.234 Aggregator: AS54900 46.97.191.6 (A	DemoTier1ISPJun02b.BGP/AS1234
2002-06-26 19:51:50.009144	50.84.255.77	Announce	117.166.0.0/16	AS Path: 54900 (IGP) Local-Pref: 100 MED: 50 Communities: 65326:65326 65326:4 Next Hop: 50.84.217.213 Originator Cluster List: 255.255.172.234 Aggregator: AS54900 46.97.191.6 (A	DemoTier1ISPJun02b.BGP/AS1234

48794 entries 2002-06-26 19:51:50 - 20:05:01

Figure 87 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.

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

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose **Analysis** → **Root Cause Analysis**.
- 3 Select the desired start and end times with the blue cross-hairs.

The Root Cause Analysis Results window opens, as shown in [Figure 88](#). For more information on using root cause analysis, see [Root Cause Analysis](#) on page 143.

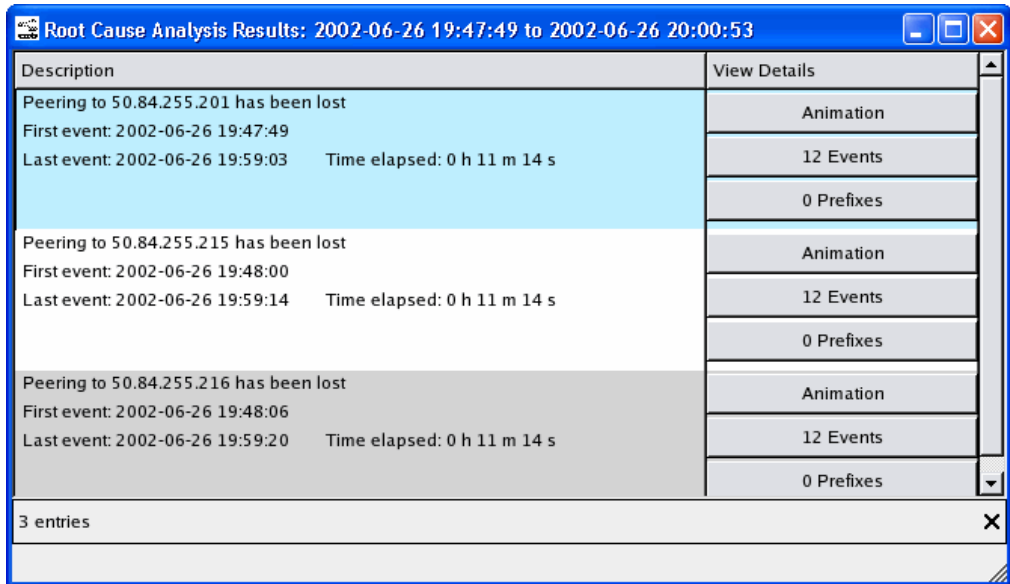


Figure 88 Root Cause Analysis Window

Correlating Time Series Data

The power of routing navigation is extended 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 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 and performing a time correlation with routing events can help diagnose the root cause of the anomaly.

You can import data in MRTG ASCII `.log` file format, Round Robin Database (rrdtool) `.rrd` binary format version 1 or 3 little-endian architecture, RRD xml dump 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 appliance. The administrator must first enable the FTP server. See “Administration” in the *HP Route Analytics Management System Administrator Guide*.

To upload files to the appliance, perform the following steps:

- 1 FTP or SFTP to the appliance using the IP address of the appliance.
- 2 Log in with your user name and password.



The administrator must enable FTP access for your account.

- 3 Change the directory to `pub`.
- 4 Transfer one or more files to the appliance.

To display a time series file (all formats), perform the following steps:

- 1 Open the client application and choose **Reports** → **Correlate Time Series**.
- 2 The available files are listed on the left side of the window. Select a file to display the time series data.

The green cursor in the time series graph is time-aligned with the cursor in the History Navigator window 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.



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.

When displaying MRTG data, note that 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 option is provided on several tables, including the RIB Browser and Events List, to allow you to focus in on items of interest. [Figure 89](#) 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 following filter levels are available:

- 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 200 for examples of the parameter syntax as illustrated using filter expressions.



With a simple filter, you type 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 90](#) 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.
- You can also pre-filter events for the following features:

- Root Cause Analysis
- Event Lists
- Event Analysis

This option is prompted if you have more than 500k events for the system. Using this pre-filter will cut down on the time it takes to generate the information you are looking for.

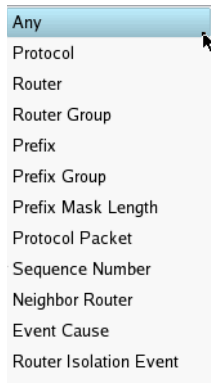


Figure 89 Filter By Drop-Down List

In many cases, the built-in **Filter by** selections, such as the ones shown in [Figure 89](#), provide sufficient flexibility in filtering.

The Router filter accepts a space-separated list of router addresses or names when several specific routers are of interest. The Community filter accepts a space-separated list of community strings when prefixes with different community strings are of interest. The filter matches if any of the community strings matches (OR relationship). The Sequence Number filter accepts LSP packet sequence numbers.

The protocol related filters, such as BGP Ingress Router, allow you to specify the IP address of the node.

To set up a simple filter, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose the report of interest.
- 3 Select an operator from the Filter by drop-down list.

A text box is shown on the right of the Filter by parameter.

- 4 Type the address of the node in the text box.

For example, if you want to see only the events that are reported by the node with IP address 192.168.167.166, choose **Router** in the Filter by drop-down list and then enter the IP address in the text box (Figure 90).



Figure 90 Parameter Text Box

- 5 Click **Show** to list only items that match the address, or click **Hide** to list only the items that do not match the address.

To set up an advanced filter, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose the report of interest.
- 3 Select **Advanced** from the Filter by drop-down list.

The Composing Advanced Filter window opens, as shown in Figure 91.

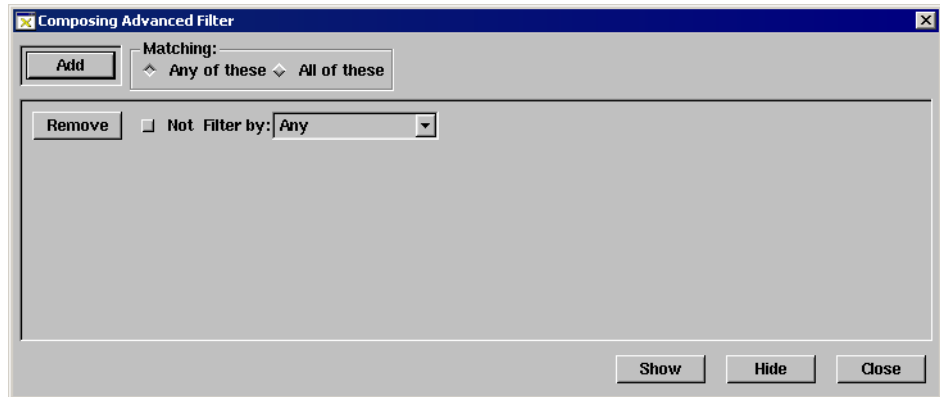


Figure 91 Advanced Filter Window

- 4 Choose a filter operator from the Not Filter by drop-down list.



The Remove button removes the Not Filter By field.

Some operators require that you type the parameter in a text box; others let you choose among items in a list.

- 5 Specify the appropriate parameter value.
- 6 To exclude matching items, click **Not** for that operator.
- 7 To add another operator to the filter, click **Add** in the upper left corner of the window and define the parameters for the new operator.
- 8 After you add 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.
- 9 Click **Show** to list all events that match the filter, or click **Hide** to list only the events that do not match the filter.

The filter is translated internally into a filter expression that combines the filter operators with the parameters that you specified.

You can combine multiple levels of advanced filters to construct any logical AND-OR expression.

To enter a filter expression manually, perform the following steps:

- 1 Open the client application and choose **Reports** → **History Navigator** to open the main History Navigator window.
- 2 Choose the report of interest.
- 3 Choose **Expression** from the Filter by drop-down list.
- 4 If desired, select a filter from the Custom Filters drop-down list, which will then populate the adjacent text box as shown in [Figure 92](#). Otherwise, go to Step 3. You can enter and save filter expressions in the Custom Filter Repository as described in [Creating Custom Filters](#) on page 85.
- 5 If necessary, modify the selected expression or enter a new expression in the text box.

See [Expression Syntax](#) on page 199 for information about the syntax used to enter expressions, and [Expression Definitions](#) on page 200 for a complete list of operators and examples showing their use.



Figure 92 Expression Text Box

- 6 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 include multiple terms (operators and parameters).

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

Regular Expression

A regular expression is a string that is used to describe or match a set of strings, according to certain syntax rules. Regular expressions are used to search and manipulate bodies of text based on certain patterns.

The following is an example of a string using a regular expression:

`asPath reg exp <asn>`

```
asPath regexp ^123
```

Matches the AS path with the first hop identified as 123.

```
aspPath _123_
```

Matches AS path having “123” in any one of its hops.

For further information about regular expressions, see the following document at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ftersv_c/ftsappx/tcfaapre.htm#wp1020148

Expression Definitions

This section defines the filter operators 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
```

asPath regexp <regular expression>

Matches the as path matching the regular expression. The following example shows the return AS path ending with the number 655 (as path: 124 444 1655. matches, but as path .123 655 111. does not as):

```
AsPath regexp 655$
```

availableBandwidthAfter <n> <relop>

Matches the available bandwidth after the planned changes. For example,

```
availableBandwidthAfter 100 lt
```

availableBandwidthBefore <n>

Matches the available bandwidth before the planned changes. For example,

```
availableBandwidthBefore 1000 lt
```

availableBandwidthChange <n> <relop>

Matches the difference of the available bandwidth before and after the planned changes. For example,

```
availableBandwidthChange 100 eq
```

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)

capacity <n> <relop>

In RAMS Traffic, matches the traffic link with capacity equal, less than or greater than the given capacity. For example,

```
capacity 100 lt
```

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.

[destination / MPFilterFlowDst](#)

In RAMS Traffic, matches traffic flow with the specified destination prefix. For example,

```
destination 182.168.0.1/24
```

Matches traffic flow destinations with the prefix of 192.168.0.1/24

[destinationTrafficAfter <n> <relop>](#)

In RAMS Traffic, matches the destination traffic after the planned changes. For example,

```
destinationTrafficAfter 1000 lt
```

[destinationTrafficBefore <n> <relop>](#)

In RAMS Traffic, matches the destination traffic before the planned changes. For example,

```
destinationTrafficBefore 100 lt
```

[egressCapacity <value> <gt/eq/lt>](#)

Matches with the specified egress capacity value in bps according to greater than, equal to, or less than comparisons. For example,

```
egressCapacity 100 gt eq
```

Matches egress capacity greater than 100 bps

[egressTraffic <value> <gt/eq/lt>](#)

In RAMS, matches with the specified egress traffic value in bps according to greater than, equal to, or less than comparisons. For example,

```
egressTraffic 100 gt eq
```

Matches egress capacity greater than 100 bps

`egressUtilization <value> <gt/eq/lt>`

Matches with the specified egress utilization value in bps according to greater than, equal to, or less than comparisons. For example,

```
egressUtilization 100 gt eq
```

Matches egress capacity greater than 100 bps.

`eventCause <cause>`

Matches events with the specified cause of a neighbor or prefix going down.

Causes include:

- Premature
- Expired

`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 rexpensing
eventType drop rexpensing
eventType change rexpensing
eventType drop *
eventType add *
eventType change *
eventType * router
eventType * neighbor
eventType * prefix
eventType * rexpensing
```

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)

`exitRouter <ip address>`

Matches exit router with a given IP address. For example,

```
exitRouter 192.168.0.1
```

Matches the exit router with the IP address of 192.168.0.1.

`exportingInterface <interface address>`

Matches flow export router with given router interface IP address. For example,

```
exportingRouter 192.168.0.1
```

Matches the flow export router interface with the IP address of 192.168.0.1

`exportingRouter <router name/ip>`

Matches flow export router with the specified router name or IP address. For example,

```
exportingRouter 192.168.0.1
```

Matches the flow export router with the IP address of 192.168.01

`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 So0:13632376:123
```

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:

- EIGRP: Internal, ASExt_Type2, ASExt_Type1, Loopback, Dialup, AutoSum, ManualSum, StaticInt, StaticExt, NotFoundInt, NotFoundExt
- ISIS: Internal, ASExt_Type2, ASExt_Type1, TE, TEL2L1, InternalL2L1, AreaExtL2L1, ASExt_Type1L2L1, or ASEXT_Type2L2L1
- OSI: ESNeighbor, PrfxNeighbor, PrfxNeighborComparable
- OSPF: Internal, AreaExt, ASExt_Type2, or ASExt_Type1

For example, in an OSPF network:

```
igpPrefixType AreaExt
```

igpSeqNum <number>

Matches LSP packet sequence numbers. States include:

Equal

Less than

Greater than

For example:

```
igpSeqNum <number> eq  
igpSeqNum <number> lt  
igpSeqNum <number> gt
```

igpState <state>

Matches IGP prefixes with the specified area. States include:

- Up

- Down

`interface <IP Address>`

Matches the interface with the given IP address. For example,

```
interface 192.168.0.1
```

Matches the interface 192.168.0.1

`interfaceIdx <Interface Index>`

Matches the interfaces with the specified interface index. For example,

```
interfaceIdx 1
```

Matches interfaces using index 1

`inTraffic <value> <gt;/eq/lt>`

In RAMS Traffic, this matches communities with the specified traffic (bps) flowing out of a community according to greater than, equal to, or less than comparisons. For example:

```
inTraffic 100 gt eq
```

Matches total traffic received by a community greater than or equal to 100 bps.

`linkBandwidth <value> <gt;/eq/lt>`

Matches EIGRP links with the specified bandwidth value according to greater than, equal to, or less than comparisons. The following example shows the matches for EIGRP links with bandwidth ≥ 1 :

```
linkBandwidth 1 gt eq
```

`linkDelay <value> <gt;/eq/lt>`

Matches EIGRP links with the specified delay value according to greater than, equal to, or less than comparisons. The following example matches EIGRP links with delay ≥ 1 :

```
linkDelay 1 gt eq
```

`linkState <state>`

Matches links with the specified state. States include the following:

- Up
- Down

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:

```
med 987 and neighAS 208
```

metricBandwidth <value> <gt/eq/lt>

Matches EIGRP links with the specified EIGRP inverse bandwidth value according to greater than, equal, or less than comparisons. The metric value is $(10^7 / bw) * 256$, where bw is in units of kilobits per second. For example,

```
metricBandwidth 25600 gt eq
```

matches EIGRP links with inverse bandwidth ≥ 25600 which is bandwidth ≤ 100 Mb/s

metricDelay <value> <gt/eq/lt>

Matches EIGRP links with the specified EIGRP delay metric according to greater than, equal to, or less than comparisons. The delay metric is in units of 10 μ s, multiplied by 256. For example,

```
metricDelay 2560 gt eq
```

matches EIGRP links with delay ≥ 100 μ s

metric <value> <gt/eq/lt>

Matches links with the specified metric value according to greater than, equal to, or less than comparisons. The following example matches links with metric ≥ 1 :

```
metric 1 gt eq
```

`mplsLabels <n> [atHead] [atTail]`

Matches MPLS label anywhere in the label stack, or optionally selects the label at the head or tail. The following example matches MPLS labels with the first label 123:

```
mplsLabels 123 atHead.
```

`mplsLabels regex <regular expression>`

Matches labels matching regular expression. The following example shows MPLS labels starting with 111:

```
mplsLabels regexp ^111
```

`neighbor <router>`

Matches a neighbor router in an events list using any of the forms of router identification described above for `router`.

```
neighbor labnet-gw
```

`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
```

outTraffic <value> <gt/eq/lt>

In RAMS Traffic, matches communities with the specified traffic (bps) flowing out of a community according to greater than, equal to, or less than comparisons. For example,

```
outTraffic 100 gt eq
```

Matches total traffic flowing out of a community greater than or equal to 100 bps.

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
```

peeringDestination <value> <gt/eq/lt>

In RAMS Traffic, matches ASs with the specified traffic whose final destination is the AS according to a greater than, equal to, or less than comparison. For example,

```
peeringDestination 100 gt eq
```

Matches destination traffic greater than or equal to 100 bps.

peeringNextHop <value> <gt/eq/lt>

In RAMS Traffic, matches ASs with the specified traffic flow transiting across the AS according to greater than, equal to, or less than comparisons. For example,

```
peeringNextHop 100 gt eq
```

Matches destination traffic greater than or equal to 100 bps.

peeringTotal <value> <gt/eq/lt>

In RAMS Traffic, matches ASs with the specified traffic flow from the AS according to greater than, equal to, or less than comparisons. For example,

```
peeringTotal 100 gt eq
```

Matches egress capacity greater than or equal to 100 bps.

percent <number>

In RAMS Traffic, matches traffic groups with the percentage of the total traffic flowing for the traffic group which is greater than or equal to the specified percentage. For example,

```
percent 0.10
```

Matches the traffic group whose traffic flow is greater than or equal to 10% of the total traffic.

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
```

`routeTarget RT:<route_target>`

`routeTarget So0<source_of_origin>`

Matches VPN routers with the specified VPN route target (see [extCommunity on page 206](#) for input format). For example,

```
routeTarget RT:59300:460210
RouteTarget So0: 12632376:123
```

`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
```

routerState <state>

Matches routers with the specified state. States include the following:

- Up
- Down

routerType <type>

Matches routers with the specified router type. Router types include the following:

- Internal
- LANPseudonode
- Area BR
- AreaBR_ASBR
- ASBorderRouter
- VirtualRouter
- RouteRecorder
- IBGPpeer
- EBGPpeer
- RouteReflector
- Originator
- EBGPNextHop
- NeighborAS
- Implicit
- IBGP
- Static
- L1Internal
- L2Internal
- L1L2Router
- L1L2Router
- L1L2RouterASBR

- ASBRProxyOutsideArea

`secondHopAS <asn>`

Matches the second hop AS, meaning, the one after the neighbor AS in an AS path. For example,

```
secondHopAS 288
```

`source <ip prefix>`

In RAMS, matches traffic flows with the specified source prefix. For example,

```
source 182.168.0.1/24
```

Matches traffic flow with the source prefix of 182.168.0.1/24

`staticNexthopType <type>`

Matches the specified nexthop type for a static route. The available types are: Network, Interface, Gateway, Default. For example,

```
staticNexthopType Network
```

`totaltrafficAfter <n> <relop>`

In RAMS Traffic, matches the total traffic after the planned changes. For example,

```
totaltrafficAfter 100 eq
```

`totaltrafficBefore <n> <relop>`

In RAMS Traffic, matches the total traffic before the planned changes. For example,

```
totaltrafficBefore 100 eq
```

`totalTrafficChange <n> <relop>`

In RAMS Traffic, matches the difference of total traffic before and after the planned changes. For example,

```
totalTrafficChange 100 eq
```

trafficAfter <n> <relop>

In RAMS Traffic, matches the specified traffic after the planned change. For example,

```
trafficAfter 1000 eq
```

trafficBefore <n> <relop>

In RAMS Traffic, matches the specified traffic before the planned changes. For example,

```
trafficBefore 200 eq
```

trafficChange <n> <relop>

In RAMS Traffic, matches the specified traffic changes. For example,

```
trafficChange 1000 eq
```

traffic <value> <gt/eq/lt>

In RAMS Traffic, matches total egress traffic greater than or equal to 100 bps. For example,

```
traffic 100 gt eq
```

Matches traffic greater than or equal to 100 bps.

transitBandwidthAfter <n> <relop>

Matches the transit bandwidth after the planned changes. For example,

```
transitBandwidthAfter 1000 lt
```

transitBandwidthBefore <n> <relop>

Matches the transit bandwidth before the planned changes. For example,

```
transitBandwidthBefore 1000 gt
```

utilizationAfter <n> <relop>

In RAMS Traffic, matches the specified utilization of the traffic link after the planned change. For example,

```
utilizationAfter 100 eq
```


utilizationBefore <n> <relop>

In RAMS Traffic, matches the specified utilization of the traffic link before the planned change. For example,

```
utilizationBefore 100 eq
```

utilizationChange <n> <relop>

In RAMS Traffic, matches the specified utilization of the traffic link with the specified utilization changes. For example,

```
utilizationChange 200 gt
```

vpnCustomer <name>

Matches VPN routes with the specified VPN customer. For example,

```
vpnCustomer Customer1
```

vpnPrefix <target:addr/masklen> [moreSpecifics][lessSpecifics][ge <masklen>][le <masklen>]

Matches a VPN prefix, which is composed of a route distinguisher (RD) plus a prefix; see [Chapter 8, “VPN Routing”](#) for a description of RD 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 192.168.0.36:65522:101:10.2.0.0/16
vpnPrefix 192.168.0.36:65522:101:10.2.0.0/16 moreSpecifics
vpnPrefix 192.168.0.36:65522:101:10.2.0.0 ge 16
vpnPrefix 192.168.0.36:65522:101:10.2.0.0 ge 16 le 24
```

5 Network Planning

This chapter describes how to use Route Analytics Management System to plan for network growth and change.

Chapter contents:

- [About the Network Planning Tools](#) on page 220
- [Working with Planning Reports](#) on page 259
- [Understanding Planning Reports](#) on page 264
- [Working with Capacity Planning Tools](#) on page 279


About the Network Planning Tools

The Route Analytics Management System network planning tools help you identify and eliminate hot spots and avoid potential service failures. You can perform failure analysis and move prefixes among border routers. By combining routing and traffic data, you can view traffic trends and their impact on the available capacity and reliability of the network.

In contrast with other tools that are based only on synthetic models of network activity or limited link utilization measurements, the planning tools in RAMS and RAMS with traffic analysis add-on are based on actual measurements.

To use the Route Analytics Management System planning tools, you enter Planning mode on the routing topology map. In Planning mode, you can view edits, import and export data, or undo changes. In RAMS Traffic, you can also compare network activity before and after applied changes took effect to analyze the differences in traffic measurements that resulted from simulated network modifications. Using Planning Reports, you can analyze how traffic changes across the entire network and on specified nodes, interfaces, exit routers, next-hop ASs, or destination ASs.

To enter Planning mode, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Click the mode icon in the lower left corner of the window and choose the Planning mode icon .


When you enter Planning mode, the options listed in the Planning menu are activated.



If you are recording a BGP VPN topology when you switch to Planning Mode, VRF configurations are automatically discovered based on a heuristic algorithm.

Support is also provided for capacity planning. To access the capacity planning features, you must enter Analysis mode.

To enter Analysis mode to access the capacity planning tools, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Click the mode icon in the lower left corner of the window and choose the Analysis mode icon .
- 3 When you enter Analysis mode, the Capacity Planning item in the Planning menu is activated.

Planning Menu

In Planning mode, use the Planning menu at the top of the routing topology map window ([Figure 93](#)) to perform the network planning tasks described in this chapter. Working in Planning mode, you can simulate changes to the network by editing the topology map. For instance, simulating the addition of a node allows you to see realistic effects of the new router on network activity.



As noted in this section, some of the options found in the Planning menu are for RAMS Traffic only.

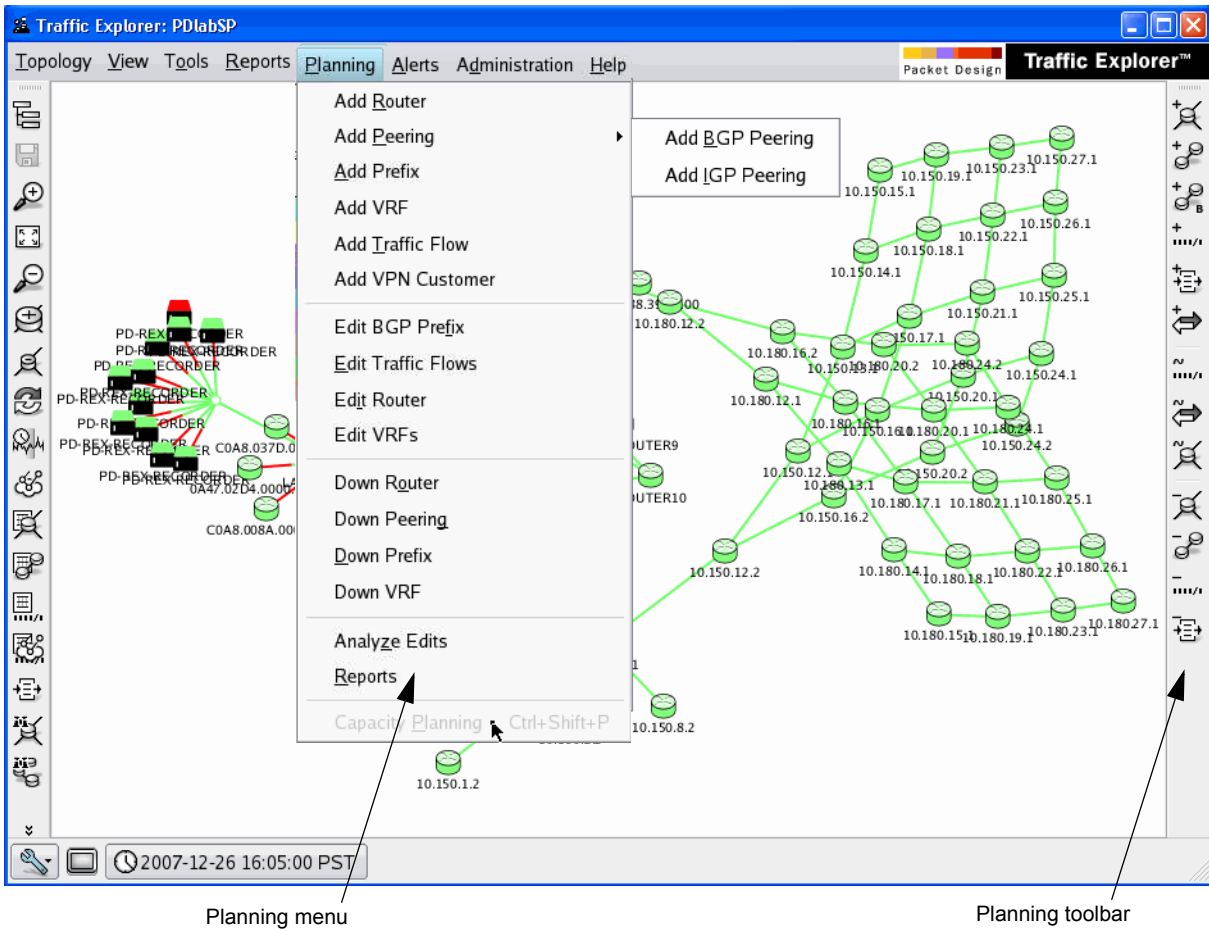


Figure 93 Planning Menu and Toolbar

The Planning menu includes the following items:

- **Add Router**—Places a new node on the topology map.
- **Add Peering**—Creates a peering relationship between two nodes on the topology map.
 - **Add BGP Peering**—Creates an eBGP peering relationship between two nodes on the topology map.
 - **Add IGP Peering**—Creates an IGP peering relationship between two nodes on the topology map.

- **Add Prefix**—Applies prefixes to a router on the topology map. For BGP routers, add prefixes manually or select a filtering method for the prefix.
- **Add OSI Prefix**—Applies OSI prefixes to an OSI ISIS router on the topology map.



The Add OSI Prefix option is available only if OSI ISIS is included on the routing topology map.

- **Add VRF**—Adds Virtual Routing & Forwarding, which allows multiple instances of a routing table to coexist within the same router at the same time. The routing instances are independent, thus allowing the same or overlapping IP addresses to be used without conflicting with each other.



The Add VRF option is available only when VPN is licensed on the appliance and is included in the opened topology.

- **Add Traffic Flow**—Creates one or more flows from one node to another on the topology map. (RAMS Traffic only)
- **Add VPN Customer**—Opens the Add Customer Wizard, which guides you through the process of adding a full mesh, or hub and spoke VPN customer to the network, including VRF routes.



The Add VPN Customer option is available only when VPN is licensed on the appliance and is included in the opened topology.

- **Edit BGP Prefix**—Removes or changes the attributes of a prefix on a particular node on the topology map. Change multiple prefixes at once by selecting more than one prefix from the table.
- **Edit Traffic Flows**—Launches the Edit Flows window, where you can make changes to IPv4 Flows or VPN Flows, including adding, moving, and deleting a flow. (RAMS Traffic only)
- **Edit Router**—Edits the overload bit for an ISIS node.
- **Edit VRFs**—Enables editing of the Virtual Routing and Forwarding router table instances.



The Edit VRFs option is available only when VPN is licensed on the appliance and is included in the opened topology.

- **Down Router**—Changes the state of a node from Up to Down, simulating what would happen if the selected router should fail.
- **Down Peering**—Changes the state of a peer relationship from Up to Down, simulating what would happen if the selected peering should fail. Bring down all the peerings in the table or only selected relationships.
- **Down Prefix**—Changes the state of one or more prefixes from Up to Down on a particular router, simulating what would happen if the selected prefix(es) are withdrawn.
- **Down VRF**—Changes the state of one or more VPN nodes from Up to Down on a particular router, simulating what would happen if the selected item should fail.



The Down VRF option is available only when VPN is licensed on the appliance and is included in the opened topology.

- **Reports**—Launches the Planning Reports window, where the edits made to the topology map display. Analyze, undo, import, and export these edits in the Planning Reports window. Similar reports showing the effect of edits on network traffic are discussed in [Chapter 9, “Traffic Reports”](#) (RAMS Traffic only)
- **Analyze Edits**—Updates all traffic and routing edits simultaneously.
- **Capacity Planning**—Launches the Capacity Reports window, which enables you to view an estimate of what future traffic demands could be like, based on past data that has been collected. This enables you to plan potential expansion of the network in order to meet future demands. See [Working with Capacity Planning Tools](#) on page 279 for more information. (RAMS Traffic only)



You must be in Analysis mode to enable the Capacity Reports option in the Planning menu.


- **Show Edits**—Displays edits that have been made to the topology (present only if the opened topology does not include traffic).

The Planning Toolbar

By default, the Planning toolbar is docked on the right side of the Topology window (Figure 93). You can access planning function from the toolbar, or use the Planning menu, as described in this chapter.

Move the toolbar to the left side or the top or bottom of the window by dragging the dimpled strip at the top of the toolbar. Add and edit elements on the topology map using these buttons.

Table 18 Planning Toolbar

	Add Router	See Add Router on page 226 for more information.
	Add IGP Peering	See Add IGP Peering on page 229 for more information.
	Add BGP Peering	See Add BGP Peering on page 227 for more information.
	Add Prefix	See Add a Prefix on page 230 for more information.
	Add VRF	See Add VRF on page 235 for more information.
	Add Traffic Flow	See Add a Traffic Flow on page 249 for more information. (RAMS Traffic only)
	Edit BGP Prefix	See Edit a BGP Prefix on page 235 for more information.
	Edit Traffic Flow	See Edit Traffic Flows on page 246 for more information. (RAMS Traffic only)
	Edit Router	See Edit Node Properties on page 253 for more information.
	Down Router	See Bring Down a Router on page 254 for more information.
	Down Peering	See Bring Down Peerings on page 255 for more information.
	Down Prefix	See Bring Down a Prefix on page 257 for more information.
	Down VRF	See Bring Down VRF on page 258 for more information.
	Analyze Edits	Select to update all traffic and routing edits simultaneously.

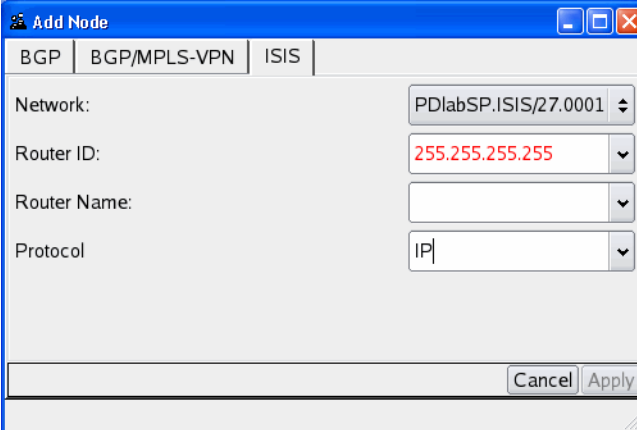
Add Router

Use the Add Router function in Planning mode to simulate the effect of adding one or more nodes to the network. When you add a node, you must specify its protocol and properties. You can then create peering relationships with other nodes on the network as described in [Add Peering](#) on page 227. In RAMS with BGP routers, the node is automatically peered.

You can also add a protocol instance to a node, and this procedure is described in [Adding a Protocol Instance to an Existing Node](#), below.

To add a router, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Add Router** from the Planning menu.
- 3 Click the desired protocol tab ([Figure 94](#)).



The screenshot shows a dialog box titled "Add Node" with a blue header. It has three tabs: "BGP", "BGP/MPLS-VPN", and "ISIS". The "BGP" tab is active. The dialog contains the following fields:

- Network:** A dropdown menu with the selected value "PDlabSP.ISIS/27.0001".
- Router ID:** A dropdown menu with the selected value "255.255.255.255".
- Router Name:** An empty dropdown menu.
- Protocol:** A dropdown menu with the selected value "IP".

At the bottom right of the dialog, there are two buttons: "Cancel" and "Apply".

Figure 94 Add Node

- 4 The network you are currently editing appears in the first text box. If necessary, click the down arrow to choose a different network from the drop-down list. The node will be added to the topology of the network specified in the text box.
- 5 Specify the Router ID or System ID (for OSI ISIS routers) in the field provided.

- 6 Type a name for the node in the Router Name text box.
- 7 (ISIS only) Select the network layer protocol for the node from the **Protocol** drop-down list.
- 8 Click **Apply** to save the node.

Adding a Protocol Instance to an Existing Node

You can add a protocol instance to an existing node by using a procedure similar to the Add a Node procedure, above.

To add a protocol instance to an existing node, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Add Router** from the Planning menu.
- 3 Click a node on the topology map.
- 4 Choose a protocol to add to the node.
- 5 Click **Apply**.

Add Peering

You can create peerings between two nodes to simulate the effect that the specified relationship would have on the network.

Add BGP Peering

To Add a BGP peering, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Add Peering** → **Add BGP Peering** from the Planning menu.

- 3 Click a node on the topology map to specify the source node for the new peering (Figure 95).

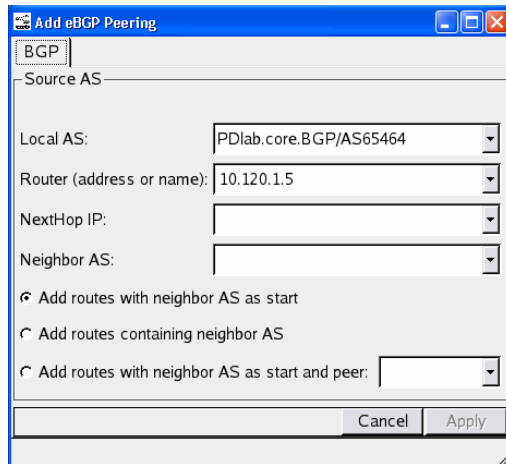


Figure 95 Add eBGP Peering

- 4 The AS you are currently editing appears in the Local AS text box. If necessary, click the down arrow to choose a different AS from the drop-down list. The peering will be added to the topology of the AS specified in the text box.
- 5 In the Router text box, specify the IP address or name of the source node in the peering.
- 6 In the NextHop IP text box, type or choose the next hop IP address of the source node.
- 7 The Neighbor AS text box is populated with the Neighbor AS number you are creating a peering for. You may edit this box by either entering other neighboring AS numbers, or selecting an AS number from the drop-down menu.
- 8 Select one of the following options:
 - Add routes with neighbor AS as start.
 - Add routes containing neighbor AS.
 - Add routes with neighbor AS as start and peer.
- 9 Click **Apply**.

Add IGP Peering

Create an IGP peering between two nodes to simulate the effect this relationship would have on the network.

To create an IGP peering, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Add Peering** → **Add IGP Peering** from the Planning menu.
- 3 Click a node on the topology map to specify the source node for the new peering.
- 4 Click a node on the topology map to specify the destination node for the new peering (Figure 96).

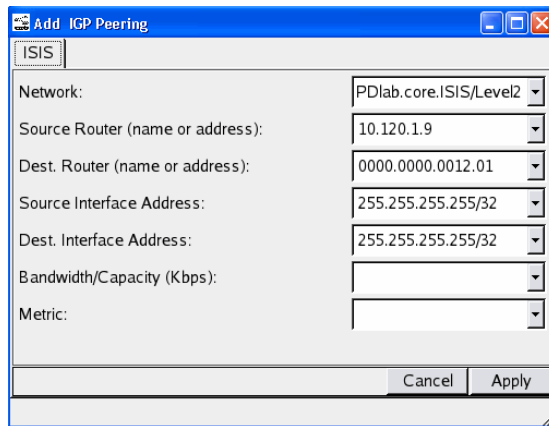


Figure 96 Add IGP Peering

- 5 The network you are currently editing appears in the Network text box. If necessary, click the down arrow to choose a different network from the drop-down list. The peering will be added to the network specified in the text box.
- 6 The Source Router text box is populated with the IP address or name of the source node in the peering. Edit this text box if necessary.
- 7 The Dest Router text box is populated with the IP address or name of the destination node in the peering. Edit this text box if necessary.

- 8 The Source Interface Address text box is populated with the default IP address. Replace the default value with the address of the source interface. This address can be followed by a mask length, such as 192.168.1.101/24.
- 9 The Dest Interface Address text box is populated with the default IP address. Replace the default value with the address of the destination interface. This address can be followed by a mask length, such as 192.168.1.101/24.
- 10 Enter or select the amount of available bandwidth allocated for this peering in the Bandwidth/Capacity text box.
- 11 Enter or select the metric value for the peering.

Metric values help traffic determine the best path to take through the network and typically take bandwidth, communication cost, delay, hop count, load, and reliability into consideration.
- 12 Click **Apply**.

Add a Prefix

Simulate the effect of adding one or more prefixes to the topology by using the Add Prefix function. When you add a prefix, its attributes can be specified manually or by using a filter.

To begin adding a prefix, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Add Prefix** from the Planning menu.
- 3 Click a node on the topology map to specify the router that will advertise the prefix. You can move the prefix later, if necessary.
- 4 Choose a protocol for the prefix by clicking the appropriate tab.

Adding a Prefix for BGP or BGP/MPLS-VPN Routers

If you select the BGP or BGP/MPLS-VPN tab in the Add Prefix window, use one of these methods:

- Type the attributes of the prefix manually.
- Use one or more filtering methods.

To manually add a prefix, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Planning** → **Add Prefix** and click a node on the map to specify the router that will advertise the prefix.
- 3 Click the **Manually** radio button option at the top of the Add Prefix window. (This is selected by default when you click **Add Prefix**).
- 4 The topology you are currently editing appears in the Network text box. If necessary, click the down arrow to choose a different network from the drop-down list.
- 5 In the Router text box, type the IP address or name of the router that advertises the prefix.
- 6 In the Type text box, enter the peer type of the router.
- 7 In the RD (route distinguisher) field, select the VRF label for the prefix. (BGP/MPLS-VPN only)
- 8 In the MPLS Label field, select the label for the prefix. (BGP/MPLS-VPN only)
- 9 In the Prefix text box, type the address of the new prefix.
- 10 Set the attributes of the prefix by specifying Origin (which needs to be populated with one of three strings—IGP, BGP, or Incomplete, AS Path, the NextHop IP address, the Local Pref (optional), MED value (optional), and Originator ID (this attribute displays only if the originating node is BGP).
- 11 Click **Apply**.

To add a prefix using a filter, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Add Prefix** from the Planning menu and click the desired node to open the Add Prefix window.
- 3 Click **Using Filter** at the top of the window.
- 4 In the **RD** (route distinguisher) field, select the VRF label for the prefix. (BGP/MPLS-VPN only)

- In the MPLS Label field, select the label for the prefix. (BGP/MPLS-VPN only)

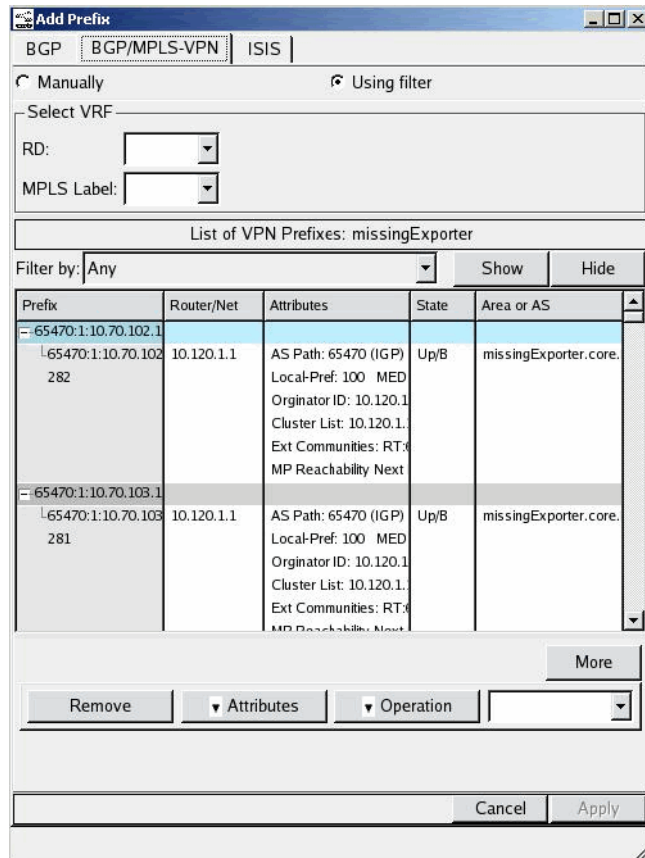


Figure 97 Using Filters Radio Button

- Use the **Filter by** drop-down list to choose which prefixes to show or hide in the table.

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 [Using Filters](#) on page 195 in [Chapter 4, “The History Navigator”](#) for examples of the parameter syntax using filter expressions described in [Expression Syntax](#) on page 199.



With a simple filter, you type 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.

You can choose two or more different operators from a list and specify their corresponding parameters to be matched or excluded. The Composing Advanced Filter window opens when **Advanced** is selected.

Filter expressions let you manually enter a filter expression that is too complex to be set up with either simple or advanced filter menus.

See [Using Filters](#) on page 195 in [Chapter 4, “The History Navigator”](#) for more detailed information.

- 7 Click **Show** to list only items that match the parameters of the filter, or click **Hide** to list only items that do not match the parameters of the filter.
- 8 Click on a prefix in the table to highlight it.
- 9 Choose a filtering method for the highlighted prefix from the **Attributes** drop-down list and type a corresponding value in the text box to the right.
- 10 Use the **Operation** drop-down list to **Set**, **Append** or **Prepend** the value to the corresponding attribute of the prefix.

For example, to set the local preference value of the highlighted prefix to 99, choose **Local Pref** from the Attributes list, type 99 in the text box and choose **Set** from the Operation list.
- 11 Click **More** to apply additional filtering methods to the prefix or **Remove** to remove the last filtering method applied to the prefix.
- 12 Click **Apply**.
- 13 Click **Close (X)** to close the window.

Add prefix for ISIS Routers

If you chose the **ISIS** tab in the Add Prefix window, the Add Prefix window opens:

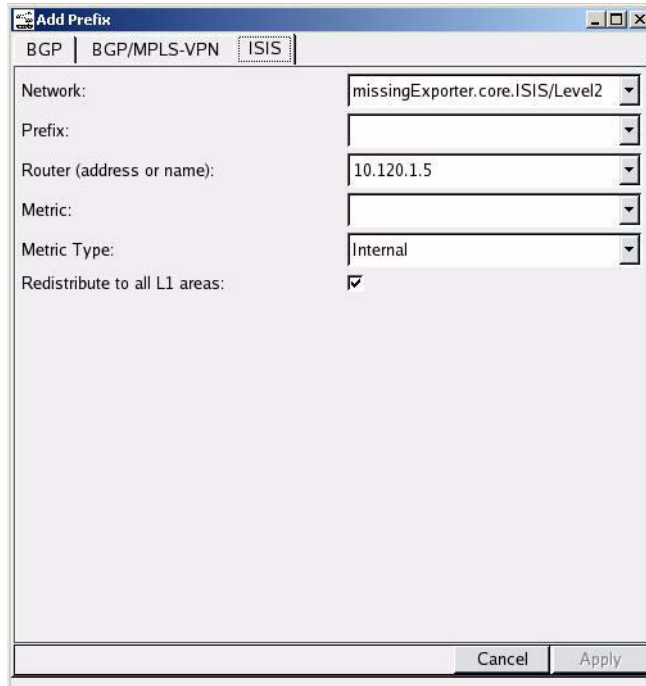


Figure 98 Add Prefix (ISIS)

To add a prefix to an ISIS router, perform the following steps:

- 1 Follow the steps for [Add a Prefix](#) on page 230.
- 2 Click an ISIS router on the topology map.
- 3 The network you are currently editing appears in the Network text box. If necessary, click the down arrow to choose a different network from the drop-down list.
- 4 Type the address of the new prefix in the Prefix text box.
- 5 The Router text box is populated with the system ID or name of the node that advertises the prefix. Edit this text box if necessary.
- 6 Enter a valid metric according to the metric type.

- 7 Select the check box to redistribute to all L1 areas.
- 8 Click **Apply**.

Edit a BGP Prefix

You can edit an existing BGP prefix using many of the same steps described in [Add a Prefix](#) on page 230.

To edit a BGP prefix, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit BGP Prefix** from the Planning menu.
- 3 Click the router on the topology map that advertises the prefix to edit.

The network you are currently editing appears in the Network text box. If necessary, choose a different network from its drop-down menu.

The Router (address or name) text box is populated with the IP address or name of the node in the prefix. The Type text box is displayed if the originating prefix is BGP.

- 4 Use the **Filter By** drop-down list to select the prefix you want to modify, as described in [Add a Prefix](#) on page 230.
- 5 Click **More** to create further modifications to prefix attributes and the **Remove** button to create fewer modifications to prefix attributes.
- 6 Modify the **Attributes** of the displayed prefix.
- 7 Use the **Operation** drop-down list to **Set** or **Prepend** the modification to an existing prefix.
- 8 Click **Apply**.

Add VRF

Adding a VRF to a PE allows multiple instances of a routing table to coexist within the same router at the same time. The routing instances are independent, allowing the same or overlapping IP addresses to be used without conflicting with each other.



This option is enabled if your appliance is licensed for VPN, and if VPN protocol is present in the opened topology.

To add a VRF to a PE, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Add VRF** from the Planning menu.
- 3 On the topology map, click a VPN node that is to be the PE for the VRF.

The network you are currently editing appears in the Network text box. If necessary, click the down arrow to choose a different network from the drop-down list.

The screenshot shows a dialog box titled "Add VRF to PE" with a tab labeled "BGP/MPLS-VPN". The dialog contains the following fields and controls:

- Network:** A dropdown menu with the selected value "PDlab.core.BGP/AS65464/VPN".
- Router (address or name):** A dropdown menu with the selected value "10.120.1.4".
- Name:** An empty text input field.
- RD:** An empty text input field.
- RT Import Policy:** An empty text input field.
- RT Export Policy:** An empty text input field.
- MPLS Labels:** An empty text input field.

At the bottom right of the dialog are two buttons: "Cancel" and "Apply".

Figure 99 Add VRF to PE

- 4 Enter the router that identifies the VRF in the Router field.
- 5 Enter a name for the VRF in the Name field.
- 6 Enter a list of RTs in the RT Import Policy field.
- 7 Enter the RTs that attaches to router when in the RT Export Policy field.
- 8 Enter the MPLS label to attach to the exporting router in the MPLS Labels field.

- 9 Click **Apply** to save the information.

Add IPv4 Traffic Flow



This section applies to RAMS Traffic only.

You can add IPv4 traffic flows to the topology map using the Add Traffic Flow function. When adding a traffic flow, specify the source and destination prefixes as well as the bandwidth for the flow. To add more than one flow at a time, use the Multiple Flows tab. Edit existing flows using the Edit Flows window as described in [Edit Traffic Flows](#) on page 246.

To add an IPv4 traffic flow, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Add Traffic Flow** from the Planning menu.



You can also add traffic flow in the Edit Traffic Flows window using the **Add Flow** button described in [Edit Traffic Flows](#) on page 246.

- 3 Click a node on the topology map to open the Add Traffic Flow window ([Figure 100](#)).

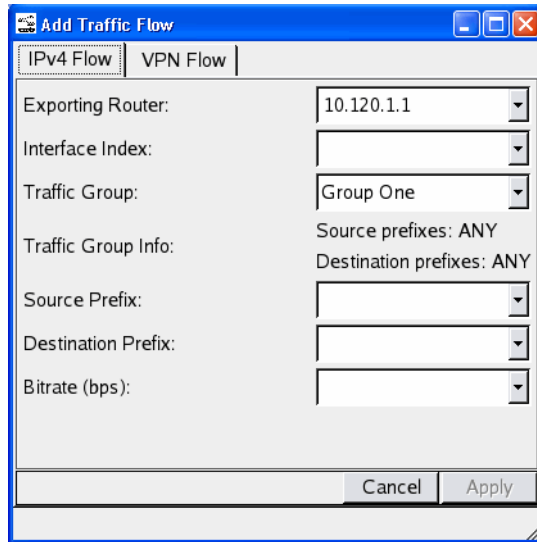


Figure 100 Add Traffic Flow-IPv4 Tab

- 4 Select the **IPv4 Flow** tab to add an IPv4 traffic flow to the node you previously selected.
- 5 In the Exporting Router text box, the address of the router chosen on the topology map appears. Choose another router by entering its address in the text box or by clicking the down arrow to select one from the drop-down list.
- 6 In the Interface Index text box, type the value of the interface index to associate with the traffic flow.
- 7 Select the traffic group you want the IPv4 traffic flow to go to from the **Traffic Group** drop-down menu.

In the Traffic Group Info section, the source and destination information reflect what was configured for the Traffic group (the traffic group selected in the previous step). You can view the configuration of these groups from the Traffic Groups web page or in the Traffic Reports window under the Traffic Group Definition column.

- 8 Type the address of the prefix where the new traffic flow originates in the Source Prefix text box.
- 9 Type the address of the destination prefix for the new traffic flow in the Destination Prefix text box.

- 10 Enter the bitrate of the new traffic flow in the Bitrate text box.
- 11 Click **Apply**.

Add VPN Traffic Flows



This section applies to RAMS Traffic only. The appliance must be licensed for VPN, and the open topology must contain VPN protocol for this option to be enabled.

The appliance supports the following methods to identify the source and destination of a VPN traffic flow:

- **PE-PE Flow**—Allows you to specify the ingress and egress PEs for the flow, without the flow belonging to a specific customer. An unspecified customer is created in the background for such flows, along with any necessary VRFs and PEs for that customer on its PEs, and a flow is created from the ingress PE to the egress PE with source and destination prefixes of 0/0. You can also specify the CoS and bitrate for the flow.
- **Customer Flow**—Allows you to specify the information necessary to determine the ingress VRF of a flow along with its destination prefix, at which point the existing VPN topology is used to determine its egress PE and VRF. Enter the necessary information to determine the ingress VRF of the flow. The destination prefix is then combined (specifically the import RTs of the ingress VRF) to determine the egress PE and egress VRF of the flow. When enough information is If there is no VPN prefix for the ingress VRF and destination prefix combination, you will be notified and no flow will be entered.
- **VRF Flow**—Allows you to specify the more explicit details of the flow, specifically the egress PE and egress VRF, which are automatically determined in the Customer flow. If there is no VPN prefix for the ingress VRF and destination prefix combination, you will be notified and no flow will be entered.

To add a VPN PE-PE traffic flow, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.

- 2 Choose **Edit Traffic Flows** from the Planning menu.
- 3 Select the VPN Flows tab and click **Add Flow**. If there is only one type of flow, tabs are not displayed.



The PE-PE flow is the default selection.

Figure 101 Add PE-PE Selection for VPN Traffic Flow

- 4 Select the way you want to specify the flow by selecting either Customer Flow or VRF Flow, or leaving the selection at PE-PE flow.
- 5 Select the IP addresses for the Ingress PE and Egress PE from the drop-down menus.
- 6 Select the **Class of Service** you want from the drop-down menu.
- 7 Enter the bitrate from the **Bitrate** drop-down menu.
- 8 Select **Apply** to save the information.

To add a VPN customer flow, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Traffic Flows** from the Planning menu.

- 3 Select the VPN Flows tab and click **Add Flow**.
- 4 Select the **Customer Flow** radio button.

The screenshot shows a window titled "Add Traffic Flow" with a blue header. Below the header, there are two tabs: "IPv4 Flow" and "VPN Flow", with "VPN Flow" being the active tab. Underneath the tabs, there are three radio buttons: "PE - PE Flow", "Customer Flow" (which is selected), and "VRF Flow". The main area of the window contains several fields, each with a dropdown arrow on the right: "Customer:", "Ingress PE:", "Ingress VRF:", "Source Prefix:", "Destination Prefix:", "Class of Service:" (with the value "0" visible), "Bitrate:", and "Egress PE:". At the bottom right of the window, there are two buttons: "Cancel" and "Apply".

Figure 102 Add Customer Flow Selection for VPN Traffic Flow

- 5 Select the customer from the drop-down menu.
- 6 Select IP addresses for the ingress PE and egress PE from the drop-down menus.
- 7 Enter the source and destination IP prefixes for the traffic that you want to identify drop-down menus.
- 8 Select the **Class of Service** from the drop-down menu.
- 9 Enter the bitrate from the **Bitrate** drop-down menu.
- 10 Select **Apply** to save the information.

To Add a VRF Flow, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Traffic Flows** from the Planning menu.
- 3 Select the VPN Flows tab and click **Add Flow**.
- 4 Select the **VRF Flow** radio button.

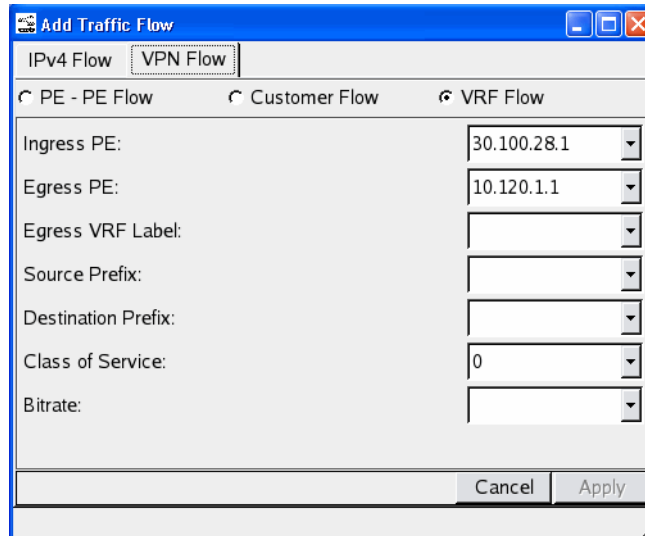


Figure 103 Add VRF Flow Selection for VPN Traffic Flow

- 5 Select IP addresses for the ingress PE and egress PE from the drop-down menus.
- 6 Enter or select a label to identify the egress VRF.
- 7 Enter the source and destination IP prefixes for the traffic that you want to identify drop-down menus.
- 8 Select the **Class of Service**.
- 9 Enter the bitrate from the **Bitrate** drop-down menu.
- 10 Select **Apply** to save the information.

Add VPN Customer

You can add VPN customers easily using the **Add VPN Customer** option. This is a wizard-based operation, which seamlessly takes you through the add customer process.



This option is enabled if your appliance is licensed for VPN, and if VPN protocol is present in the opened topology.

To add a VPN customer to the topology, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Add VPN Customer** from the Planning menu.
- 3 Enter the customer name in the Customer field.
- 4 Select the VPN topology for this customer by clicking on either the **Full Mesh** or **Hub-and-Spoke** radio buttons.

Two columns are shown and identified below each column: **Available PEs** is on the left, and **Selected PE's** is shown on the right. Both have Select (RegEX) and a drop-down menu at the top of each column.

- 5 Select the available PE's for this customer by double-clicking on the PE or by clicking on the PE, and then clicking on the right-arrow (->) shown between the columns.

If you selected Full Mesh in Step 4, the Select Customer RTs window opens. Continue to Step 6.

If you selected Hub-and-Spoke in Step 4, continue to Step 7 where you will be selecting Hub-and-Spoke PE's in the Define Hub-and Spoke Configuration window.

- 6 If you selected Full Mesh in Step 4, enter the customer's RTs in the **Full Mesh RTs** text box in the Select Customer RTs window, click **Next** and continue to Step 8 and to the Add Customer Routes window.
- 7 If you selected Hub-and-Spoke in Step 4, the Define Hub-and Spoke Configuration window opens. Two columns display: the column on the left displays Hub PEs at the bottom of the column, and the column on the right displays Spoke PEs at the bottom of its column. Select the Hub and Spoke PE's, and click **Next** to continue.

The Add Customer Routes window opens.

- 8 Enter the prefix range used by the routes in this VPN topology in the Prefix Range text field, and click **Next**.

The Select VPN Traffic Sources window opens.

- 9 Choose either the **All PEs** radio button if you want all customer PEs selected as VPN traffic sources, or select the **Specify PEs** radio button to select specific sources, selecting them from the **Available Routers** column (shown on the left), and click **Next**.

The Select VPN Traffic Destinations window opens.

- 10 Choose either the **All PEs** radio button if you want all customer PEs selected as VPN traffic destinations, or select the **Specify PEs** radio button to select specific destinations, and select them from the Available Routers column (shown on the left), and click **Next**.

The Specify Traffic Flow Distribution window opens.

- 11 Enter the Class of Service from the corresponding drop-down menu.
- 12 Enter the average bitrate per flow in the corresponding text box.
- 13 Select the distribution type from the following three choices: Equal, Uniform, and Pareto.
- 14 Click **Next**.

The Review Traffic Flow Distribution window opens.

- 15 Review the information you entered in the previous screen. You can go back to previous screens to edit what you entered in previous steps. You can also edit the CoS and bitrate of the flows shown on the Review Traffic Flow Distribution window. When you are satisfied with the information shown and have added all the flow distributions that you want, click **Next**.

The Review Customer Topology window opens.

- 16 If desired, edit the information shown within the following tabs:
 - VRFs:** Name
 - VPN Prefixes:** AS Path, Local Pref, MED
 - VPN Flows:** Cos, Bitrate.
- 17 Click **Finish** when you are done editing the Review Customer Topology window.

Edit BGP Prefixes

You can modify BGP prefixes from the Planning menu.

To change a prefix, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.

- 2 Choose **Edit BGP Prefix** from the Planning menu.
- 3 Click a router on the topology map that advertises the prefix you want to change.
- 4 The Change Prefixes window opens to show the following columns of information:
 - The **Prefix**—Displays prefixes on the topology map.
 - The **Router/Net**—Lists the router that advertises the prefix and current topology name.
 - The **Attributes**—Displays prefix attributes, such as AS path, Local preference, and next hop IP addresses.
 - The **State**—Displays the current state of the prefix (such as Up or Down).
 - The **Area or AS**—Displays the AS of the network.
- 5 Use the **Filter By** drop-down list to select the prefix you want to modify. There are three levels of filtering:
 - a Simple filters let you choose a single operator (such as “router”) from the drop-down list and specify one or more parameters (such as router IP addresses or names) to be matched or excluded.
 - b Advanced filters let you choose two or more different operators from a list and specify their corresponding parameters to be matched or excluded.
 - c Filter expressions let you manually enter a filter expression that is too complex to be set up with either simple or advanced filter menus.
 - The Show button will list only items that match the parameters of the filter.
 - The Hide button will list only items that do not match the parameters of the filter.
- 6 Click on a prefix in the table to highlight it.
- 7 Choose a filtering method for the highlighted prefix from the **Attributes** drop-down list and type a corresponding value in the text box at the right of the screen.

- 8 Use the **Operation** drop-down list to **Set**, **Append**, or **Prepend** the value to the corresponding attribute of the prefix.

For example, to set the local preference value of a prefix to 99, choose **Local Pref** from the **Attributes** list, type 99 in the text box, and choose **Set** from the Operation list.

- 9 Click **Apply**.

Edit Traffic Flows



This section applies to RAMS Traffic only.

The ability to edit IPv4 and VPN traffic flows in Planning mode allows you to plan the most effective routing scenario for your network. You can manipulate traffic flows using the functions available in the Edit Traffic Flows window.

To edit IPv4 traffic flows, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Traffic Flows** from the Planning menu.

The screenshot shows the 'Edit Traffic Flows' window with the 'IPv4 Flows' tab selected. The window title is 'Edit Traffic Flows'. Below the tabs, there is a section titled 'Edit IPv4 Traffic Flows'. A 'Filter by:' dropdown is set to 'Any', with 'Show' and 'Hide' buttons to its right. Below this is a table with the following columns: Source Prefix, Destination Prefix, Exporting Router, Traffic Group, and Bit Rate (bps). The table contains six rows of data. At the bottom of the window, there is a status bar showing '341 entries' and several action buttons: 'Flow Server', 'Add Flow', 'Change', 'Delete', 'Move', and 'Close'.

Source Prefix	Destination Prefix	Exporting Router	Traffic Group	Bit Rate (bps)
10.64.12.0/24	10.73.6.0/24	10.120.13.2	Other	1.91M
10.64.12.0/24	12.90.1.0/24	10.120.13.2	Other	1.91M
11.92.2.0/24	10.64.10.0/24	10.120.13.2		6.44K
11.91.2.0/24	10.64.10.0/24	10.120.13.2		6.44K
11.91.2.0/24	10.64.10.0/24	10.120.13.2		6.44K
11.91.2.0/24	10.64.10.0/24	10.120.13.2		6.44K

Figure 104 Edit Traffic Flows

- 3 Limit the list of traffic flows shown using the **Filter by** drop-down list. Filter by the following choices: Any, Source, Destination, Flow Exporter, or use the Advanced Filtering window.

You can perform the following functions using the Edit IPv4 Traffic Flows window. At the bottom of this window, select from the following buttons:

- **Flow Server:** Select this to open the Add Flow Distribution window. See [Add a Flow Server](#) on page 247 for more information.
- **Add Flow:** Select this to invoke the Add IPv4 Traffic Flow window. See [Add a Flow Server](#) on page 247 for more information.
- **Change:** Choose from two options: **All** will invoke the Change flow bitrate to window, where you can edit all flows. Choose **Selected**, and the **Bitrate** column in the Edit IPv4 Traffic flow window becomes editable. See [Change the Bitrate of a Flow](#) on page 249 for more information.
- **Delete:** Delete one or more flows by pressing this button. See [Delete a Flow from a Router](#) on page 250.
- **Move:** Change the exporting/ingress router for one or more traffic flows by pressing this button. See [Move a Traffic Flow from One Router to Another](#) on page 250 for more information.

Add a Flow Server

You can add flow servers from the Planning menu.

To add a flow server, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Traffic Flows** from the Planning menu.
- 3 Click **Flow Server** at the bottom of the Edit IPv4 Traffic Flows window to add a flow server to the simulated network.

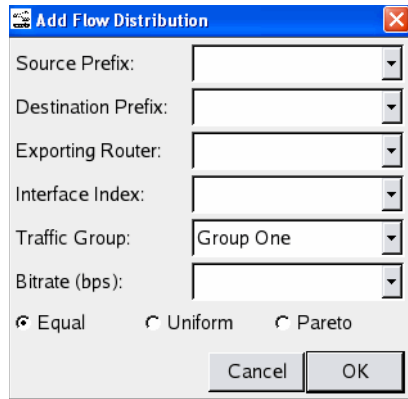


Figure 105 Add Flow Distribution

- 4 Enter the source prefix, destination prefix, exporting router, interface index, traffic group, and bitrate (bps) of the new server in the appropriate text boxes.
- 5 Choose how traffic will flow from the new server to its clients by clicking **Equal**, **Uniform** or **Pareto**.
 - **Equal** traffic distribution means that each flow has the average bitrate entered in the previous step.
 - **Uniform** traffic distribution means that each flow has an equal probability of having any bitrate from 0 bps to twice the bitrate entered in the previous step.
 - A **Pareto** distribution is that in a flow distribution, a small number of flows will have a high bitrate, while most of the flows will have a lower bitrate. The average bitrate of the flows generated will be equal to the bitrate that was entered in the previous step.
- 6 Click **OK**.

Add a Traffic Flow

See [Add IPv4 Traffic Flow](#) on page 237 for instructions.

Change the Bitrate of a Flow

Edit the bitrate of a flow to increase or decrease the amount of traffic flowing through the network. Bitrate is in bits per second (bps).

To change the bit rate of a flow, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Traffic Flows** from the Planning menu.
- 3 Click a flow in the table to highlight it.
Hold down the **CTRL** key and click to highlight more than one flow at a time.
- 4 Right-click the highlighted flows and choose **Change Flow**.

You can also perform this function using the Change button at the bottom of the Edit IPv4 Traffic Flows window. Choose **Selected** to change the bit rate in only highlighted flow or **All** to change every flow shown in the table.

- 5 Configure the following values:
 - **Set (bps)**—Assigns a single bitrate value to specified traffic flows. For example, to set the bitrate of specified flows to 5, click **Set** and type 5 in the text box.
 - **Scale (decimal)**—Multiplies the bitrate by N, where N is the value you supply. For example, to triple the bitrate of all highlighted traffic flows, click **Scale** and type 3 in the text box. A bitrate of 2 bps is now 6 bps. A bitrate of 10 bps is now 30 bps.
 - **Add (bps)**—Increases the bitrate of highlighted traffic flows by adding N to the current value, where N is the value you supply. For example, to increment all selected flows by 5, click **Add** and type 5 in the text box. A bitrate of 2 bps is now 7 bps. A bitrate of 10 bps is now 15 bps.
 - **Add Proportional (bps)**—Increases the bitrate of highlighted flows so the total bitrate of the set of flows is equal to N (where N is the value you supply). For example, to increase the total bitrate of a set of flows from an exporting router to equal 200, click **Add Proportional** and type

200 in the text box. Each highlighted flow is proportionally increased based on its original value. A set of three flows with bitrates of 103 bps, 23 bps, and 7 bps are increased to 155 bps, 35 bps, and 10 bps.

- 6 Click **OK** to save your changes.

Delete a Flow from a Router

Remove one or more traffic flows from the Edit IPv4 Traffic Flows window. The flow will be removed from the topology.

To delete a flow from a router, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Traffic Flows** from the Planning menu.
- 3 Click a flow in the table to highlight the flow.

Hold down the **CTRL** key and click to highlight more than one flow at a time.

- 4 Right-click the highlighted flow(s) and choose **Delete Flow** from the pop-up menu.

You can also perform this function using the **Delete** button at the bottom of the Edit Flows window. Choose **Selected** to delete only highlighted flows or **All** to delete every flow in the table.

- 5 Click **Yes** to complete deletion or click **No** to cancel.



Undo the deletion using the Planning Reports window List of Edits, as described in the [Working with Planning Reports](#) section.

Move a Traffic Flow from One Router to Another

This procedure allows you to change the exporting/ingress router for one or more traffic flows.

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Traffic Flows** from the Planning menu.
- 3 Click a flow in the table to highlight the flow.

Hold down the **CTRL** key and click to highlight more than one flow at a time.



Use the **Filter by** drop-down menu to limit the list of results that display.

- 4 Right-click the highlighted flow(s) and choose **Move flow** from the pop-up menu.

You can also perform this function using the **Move** button at the bottom of the Edit Flows window. Choose **Selected** to move only highlighted flows or **All** to move every flow in the table.

- 5 Type the address of the router where you'll move the traffic flow.
- 6 Type the interface index for the traffic flow exporter.
- 7 Click **OK** to save your changes.

Edit VPN Traffic Flows



This section applies to RAMS Traffic only. This option is enabled if your appliance is licensed for VPN, and if VPN protocol is present in the opened topology.

To edit VPN traffic flows, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Traffic Flows** from the Planning menu.
- 3 Select the **VPN Flows** tab to open the Edit VPN Traffic Flows window.

Source Prefix	Destination P	Ingress P/PE	Egress PE	Egress VRF L	Class of Service	Bit Rate (bps)
10.70.103.1/3	10.120.25.1/3	10.120.1.2:1	10.120.1.9	48	0	755.63K
10.120.79.1/3	10.120.29.1/3	10.120.1.2:1	10.120.1.9	49	0	755.59K
10.70.112.0/2	10.111.112.0	10.120.1.1:4	10.120.1.7	1163	0	401.90K
10.70.102.1/3	10.111.1.1/32	10.120.1.1:4	10.120.1.7	1161	2	399.61K
10.70.103.1/3	10.111.2.1/32	10.120.1.3:1	10.120.1.7	1160	3	399.49K
10.70.104.1/3	10.111.3.1/32	10.120.1.1:4	10.120.1.7	1159	0	399.25K

Figure 106 Edit VPN Traffic Flows

This window displays all of the VPN traffic flows currently running in the system. At the bottom of this window are the following buttons:

Add Flow: Select this to invoke the Add VPN Traffic Flow window. See [Add a Flow Server](#) on page 247 for more information.

Change: Select this to change the bitrate of all flows in the table, or all flows currently selected in the table. See [Change the Bitrate of a Flow](#) on page 249 for more information.

Delete: Select this to delete the bitrate of all flows in the table, or all flows currently selected in the table. See [Delete a Flow from a Router](#) on page 250 for more information.

VPN Filter: Select this to filter all of the flows in the window.

Close: Select this to close the window.

Using the VPN Filter

Use this window to display a subset of VPN Traffic Flows.

To use the VPN Filter, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Traffic Flows** from the Planning menu.

- 3 Click **VPN Filter** to edit the VPN filters.

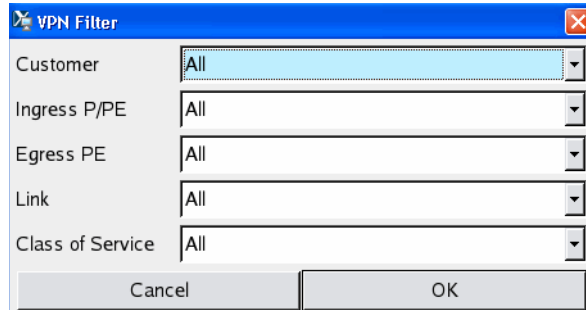


Figure 107 VPN Filter

- 4 Select values from the drop-down menus, or select **All**.
- 5 Click **OK**.

Edit Node Properties

Use this option to set the overload bit for ISIS routers.

To edit a node, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Edit Router** from the Planning menu.
- 3 On the topology map, select the node you wish to edit.

The network information appears in the Network field, and the router's address or name will display in the Router field.

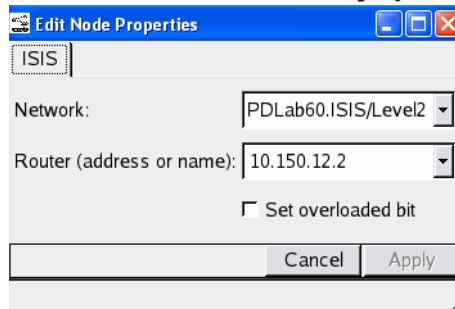


Figure 108 Edit Node Properties

- 4 Select **Set overloaded bit** to disable the transit traffic from being routed, and click on **Apply**.

Edit VRFs



This option is enabled if your appliance is licensed for VPN, and if VPN protocol is present in the opened topology.

To edit a VRF, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.

- 2 Choose **Edit VRFs** from the Planning menu.

The Edit VRFs window opens to show all of the VRFs in the current VPN topology.

- 3 To edit an entry, click the box in which the entry appears.



Edited values are shown in purple. PE, RD, and AS cannot be edited.

- 4 Click **Apply** to apply the VRF edits.



VRF parameters are cleared when you exit Planning Mode.

Bring Down a Router

The Down Router function changes the state of a node from up to down, simulating the impact on network activity should the selected router fail.

To bring down a router, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.

- 2 Choose **Down Router** from the Planning menu.

- 3 On the topology map, click a node to bring down.

As an alternative to steps 1 and 2, you can right-click a node to bring up its information panel, then click **Down** on the panel.

The node turns red, indicating that its state is Down.



To bring down a single IGP protocol instance on a node, right-click on the node to bring up its information panel, select the appropriate tab, and then click **Down**.

- 4 To bring a node back up, right-click it.

The node information panel for the node appears.

- 5 Click **Up** for each protocol tab shown on the node information panel.

The node is no longer red, indicating that its state is Up.

Bring Down Peerings

The Down Peering function changes the state of a peer relationship from up to down, simulating the impact on network activity should the selected relationship fail.

For BGP protocol, the peerings from and to the NextHop are taken down. For OSPF and ISIS protocols, both halves of the duplex link are taken down. For the EIGRP protocol, only one half is taken down, but note that all peers of the selected interface are brought down as well.

To bring down a peering, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Down Peering** from the Planning menu.
- 3 On the topology map, click the node whose peering you want down.
- 4 Click the tab for the appropriate protocol.

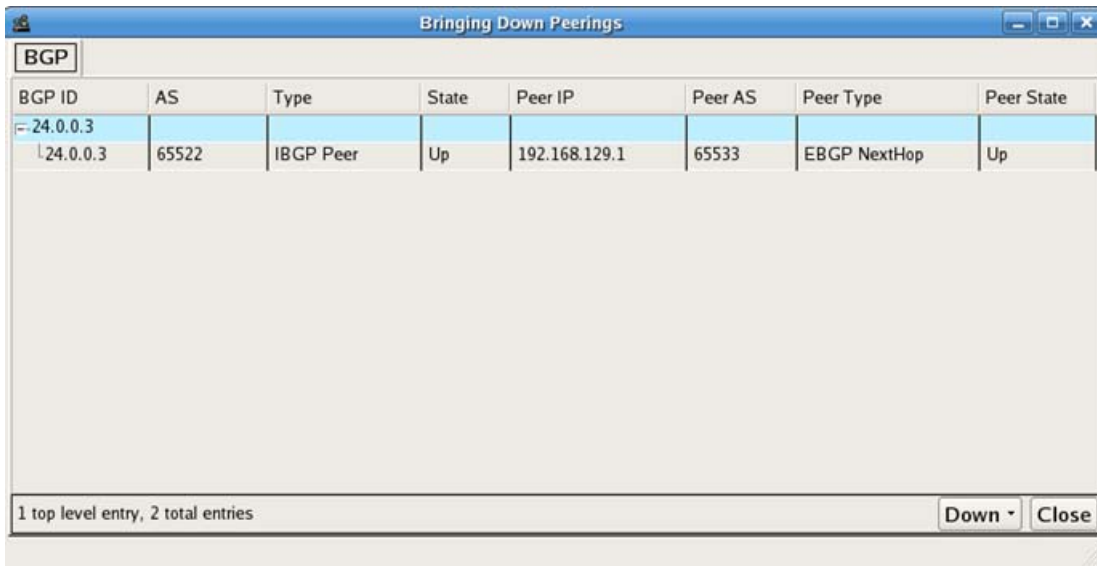


Figure 109 Bringing Down Peerings

- 5 Click on a peering to highlight it in the table.
- 6 Click **Down** or right-click the peering(s).
- 7 Choose **All** to bring down all peerings in the table or **Selected** to bring down only highlighted peering(s).
- 8 Click **Yes** to complete the process of bringing down the peering(s). Click **No** to return to the Bringing Down Peerings window without bringing down the peering(s).
- 9 Click **Close** to close the window.



Alternatively, you can bring down a peering by right-clicking a link to bring up its information panel, then clicking **Down** on the panel.

Bring Down a Prefix

The Down Prefix function changes the state of a prefix from up to down, simulating the impact on network activity should the selected prefix be withdrawn.

To bring down a prefix, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Down Prefix**.
- 3 On the topology map, click the node that advertises the prefix you'll bring down.
- 4 Click the tab for the protocol.

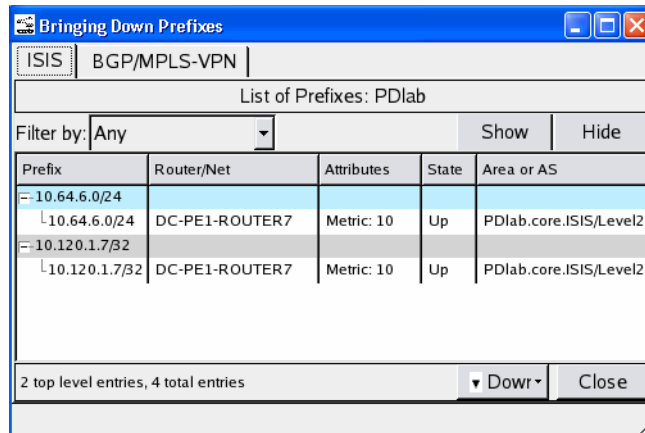


Figure 110 Bringing Down Prefixes

- 5 Use the **Filter By** drop-down list to choose the attributes you'll use to narrow the list of prefixes shown in the table. For more information about choosing a filter, see [Add a Prefix](#) on page 230.
- 6 Click **Show** to list only items that match the parameters of the filter, or click **Hide** to list only items that do not match the filter parameters.
- 7 Click a line in the table to highlight the prefix to bring down.

Hold down **Ctrl** and click the mouse button to highlight more than one prefix at a time.

- 8 Right-click the highlighted prefix(es) and choose **All** or **Selected** from the pop-up menu.

You can also click **Down** at the bottom of the Bringing Down Prefixes window. **All** deletes every prefix listed in the table. **Selected** deletes only highlighted prefixes.

- 9 Click **Yes** to complete the process of bringing down the prefixes or click **No** to cancel the process.

Bring Down VRF



This option is enabled if your appliance is licensed for VPN, and if VPN protocol is present in the opened topology.

The Down VRF function changes the state of one or more VPN nodes to down on a particular router, simulating what would happen if the selected item should fail.

To bring down a VPN customer site, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Down VRF** from the Planning menu.
- 3 On the topology map, click on a VPN node to select the customer site PE router.
- 4 From the Network field, select the network of the customer you site you want to bring down.

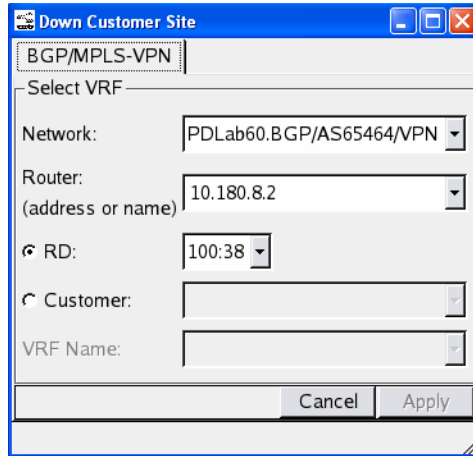


Figure 111 Down Customer Site

- 5 From the Router field, select the router's address.
- 6 You now have the choice of two radio buttons that display, **RD** or **Customer**. You cannot select both radio buttons.
- 7 The **RD** radio button identifies the VRF for the customer. Select the RD that identifies the VRF, and continue to Step 10.
- 8 If you select the **Customer** radio button, its field populates from customers to choose from. Make your selection, and proceed to the next step.
- 9 In the VRF Name field, select the VRF name for the customer you selected in the previous step.



This field does not activate if you chose RD in Step 7.

- 10 Click **Apply**.

Working with Planning Reports



Planning Reports apply to RAMS without traffic only.

RAMS uses present-time statistics derived from traffic data to help plan realistic changes to the network. Use the resulting information to create an optimal configuration for the network, one that will maximize available resources and provide consistent quality service to users.

After using Planning mode to make changes to the topology as described in the previous sections, you can analyze the effects of those simulated changes on such variables as link utilization, bandwidth and available capacity using the Planning Reports window. This data is displayed per node, interface, exit router and more. For example, to see how the addition of a node influences link traffic, use planning reports to view how much traffic was present on each link before the node was added, after it was added and the amount of traffic that changed as a result of the edit.

Planning Report Access

You can access planning reports from the Planning menu in RAMS.

To access planning reports in RAMS, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Reports** from the Planning menu.

The Show Topology Edits window opens ([Figure 112](#)). See these sections for information on working with the planning reports:

- [Navigation Tree](#) on page 260
- [Drill-down Function](#) on page 261
- [Planning Report Icons](#) on page 262
- [Edits](#) on page 262
- [Advanced Filtering](#) on page 264

Navigation Tree

The navigation tree, shown in the left-hand pane in [Figure 112](#), defines the protocols found in your network. If your network supports multiple protocols, you will see an Aggregate category for IPv4 and VPN traffic.

You can expand or compress any category preceded by a plus or minus symbol. Within each category are reports that contain columns of generally requested information.

Drill-down Function





A drill-down menu is available at the top-right of each window (except for the Edit Reports option). Drill-down allows you break down data into finer detail. Drill-down capability is not available for all measures, either because finer detail is not stored or you have already reached the finest detail. The following list displays drill-down options found in certain planning reports. Not all of these choices are available in every drill-down, due to the nature of the report. For instance, an IPv4-related report will not display VPN-related drill-downs. The following choices are found in the drill-down menus in planning reports:

- BGP Community
- Destination AS
- Egress PE
- Exit Router
- Exporter
- Flows
- Exporters
- Interfaces
- Flow Collector
- IPv4 Flows
- Ingress P
- Ingress PE
- Link
- Neighbor AS
- Traffic Groups
- Transit AS
- VPN Flows

Planning Report Icons

The following icons are found at the top-right of the planning Reports window (see [Planning Report Access](#) on page 260).

Table 19 Planning Report Icons

	Analyze Edits	Select to update all traffic and routing edits simultaneously.
	Undo All Edits	Select to reverse the edits made.
	Import Edits	Select to import edits from another database or clipboard
	Export Edits	Select to export edits to another database or clipboard.

Edits

The Show Topology Edits window ([Figure 112](#)) displays a list of all edits made to the network (see [Planning Report Access](#) on page 260).

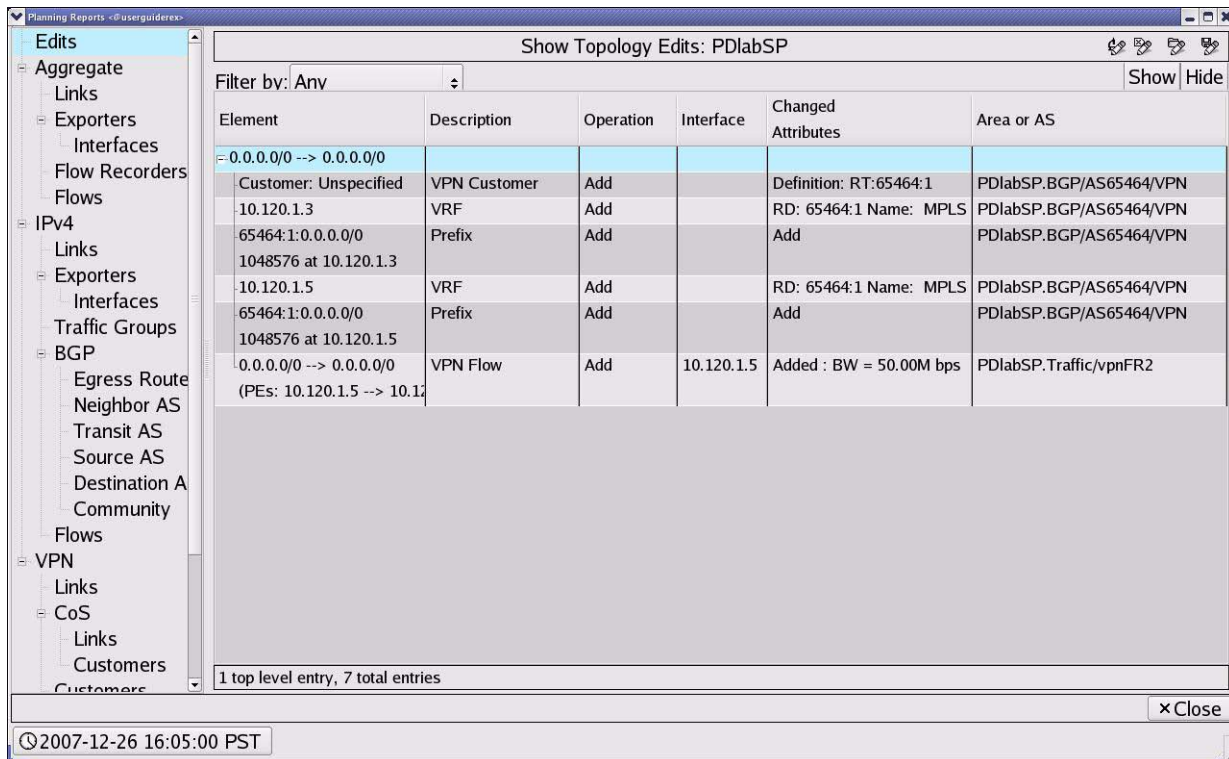


Figure 112 Show Topology Edits Window

The window includes the following columns:

- **Element**—Displays what object (or element) in the network is being affected by the particular edit. This could be a router name, a link (specified by two end points) a prefix, etc.
- **Description**—Displays the type (of a router, link, etc) that is displaying in the **Element** column.
- **Operation**—Displays the type of edit operation that occurred for the element.
- **Interface**—Displays the interface address of the element.
- **Changed Attributes**—Displays what changed for the edited element. For example, if you changed the bitrate of a flow it will display what the bitrate was before and after the edit.

- **Area or AS**—Displays the topology name of the network, which includes information on the administrative name you specified when you set up recording, protocol name, and an AS number or area.

Advanced Filtering

Simple filters let you choose a single operator from a list and specify one or more parameters to be matched or excluded.

Advanced filters let you choose two or more different operators from a list and specify their corresponding parameters to be matched or excluded. From a Filter workspace, select the drop-down list in the Filter by field and choose **Advanced**.

For more information about filtering, see [Using Filters](#) on page 195 in the Chapter 4, “The History Navigator”

Understanding Planning Reports

This section describes the contents of the specific planning reports:

- [Aggregate Reports](#) on page 264
- [IPv4 Planning Reports](#) on page 268
- [BGP Traffic Reports](#) on page 271
- [VPN Traffic Reports](#) on page 274

Aggregate Reports

The Aggregate Reports hierarchy is displayed only if both IPv4 and VPN traffic are present. These reports present the total load of both IPv4 and VPN traffic on the network.

The following planning reports are found beneath the Aggregate option in the left navigational pane:

- [Links Report](#)
- [CoS Report](#)

- [CoS Links Report](#)
- [Exporters Report](#)
- [Interfaces Report](#)
- [Flow Collectors Report](#)
- [Flows Report](#)

The Aggregate Report provides presents the following columns of information for the protocols shown in the left navigational pane:

- **Element**—Displays what object (or element) in the network is being affected by the editing. This could be a router name, a link (specified by two end points) a prefix, etc.
- **Description**—Displays the type (of a router, link, etc) that is displaying in the **Element** column.
- **Operation**—Displays the type of edit operation that occurred for the element.
- **Interface**—Displays the interface address of the element.
- **Changed Attributes**—Displays what changed for the edited elements. For example, if you changed the bitrate of a flow it will display what the bitrate was before and after the edit.
- **Area or AS**—Displays the topology name of the network, which includes information on the administrative name you specified when you set up recording, protocol name, and an AS number or area.

Links Report

Selecting this option invokes the Link Utilization Total Traffic report. Each row displaying in this report represents a link on the topology map.

The report contains the following columns:

- **Source**—Identifies the source address of the link.
- **Destination**—Identifies the destination address of the link.
- **Capacity**—Lists the capacity of the link, if known.
- **Traffic Before Edit**—Displays the amount of traffic flowing across the link before editing occurred.

- **Traffic After Edit**—Displays the amount of traffic flowing across the link after editing
- **Traffic Change**—Displays the traffic delta for the link.

CoS Report

This report displays the total amount of VPN traffic seen with each CoS.

The report contains the following columns:

- **CoS**—Displays the class of service defined for each router.
- **Traffic Before Edit**—Displays the amount of traffic flowing for each CoS before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing for each CoS after editing.
- **Traffic Change**—Displays the traffic delta for the CoS.

CoS Links Report

This report displays the total amount of CoS links seen with each Class of Service (CoS).

The report contains the following columns:

- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the links.
- **CoS**—Displays the Class of Service attributed for the link.
- **Traffic Before Edit**—Displays the amount of traffic flowing though the links before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through the links after editing.
- **Traffic Change**—Displays the traffic delta for the link.

Exporters Report

Each row shown in this table represents a router sending NetFlow data throughout the topology.

The report contains the following columns:

- **Exporter**—Displays the address of the exporting router.
- **Traffic Before Edit**—Displays the amount of traffic flowing before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing after editing.
- **Traffic Change**—Displays the traffic delta for the link.

Interfaces Report

Each row represents a router interface where traffic was seen and exported over the Network.

The report contains the following columns:

- **Exporter: Interface Index**—Identifies a network interface on the exporting router by its SNMP interface index.
- **Traffic Before Edit**—Displays the amount of traffic flowing before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing after editing.
- **Traffic Change**—Displays the traffic delta for the link.

Flow Collectors Report

Each row in this report represents a Flow Collector on the network.

The report contains the following columns:

- **Flow Collector**—Identifies the Flow Collectors found on the network.
- **Traffic Before Edit**—Displays the amount of traffic flowing across the link before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing across the link after editing.
- **Traffic Change**—Displays the traffic delta for the link.

Flows Report

Each row in this report represents a prefix-to-prefix flow found in the network.

The report contains the following columns:

- **Flow Source**—Identifies the source address for the flow.
- **Flow Destination**—Identifies the destination address for the flow.
- **Exporter**—Identifies exporting routers found in the network.
- **Traffic Group**—Identifies all traffic groups for the flow found on the network (IPv4 flows only).
- **ToS/CoS**—Displays Type of Service (Tos) and Class of Service (CoS) for the flow.
- **Egress PE**—Displays each PE router found at the edge of an ISP (VPN flows only).
- **Traffic Before Edit**—Displays the amount of traffic flowing across the link before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing across the link after editing.
- **Traffic Change**—Displays the traffic delta for the link.

IPv4 Planning Reports

This section describes the following IPv4 Planning reports that are available:

- [Links Report](#)
- [CoS Report](#)
- [CoS Links Report](#)
- [Exporters Report](#)
- [Interfaces Report](#)
- [Traffic Groups Report](#)
- [Flows Report](#)

Links Report

This report displays every IPv4 link found in the network. Selecting this option invokes the Link report. Every row displaying in this report represents a link on the topology map.

The report contains the following columns:

- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the links.
- **Traffic Before Edit**—Displays the amount of traffic flowing through the links before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through the links after editing.
- **Traffic Change**—Displays the traffic delta for the link.

CoS Report

This report displays the total amount of VPN traffic seen with each CoS.

The report contains the following columns:

- **CoS**—Displays the class of service defined for each router.
- **Traffic Before Edit**—Displays the amount of traffic flowing for each CoS before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing for each CoS after editing.
- **Traffic Change**—Displays the traffic delta for the CoS.

CoS Links Report

This report displays the total amount of CoS links seen with each Class of Service (CoS).

The report contains the following columns:

- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the links.
- **CoS**—Displays the Class of Service attributed for the link.
- **Traffic Before Edit**—Displays the amount of traffic flowing through the links before editing occurred.

- **Traffic After Edit**—Displays the amount of traffic flowing through the links after editing.
- **Traffic Change**—Displays the traffic delta for the link.

Exporters Report

Each row shown in this table represents a router sending NetFlow data throughout the topology.

The report contains the following columns:

- **Exporter**—Identifies the exporting router.
- **Traffic Before Edit**—Displays the amount of traffic flowing through the exporters before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through the exporters after editing.
- **Traffic Change**—Displays the traffic delta for the exporters.

Interfaces Report

Each row represents a router interface where traffic was seen and exported over the Network.

The report contains the following columns:

- **Exporter, Interface Index**—Identifies a network interface on the exporting router by its SNMP interface index.
- **Traffic Before Edit**—Displays the amount of traffic flowing before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing after editing.
- **Traffic Change**—Displays the traffic delta for the link.

Traffic Groups Report

This report displays the IPv4 traffic groups found in the network. For more information about traffic groups, see “Administration” in the *HP Route Analytics Management System Administrator Guide*.

The report contains the following columns:

- **Traffic Group**—Identifies all traffic groups found in the network.
- **Traffic Before Edit**—Displays the amount of traffic flowing for the group before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing for the group after editing.
- **Traffic Change**—Displays the traffic delta for the groups.

Flows Report

Each row in this report represents a prefix-to-prefix IPv4 flow found in the network.

The report contains the following columns:

- **Flow Source**—Identifies the source address for the flow.
- **Flow Destination**—Identifies the destination address for the flow.
- **Exporter**—Identifies exporting routers found in the network.
- **Traffic Group**—Identifies all traffic groups for the flow found on the network (IPv4 flows only).
- **ToS/CoS**—Displays Type of Service (Tos) and Class of Service (CoS) for the flow.
- **Egress PE**—Displays each PE router found at the edge of an ISP (VPN flows only).
- **Traffic Before Edit**—Displays the amount of traffic flowing across the link before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing across the link after editing.
- **Traffic Change**—Displays the traffic delta for the link.

BGP Traffic Reports

This section describes the following available BGP Traffic reports:

- [Egress Router Report](#)
- [Neighbor AS Report](#)

- [Transit AS Report](#)
- [Source AS Report](#)
- [Destination AS Report](#)
- [Community Report](#)

Egress Router Report

Each row in this report lists all the neighboring ASs (the immediate neighbor for the Exit Router) found in the network.

The report contains the following columns:

- **Egress Router**—Displays each exiting router in the network.
- **Next Hop**—Identifies the next router along the exit router's path.
- **Traffic Before Edit**—Displays the amount of traffic flowing through the neighboring ASs before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing for the neighboring ASs after editing.
- **Traffic Change**—Displays the traffic delta for the neighbor ASs.

Neighbor AS Report

Each row in this report lists all the neighboring ASs (the immediate neighbor for the Exit Router) found in the network.

The report contains the following columns:

- **Neighbor AS**—Displays every neighboring AS in the network.
- **Traffic Before Edit**—Displays the amount of traffic flowing through the neighboring ASs before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing for the neighboring ASs after editing.
- **Traffic Change**—Displays the traffic delta for the neighbor ASs.

Transit AS Report

This report displays all of the traffic passing through a given AS (but not starting or ending with this particular AS) along the path to its destination.

The report contains the following columns:

- **Transit AS**—Identifies the transit AS in the network.
- **Traffic Before Edit**—Displays the amount of traffic flowing through transit ASs before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through transit ASs after editing.
- **Traffic Change**—Displays the traffic delta for the ASs.

Source AS Report

This report displays the inferred source AS of all the traffic flows passing through the network.

For every flow, the appliance finds the most-specific BGP route to the source of the flow, and uses the originating AS of this route to determine the breakdown of traffic for this report. This enables the appliance to find what AS originated that route, thus giving you the most-likely source AS.

The report contains the following columns:

- **Source AS**—Identifies the source AS in the network.
- **Traffic Before Edit**—Displays the amount of traffic originating from the source ASs before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through source ASs after editing.
- **Traffic Change**—Displays the traffic delta for the ASs.

Destination AS Report

Each row lists the amount of traffic categorized by the AS of its ultimate destination.

The report contains the following columns:

- **Destination AS**—Identifies each destination AS in the network.
- **Traffic Before Edit**—Displays the amount of traffic flowing through the destination ASs before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through the destination ASs after editing.

- **Traffic Change**—Displays the traffic delta for the destination ASs.

Community Report

This report shows the amount of traffic that is destined for routes belonging to different BGP communities. Community attributes are a way for ISPs to apply certain kinds of routing policies to the routes received by a particular router. Each route can belong to zero or more communities, and the communities to which a route belongs are carried as attributes of the route.

The report contains the following columns:

- **First 2 Octets**—Displays the first two AS numbers for the given community attribute.
- **Second 2 Octets**—Displays the second two AS numbers for the given community.
- **Traffic Before Edit**—Displays the amount of traffic flowing through exit routers before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic using routes with a given community attribute.
- **Traffic Change**—Displays the traffic delta for the exit routers.

VPN Traffic Reports

The following VPN traffic-related planning reports are available:

- VPN Links Report
- VPN CoS Report
- VPN CoS Links Report
- VPN CoS Customers Report
- VPN Customers Report
- Ingress PE Report
- Exporters Report
- Interfaces Report
- Egress PE Report

- [VPN Flows Report](#)

VPN Links Report

This report displays every VPN link carrying traffic in the network. Selecting this option invokes the Link report. Every row displaying in this report represents a link on the topology map.

The report contains the following columns:

- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the links.
- **Traffic Before Edit**—Displays the amount of traffic flowing through the links before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through the links after editing.
- **Traffic Change**—Displays the traffic delta for the link.

VPN CoS Report

This report displays the total amount of VPN traffic seen with each CoS.

The report contains the following columns:

- **CoS**—Displays the class of service defined for each router.
- **Traffic Before Edit**—Displays the amount of traffic flowing for each CoS before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing for each CoS after editing.
- **Traffic Change**—Displays the traffic delta for the CoS.

VPN CoS Links Report

This report displays the total amount of CoS links seen with each Class of Service (CoS).

The report contains the following columns:

- **Source**—Displays the source address for the link.

- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the links.
- **CoS**—Displays the Class of Service attributed for the link.
- **Traffic Before Edit**—Displays the amount of traffic flowing though the links before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through the links after editing.
- **Traffic Change**—Displays the traffic delta for the link.

VPN CoS Customers Report

This report displays the total amount of CoS Customers seen with each CoS.

The report contains the following columns:

- **Customer**—Displays every VPN customer found in the network.
- **CoS**—Defines the Class of Service for each VPN customer found on the network.
- **Traffic Before Edit**—Displays the amount of traffic flowing through each customer before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through each customer after editing.
- **Traffic Change**—Displays the traffic delta for the customer.

VPN Customers Report

This report displays the traffic seen by each VPN customer.

The following columns display for this report:

- **Customer**—Displays every VPN customer found in the network.
- **Traffic Before Edit**—Displays the amount of traffic flowing through each customer before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through each customer after editing.
- **Traffic Change**—Displays the traffic delta for the customer.

Ingress PE Report

This report displays each Ingress PE router found on the network.

The report contains the following columns:

- **Ingress PE**—Identifies the Ingress PE.
- **Traffic Before Edit**—Displays the amount of traffic flowing through each Ingress PE before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through each Ingress PE after editing.
- **Traffic Change**—Displays the traffic delta for the Ingress PE.

Exporters Report

This report shows every exporting router found in the network.

The report contains the following columns:

- **Exporter**—Displays the address of the exporting router.
- **Traffic Before Edit**—Displays the amount of traffic flowing before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing after editing.
- **Traffic Change**—Displays the traffic delta for the link.

Interfaces Report

Each row represents a router interface where VPN traffic was seen and exported over the Network.

The report contains the following columns:

- **Exporter: Interface Index**—Identifies a network interface on the exporting router by its SNMP interface index.
- **Traffic Before Edit**—Displays the amount of traffic flowing before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing after editing.
- **Traffic Change**—Displays the traffic delta for the link.

Egress PE Report

This report shows each PE router found at the edge of an ISP.

The report contains the following columns:

- **Egress PE**—Identifies the Egress PE.
- **Traffic Before Edit**—Displays the amount of traffic flowing through each Ingress PE before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing through each Ingress PE after editing.
- **Traffic Change**—Displays the traffic delta for the Ingress PE.

VPN Flows Report

This report lists every prefix-to-prefix flow for VPN traffic.

The report contains the following columns:

- **Flow Source**—Identifies the source address for the flow.
- **Flow Destination**—Identifies the destination address for the flow.
- **CoS**—Identifies the Class of Service for the flow.
- **Exporter**—Identifies exporting routers found in the network.
- **Egress PE**—Displays each PE router found at the edge of an ISP (VPN flows only).
- **Traffic Before Edit**—Displays the amount of traffic flowing across the link before editing occurred.
- **Traffic After Edit**—Displays the amount of traffic flowing across the link after editing.
- **Traffic Change**—Displays the traffic delta for the link.


Working with Capacity Planning Tools



Capacity Planning applies to RAMS only. To enable capacity planning, you must be in Analysis mode.

Capacity planning enables you to view an estimate of what future traffic demands may be like, based on past data that has already been collected. A linear regression model is used to extrapolate traffic demands into the future. This allows you to plan potential expansion of the network in order to meet future demands. This feature enables you to be sure that the network will have the capacity to carry future traffic loads.

To access the capacity planning reports, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 If you are not already in Analysis mode, click the icon in the lower right corner of the window and choose the Analysis mode icon .
- 3 Choose **Capacity Planning** from the Planning menu. The Aggregate window opens.

Navigation Tree and Report Window Settings

The navigation tree in the left pane of the Capacity Planning window defines the protocols of your network. If your network supports multiple protocols, you will see an Aggregate category for IPv4 and VPN traffic.

You can expand or hide any category that is preceded by a plus or minus symbol. Within each category are reports that contain columns of generally requested information.

Use the Trending menu ([Figure 113](#)) to set parameters to control the trending period.

Start Trending From

6 Months ago

Statistic

Avg

Min

Max

95%ile

Model

Linear

Exponential

End Trending At

Date 2008-04-27

Traffic Level 6 Mbps

Cancel OK

Figure 113 Trending Options

Aggregate Capacity Planning Reports

This section describes the following aggregate capacity planning reports:

- [Links Report](#)
- [CoS Report](#)
- [CoS Links Report](#)
- [Exporters Report](#)
- [Interfaces Report](#)
- [Flow Collectors Report](#)

Links Report

Selecting this option invokes the Links report. Every row displaying in this report represents a link on the topology map.

The report contains the following columns:

- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the link.
- **Daily %-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

CoS Report

This report displays the total traffic amount of all exporting routers with a particular class of service assigned to the routers.

The report contains the following columns:

- **CoS**—Defines the Class of Service for each VPN Customer found in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that

95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

CoS Links Report

Each line of the displays the total amount of traffic per link at each class of service.

The report contains the following columns:

- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the links.
- **CoS**—Defines the Class of Service for each VPN Customer found in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

Exporters Report

Each row shown in this report represents a router sending NetFlow data throughout the topology.

- **Exporter**—Displays the address of the exporting router.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

Interfaces Report

This report displays how much traffic each exporting router detects, broken down by network interface. The interfaces are identified by the exporting router and the SNMP interface index. This report shows the amount of traffic that can be expected to arrive on each router interface at some point in the future.

The report contains the following columns:

- **Exporter: Interface Index**—Identifies a network interface on the exporting router by its SNMP interface index.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

Flow Collectors Report

Each row in this report represents a Flow Collector on the network.

The report contains the following columns:

- **Flow Recorder**—Identifies the Flow Collectors found on the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

IPv4 Capacity Planning Reports

This section describes the following IPv4 Capacity Planning reports:

- [Links Report](#)
- [CoS Report](#)
- [CoS Links Report](#)

- [Exporters Report](#)
- [Interfaces Report](#)
- [Traffic Groups Report](#)

Links Report

This report displays every IPv4 link found in the network.

- The report contains the following columns:
- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the link.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

CoS Report

This report displays the total traffic amount of all exporting routers with a particular class of service assigned to the routers.

The report contains the following columns:

- **CoS**—Defines the Class of Service for each VPN Customer found in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

CoS Links Report

Each line of the displays the total amount of traffic per link at each class of service.

The report contains the following columns:

- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the links.
- **CoS**—Defines the Class of Service for each VPN Customer found in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

Exporters Report

Each row shown in this report represents a router sending NetFlow data throughout the topology.

The report contains the following columns:

- **Exporter**—Displays the address of the exporting router.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

Interfaces Report

This report displays how much traffic each exporting router detects, broken down by network interface. The interfaces are identified by the exporting router and the SNMP interface index. This report shows the amount of traffic that can be expected to arrive on each router interface at some point in the future.

- **Exporter: Interface Index**—Identifies a network interface on the exporting router by its SNMP interface index.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

Traffic Groups Report

This report displays the traffic groups found in the network. For more information about traffic groups, see “Administration” in the *HP Route Analytics Management System Administrator Guide*.

The report contains the following columns:

- **Traffic Group**—Identifies all traffic groups found in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

BGP Capacity Planning Reports

This section describes the following BGP Capacity Planning reports:

- [Egress Router Report](#)
- [Neighbor AS Report](#)
- [Transit AS Report](#)
- [Source AS Report](#)
- [Destination AS Report](#)

Egress Router Report

This report shows traffic segregated by egress PE.

The report contains the following columns:

- **Egress Router**—Identifies each egress router in the network.
- **Next Hop**—Identifies each router along the exit router’s path.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that

95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

Neighbor AS Report

Each row in this report lists all the neighboring ASs (the immediate neighbor for the Exit Router) found in the network.

The report contains the following columns:

- **Neighbor AS**—Displays every neighboring AS in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

Transit AS Report

This report displays all of the AS traffic found along the path to its destination.

The report contains the following columns:

- **Transit AS**—Identifies the transit AS in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

Source AS Report

This report shows the amount of traffic from each source AS at some point in the future, calculated using trending models.

The report contains the following columns:

- **Source AS**—Identifies the source AS in the network.

- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

Destination AS Report

Each row lists the amount of traffic categorized by the AS of its ultimate destination.

The report contains the following columns:

- **Destination AS**—Identifies each destination AS in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

VPN Capacity Planning Traffic Reports

The following are VPN traffic-related Capacity Planning reports:

- VPN Links Report
- VPN CoS Report
- VPN CoS Links Report
- VPN CoS Customers Report
- VPN Customers Report
- Ingress PE Report
- Exporters Report
- Interfaces Report
- Egress PE Report

VPN Links Report

Selecting this option invokes the Links report. Every row displaying in this report represents a VPN link on the topology map.

The report contains the following columns:

- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the link.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

VPN CoS Report

This report displays the total traffic amount of all exporting routers with a particular class of service assigned to the routers.

The report contains the following columns:

- **CoS**—Defines the Class of Service for each VPN Customer found in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

VPN CoS Links Report

Each line of the displays the total amount of traffic per link at each class of service.

The report contains the following columns:

- **Source**—Displays the source address for the link.
- **Destination**—Displays the destination address for the link.
- **Capacity**—Displays the capacity value for the links.
- **CoS**—Defines the Class of Service for each VPN Customer found in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

VPN CoS Customers Report

Each line of this report displays how much traffic is being sent to this customer at each class of service.

The report contains the following columns:

- **Customers**—Displays every VPN customer found in the network.
- **CoS**—Defines the Class of Service for each VPN customer found on the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

VPN Customers Report

This report displays the total number of user-defined VPN Customers found on the network.

The report contains the following columns:

- **Customers**—Displays every VPN customer found in the network.
- **CoS**—Defines the Class of Service for each VPN Customer found in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

Ingress PE Report

This report displays each Ingress PE router found on the network.

The report contains the following columns:

- **Ingress PE**—Identifies the Ingress PE.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

Exporters Report

Each row shown in this report represents a router sending NetFlow data throughout the topology.

The report contains the following columns:

- **Exporter**—Displays the address of the exporting router.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

Interfaces Report

This report shows the amount of traffic that can be expected to arrive on each router interface at some point in the future.

The report contains the following columns:

- **Exporter: Interface Index**—Identifies a network interface on the exporting router by its SNMP interface index.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that

95% of the five-minute intervals have traffic demands below this amount, and five % of the five-minute intervals have traffic demands above this amount.

Egress PE Report

This report shows each PE router found at the edge of an ISP.

The report contains the following columns:

- **Egress PE**—Identifies every egress PE router found in the network.
- **Daily 95%-tile**—Displays the 95th percentile of actual traffic for five-minute intervals throughout the day. Of those five-minute intervals, you can compute the 95th percentile. This is the amount of traffic such that 95% of the five-minute intervals have traffic demands below this amount, and 5% of the five-minute intervals have traffic demands above this amount.

Show Edits



This option displays only if the open topology does not include traffic. To see a list of edits made for a topology that includes traffic, see [Edits](#) on page 262.

Every edit made to the topology map is displayed in the Show Edits window. To view the edits, choose **Show Edits** from the Planning menu.

Element	Description	Operation	Interface	Changed Attributes	Area
Router12	Router	Down		State: UP -> DOWN	PACKETDESIGNLABNETWO
Router12 <-> Router12.03	Link	Down	10.64.4.12	State: UP -> DOWN	PACKETDESIGNLABNETWO
Router12.03 <-> Router12	Link	Down		State: UP -> DOWN	PACKETDESIGNLABNETWO
Router12 <-> Router12.02	Link	Down	10.64.13.12	State: UP -> DOWN	PACKETDESIGNLABNETWO
Router12.02 <-> Router12	Link	Down		State: UP -> DOWN	PACKETDESIGNLABNETWO
-10.64.4.0/24 at Router12	Prefix	Down		State: UP -> DOWN	PACKETDESIGNLABNETWO
-10.64.13.0/24 at Router12	Prefix	Down		State: UP -> DOWN	PACKETDESIGNLABNETWO
-10.120.1.12/32 at Router12	Prefix	Down		State: UP -> DOWN	PACKETDESIGNLABNETWO

1 top level entry, 9 total entries

Figure 114 Show Edits Window

This window shows edits that have been made. The following columns are included:

- **Element**—Item that has been changed.
- **Description**—Description of change.
- **Operation**—Operation performed to effect the change.
- **Interface**—Interface involved in the change.
- **Changed Attributes**—Attributes that were modified.
- **Area or AS**—Affected area or AS.

You can import edits, export edits, or undo edits that have been made. Use the buttons in the lower right corner.



Undo All Edits — Clears the list of changes in the Show Topology Edits table and removes the corresponding edits from the topology map. The original layout of the topology map is restored.



Import — Allows you to import edits from either the clipboard or from a database.



Export — Allows you to send the edits listed in the Show Topology Edits table to either the clipboard or to a database. Exported edits can then be manipulated in external programs, such as Emacs or Excel.

6 IGP Reports

This chapter describes how to use IGP reports to display information about IGP routing events in the network.

Chapter contents:

- [Understanding IGP Reports](#) on page 300
- [Accessing the IGP Report Pages](#) on page 300
- [Configuring IGP Reports](#) on page 301
- [Understanding IGP Report Contents](#) on page 303

Understanding IGP Reports

The following types of IGP reports are available:

- Summary Reports—View high-level network activity over a specified time period, display day-to-day changes, and quickly flag potential problems.
 - Network Events Summary
 - Network Churn
- Drill-Down Reports—View detailed information to verify configuration changes after troubleshooting problems.
 - Changed Metrics
 - Flapping Links
 - Prefix Origination Changes
 - New Prefixes
 - New Routers and Links
 - Prefixes Withdrawn
- Inventory Reports—View available network resources.
 - Prefix List
 - Prefix Origination from Multiple Sources

Following initial installation, we recommend that you generate and print all of the IGP reports to obtain a baseline view of network status.

To identify network problems, begin with the Summary report to identify the general problem area. You can then run additional reports to better identify the problem. For example, if the Summary report displays a large number of flapping links, run a Flapping Links report to further analyze the problem.

Accessing the IGP Report Pages

If you have a deployment with multiple Route Recorders, we recommend that you access the IGP and BGP reports pages from the centralized Modeling Engine, for the following reasons:

- The Modeling Engine is physically closer to the user.
- Requesting data from the Modeling Engine reduces overhead on the Route Recorder.

When you obtain reports directly from a Route Recorder, information local to the area or protocol being monitored is returned. When you obtain reports from the centralized Modeling Engine, information collected from recorders across entire network is returned.

To access the IGP report pages, perform the following steps:

- 1 Open the web application and choose **Reports Portal**.
- 2 On the Daily Reports page that opens by default, click **IGP Reports** on the left navigation bar to open the reports page (Figure 115).



Report data is not available until 15 minutes after recording has begun. If you attempt to run a report sooner, a “Report data not available” message is displayed, and you may see an additional message that explains why the report was not generated. If the database is not recording data, ask your administrator to start the recording process.

IGP Reports

Select Report:

Figure 115 IGP Reports Page

Configuring IGP Reports

This section describes how to configure the IGP reports.

To configure IGP reports, perform the following steps:

- 1 Open the web application and choose **Reports Portal**.

- 2 Choose **IGP Reports** on the left navigation bar.
- 3 Choose a report from the drop-down list and click **Configure Report**.
- 4 Configure the following report options:
 - Choose the desired database from the Administrative Domain drop-down list.
 - For reports that present interval options, choose the top button to specify a time period up till the current time or the bottom button to specify an exact start and end time ([Figure 116](#)).

Administrative Domain:

Interval

Last

Year: Month: Day: Hour: Minute:

through

Year: Month: Day: Hour: Minute:

Figure 116 Configuring IGP Reports - Interval Options

- For reports that present a time option, choose a time period from the drop-down lists. For the Prefix Origination from Multiple Sources report, you can also specify the minimum number of originating routers ([Figure 117](#)).

Administrative Domain:

Time

Year: Month: Day: Hour: Minute:

Minimum originating router:

Figure 117 Configuring IGP Reports - Time Options

- 5 Click **Create Report**.

The time it takes 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.

The report is generated from the selected database and displayed in a new page. You can use the print command on your browser to print a copy of the report or click **Reconfigure Report** to change the time period.

Understanding IGP Report Contents

This section describes the IGP report contents:

- [Network Events Summary](#) on page 303
- [Changed Metrics](#) on page 304
- [Flapping Links](#) on page 305
- [Network Churn](#) on page 306
- [New Prefixes](#) on page 307
- [New Routers and Links](#) on page 308
- [Prefix List](#) on page 309
- [Prefix Origination Changes](#) on page 311
- [Prefix Origination from Multiple Sources](#) on page 312
- [Prefixes Withdrawn](#) on page 314

Network Events Summary

The Network Events Summary report summarizes network changes for the specified time period and is a good place to start when diagnosing network problems or checking general network status.

Table 20 describes the fields in the report.

Table 20 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 between the two time frames, along with what the values were at the beginning and end time frames
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

Changed Metrics

The Changed Metrics report provides a 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.

Run this report after scheduled maintenance to confirm that planned metric changes have occurred.

Table 21 describes the fields in the report.

Table 21 Changed Metric Report Fields

Field	Description
Link	Link from source router to the destination router
Source Interface	The source of the link
Destination Interface	Destination of the link
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, including 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 to list the links with the highest flap count at the top.

Run this report if you suspect a problem with links in the network. For example, the Network Events Summary report may display a high incidence of flapping link events, and this report will indicate 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.

In cases where a route is flapping an abnormally high number of times, you can configure an alert on the link to monitor it more closely for a period of time to ensure that an outage is avoided. See [Chapter 11, “Alerts”](#)

Table 22 describes the fields in the Flapping Links report.

Table 22 Flapping Links Report Fields

Field	Description
Link	Link from the source to destination router
Source Interface	The source of the link
Destination Interface	The destination of the link
Count	The number of times the link has changed state
Time	The date and time the last change occurred

Network Churn

The Network Churn report displays a summary of routing events that took place over the selected time period and identifies all of the sources (routers) and number of events attributed to each source. Routing events tabulation excludes “hello” packets, which are exchanged periodically.

Run this report if the Network Events Summary report displays an unusually high level of network events.

The report has two columns. Table 23 describes the fields in the Router column and Table 24 describes the fields in the Number of Events column.

Table 23 Router Column Fields

Field	Description
Name	The router name provided by the routing protocol, if available
IP Address	Address of the router originating the events

Table 24 Number of Events Column Fields

Field	Description
Total	Cumulative total of all events
Router	Number of router events: <ul style="list-style-type: none"> •Router dynamic hostname change (for ISIS only) •ISIS overload bit change •Router type change, for example between Internal and Area Border Router (ABR) for OSPF
Prefix	Number of prefix events for this router: <ul style="list-style-type: none"> •Addition and dropping of prefix adjacencies •Changes in the metric to a prefix
Link	Number of link events for this router: <ul style="list-style-type: none"> •Addition and dropping of neighbor router adjacencies, including peering •Changes in the metric on the link to a neighbor

New Prefixes

The New Prefixes report lists all of the newly advertised prefixes for the report period, including the advertising frequency. Sources of new prefixes include new links, networks, tunnels, and routers. Run this report after scheduled maintenance to verify the changes that were made.

Table 25 describes the fields in the report.

Table 25 New Prefixes Fields

Field	Description
Prefix	IP address of the new prefix
System ID	System Identifier for the router
Name	Name of the router

Table 25 New Prefixes Fields

IP Address	IP address of the router. This column may not display if the routers do not have an IP address attributed to them
Time	Time the new prefix first appeared on the network
Count	Number of times the prefix was advertised

New Routers and Links

The New Routers and Links report lists newly advertised source and destination routers and links in the network. Run this report after new routers are inserted into the network or new links are set up to verify the changes.

Table 26 describes the fields in the report.

Table 26 New Routers Table Fields

Field	Description
IP Address	IP Address of the newly advertised router
Type	Could be: <ul style="list-style-type: none"> • unknown • internal • area-external • AS-external • both internal and area-external • both internal and AS-external • internal, area-external and AS-external
Name	The router name provided by the routing protocol, if available

Table 27 describes the fields in the report.

Table 27 New Links Table Fields

Field	Description
Link	Link from the source to destination router
Source Interface	The source of the link
Destination Interface	The destination of the link

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.

Table 28 describes the fields in the report.

Table 28 Prefix List Fields for an IGP Domain

Field	Description
Prefix	The address of the prefix.
Type	Could be: <ul style="list-style-type: none"> •unknown •internal •area-external •AS-external •both internal and area-external •both internal and AS-external •internal, area-external and AS-external

Table 28 Prefix List Fields for an IGP Domain (cont'd)

Area or AS	The area or AS where the prefix is located
Name	The router name provided by the routing protocol, if available
IP Address	IP address of the router advertising the prefix

If you chose OSI as the Administrative Domain, Table 29 describes the fields in the report.

Table 29 Prefix List Fields for an OSI Domain

Field	Description
Prefix Neighbor/ES Neighbor	The address of the prefix neighbor or ES neighbor
Type	Could be <ul style="list-style-type: none"> •unknown •internal •area-external •AS-external •both internal and area-external •both internal and AS-external •internal, area-external and AS-external
Area or AS	The area or AS where the prefix is located
System ID	The System Identifier for the router
Name	The router name provided by the routing protocol, if available

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.

Run this report every few days to identify potential problems, such as a router losing an interface or a flapping link.

Table 30 describes the fields in the report for current routers and Table 31 for the changes version of the report.

Table 30 Prefix Origination Changes Current Routers Fields for IGP Domain

Field	Description
Prefix	The prefix address of the network
Name	The name of the router (if available in the routing protocol)
IP Address	The IP address (router ID) in dotted decimal notation

Table 31 Prefix Origination Router Changes Report Fields for IGP Domain

Field	Description
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

If you choose OSI as the Administrative Domain, Table 32 describes the fields in the report for current routers and Table 33 for the changes version of the report.

Table 32 Prefix Origination Changes Current Routers Fields for OSI Domain

Field	Description
Prefix	The prefix neighbor and ES neighbor
System ID	System Identifier for the current router
Name	The router name provided by the routing protocol, if available

Table 33 Prefix Origination Router Fields for OSI

Field	Description
Prefix	The prefix neighbor and ES neighbor
System ID	System Identifier for the changed router
Name	The router name provided by the routing protocol, if available
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. Run this report to determine if redundant links or hosts (such as redundant DNS servers, “Anycast” IP Multicast Rendezvous Points) are operating normally. The absence of a redundant link or host from the list indicates that a redundant link or host is down, possibly resulting in reduced service levels or other problems within the network. This report can also detect configuration errors.

Run this report if the Prefix Origination Changes report identifies a problem or when you receive an alert that a redundant link has failed.

Table 34 describes the fields in the report.

Table 34 Prefix Origination from Multiple Sources Report Fields

Field	Description
Prefix	The IP Address of the network prefix.
Type	Could be: <ul style="list-style-type: none">•unknown•internal•area-external•AS-external•both internal and area-external•both internal and AS-external•internal, area-external and AS-external
Area or AS	The area or AS where the prefix is located
Name	Name of the router (if available in the routing protocol)
IP Address	The IP address of the router

If you selected OSI for the Administrative Domain, Table 35 describes the fields in the report.

Table 35 Prefix Origination from Multiple Sources Router Report Fields for OSI

Field	Description
Prefix	The IP Address of the network prefix
Type	Could be: <ul style="list-style-type: none"> •unknown •internal •area-external •AS-external •both internal and area-external •both internal and AS-external •internal, area-external and AS-external
Area or AS	The area or AS where the prefix is located
System ID	The System identifier of the router
Name	The name of the router (if available in the routing protocol)

Prefixes Withdrawn

The Prefixes Withdrawn report lists all of the prefixes that have been withdrawn from the network during the specified period. Run this report to identify clients that can no longer access the network or after scheduled maintenance to verify that no prefixes have been unintentionally dropped.

Table 36 describes the fields in the report.

Table 36 Prefixes Withdrawn Report Fields

Field	Description
Prefix	The IP Address of the network prefix
Name	The name of the router (if available in the routing protocol)
IP Address	The IP Address of the router, if available. This field may not display if you chose OSI as the Administrative Domain
Time	The time the prefix was withdrawn
Count	The number of times the prefix was withdrawn

7 BGP Reports

This chapter describes how to use BGP reports to display information about BGP routing events in the network.

Chapter contents:

- [Understanding BGP Reports](#) on page 318
- [Accessing the BGP Report Pages](#) on page 319
- [Generating BGP Activity Reports](#) on page 320
- [Creating BGP Logical Topology Reports](#) on page 323

Understanding BGP Reports

The following types of BGP reports are available:

- Activity Reports—Check BGP routing status on a day-to-day or shift-to-shift basis and quickly identify potential problems.
 - BGP Activity Summary
 - BGP Activity by AS
 - BGP Activity by Peer
 - Route Flap Report
 - Prefix Event Detail
- Logical Topology—View the state of the routing tables at specified times to aid in problem identification. These reports also provide an easy-to-read multiple router summary.
 - Route Distribution Detail by RRC, Next Hop, Peer Router, or Next Hop AS
 - Redundancy by Prefix
 - Baseline Redundancy by Prefix
 - AS Reachability
 - Baseline AS Reachability
 - Prefix Reachability

BGP reports are available in HTML format on Route Recorders and on the centralized Modeling Engine in deployments with multiple Route Recorders.

Following initial installation, we recommend that you generate and print all of the BGP reports to obtain a baseline view of network status. When establishing a baseline, the system looks at routes that have been up for more than 80% of the time over the course of seven days. Before a route reaches the seven day mark, its baseline is determined on a day-to-day basis (for example, 80% of 24 hours or 80% of 48 hours).

To identify network problems, begin with the Summary report to identify the general problem area. You can then run additional reports to better identify the problem.

Accessing the BGP Report Pages

If you have a deployment with multiple Route Recorders, we recommend that you access the IGP and BGP reports pages from the centralized Modeling Engine, for the following reasons:

- The Modeling Engine is physically closer to the user.
- Requesting data from the Modeling Engine reduces overhead on the Route Recorder.

When you obtain reports directly from a Route Recorder, information local to the area or protocol being monitored is returned. When you obtain reports from the centralized Modeling Engine, information collected from recorders across entire network is returned.

To access the BGP report pages, perform the following steps:

- 1 Open the web application and choose **Reports Portal**.
- 2 On the Daily Reports page that opens by default, click **BGP Reports** on the left navigation bar.

The BGP Reports Activity Summary page opens ([Figure 118](#)).



Report data is not available until 15 minutes after recording has begun. If you attempt to run a report sooner, a “Report data not available” message is displayed, and you may see an additional message that explains why the report was not generated. If the database is not recording data, ask your administrator to start the recording process.

Activity Summary

Time:

Database:

Figure 118 BGP Reports Page

Generating BGP Activity Reports

This section describes the following BGP activity reports:

- [BGP Activity Summary Report](#) on page 320
- [BGP Activity by AS Report](#) on page 321
- [BGP Activity by Peer Report](#) on page 322
- [Route Flap Report](#) on page 322
- [Prefix Event Detail](#) on page 323

BGP Activity Summary Report

The BGP Activity Summary report provides a high level overview of BGP network activity over a specified period of time, including any changes or problems with the network. Changes may include new peering sessions or routers appearing on the network.

We recommend that you run the report daily or on a per-shift basis 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, it may indicate a configuration error 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.

To generate the BGP Activity Summary report, perform the following steps:

- 1 Open the web application and choose **Reports Portal**.
- 2 Choose **BGP Reports** → **Activity Summary** on the left navigation bar.
- 3 Choose a time period and database from the drop-down lists.



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 Click **Create Report**.

If data is available as specified, the report is displayed with the following information:

- 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.



Use the Route Flap Report to determine which routers are responsible for activity spikes.

BGP Activity by AS Report

The BGP Activity by AS report provides a filtered view of BGP activity for the individual ASs that comprise the entire network. For each AS, you can identify sources of instability or excessive activity. This report is useful for private enterprise networks in which BGP connects multiple ASs.

To generate the BGP Activity by AS report, perform the following steps:

- 1 Open the web application and choose **Reports Portal**.
- 2 Choose **BGP Reports** → **Activity by AS** on the left navigation bar.
- 3 Select the desired database from the drop-down list.
- 4 Click **List AS**.

If data is available as specified, the report opens to display incoming updates and withdrawals and outgoing updates and withdrawals.

After viewing this report, refer to the [BGP Activity Summary Report](#) to view specific sources of instability or open the History Navigator window and perform an event analysis for the time period.

BGP Activity by Peer Report

The BGP Activity by Peer report allows you to identify that BGP peers that are most active and to diagnose internal churn. Start with the [BGP Activity Summary Report](#) and then run this report if you notice an unusual amount of activity that exceeds the normal expected range.

To generate the BGP Activity by Peer report, perform the following steps:

- 1 Open the web application and choose **Reports Portal**.
- 2 Choose **BGP Reports** → **Activity by Peer** on the left navigation bar.
- 3 Select the desired database from the drop-down list.
- 4 Click **List Peer**.
- 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 data is available as specified, a line chart is displayed showing 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 generate the Route Flap report, perform the following steps:

- 1 Open the web application and choose **Reports Portal**.
- 2 Choose **BGP Reports** → **Route Flap Report** on the left navigation bar.
- 3 Select the desired time period and database from the drop-down lists.

4 Click **Create Report**.

If data is available as specified, prefix ID, the peer that announced or withdrew the prefix, the date/time of the last update, and the current prefix state (announced or withdrawn).

To change the sort order, click the heading of the appropriate column.

Prefix Event Detail

The Prefix Event Detail report shows how long a problem has been happening and identifies the affected prefixes. For example, you can run this report if the [Route Flap Report](#) report identifies a flapping prefix. You can see how long a prefix has experienced intermittent service and identify 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 generate the Prefix Event Detail report, perform the following steps:

- 1 Open the web application and choose **Reports Portal**.
- 2 Choose **BGP Reports** → **Prefix Event Detail** on the left navigation bar.
- 3 Select the database from the drop-down lists.
- 4 Select a date and time from the Time drop-down lists.
- 5 Enter the in the Prefix text box.
- 6 Click **Create Report**.

The report is displayed. To change the sort order, click the heading of the appropriate column.

Creating BGP Logical Topology Reports

This section describes the following BGP logical topology reports:

- [Route Distribution Detail Route Distribution Detail Report](#) on page 324
- [Redundancy by Prefix Report](#) on page 326
- [Baseline Redundancy by Prefix Report](#) on page 326

- [AS Reachability Report](#) on page 326
- [Baseline AS Reachability Report](#) on page 328
- [Prefix Reachability Report](#) on page 328

To configure a BGP logical topology report, perform the following steps:

- 1 Open the web application and choose **Reports Portal**.
- 2 Click the name of the report to configure in the Logical Topology section.
- 3 On each report page, select the desired database from the **Database** drop-down list.
- 4 Select a date and time from the Time drop-down lists.
- 5 Click **Create Report**.

Route Distribution Detail Route Distribution Detail Report

The Route Distribution Detail report provides an insight into the distribution of BGP routes as determined by the BGP 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.

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 AS number associated with the next hop determined by the BGP path selection algorithm).

Route Distribution Detail By RRC Report

The By RRC (Route Reflect Client) report displays a bar chart showing the number of routes from each route reflector client in the topology. You can then view the route distribution information for a particular route reflector client by entering its address into the RRC Detail text box, and clicking **Create Report**. This produces a report showing a table of the routes from the selected route reflector client.

Route Distribution Detail By Next Hop Report

The By Next Hop report displays a bar chart showing the number routes with each next hop in the topology. You can then view the route distribution information on those routes containing a particular next hop by entering its address into the Next Hop Detail text box, and clicking **Create Report**. This produces a report showing a table of the routes containing the specified next hop information.

Route Distribution Detail By Next Hop AS Report

The By Next Hop AS displays a bar chart showing the number of routes with next hop AS in the topology. You can then view the route distorting information only on those routes containing a particular next hop AS by entering its AS number into the Next Hop AS Detail text box, and clicking **Create Report**. This produces a report showing a table of the routes containing specified next hop AS information.

Route Distribution Detail By Peer Router

The By Peer Router report displays a bar chart showing the number of routes from each peer router in the topology. You can then view the route distribution information for a particular peer by entering its address into the Peer Router Detail text box, and clicking **Create Report**. This will produce a report showing a table of the specified peer routes.

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 where the number of available hops differs from the number of baseline hops (see [Baseline Redundancy by Prefix Report](#) on page 326). This report can be combined with the Baseline Redundancy by Prefix Report to see the comprehensive prefix redundancy of the topology. Use this report 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, so you can quickly and easily identify prefixes that are only available through a single point path.

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.



The baseline number of next hops is calculated by looking at routes that have been up for more than 80% of the time over a course of seven days. For example, 80% of the first 24 hours, 80% of 48 hours, etc.

Baseline Redundancy by Prefix Report

The Baseline Redundancy by Prefix report identifies whether or not each routed prefix on the network is available. Run this report to ensure that all network prefixes are available.

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 where the number of available hops to the AS

differs from the number of baseline hops to the AS, and the paths taken to reach them. Use this report with the Baseline AS Reachability Report on [page 328](#) to see the comprehensive AS reachability for the topology.

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.

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 AS Reachability Report

The Baseline AS Reachability report provides an insight into whether an entire AS is reachable and through what AS paths. This report is normally run to ensure that all ASs are monitored as planned (baseline) and to assist in network planning.

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.



The baseline number of next hops is calculated by looking at routes that have been up for more than 80% of the time over a course of seven days. For example, 80% of the first 24 hours, 80% of 48 hours, etc

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.

The report is displayed in a tabular format with the following data: prefix address, destination AS, next hop, AS path.

8 VPN Routing

This chapter describes how to configure the Multi-Protocol Label Switching Virtual Private Network (MPLS VPN) protocol module and display VPN routing reports.

Chapter contents:

- [About VPN Routing on page 330](#)
- [Understanding the Reachability and Participation Index on page 331](#)
- [Creating Customer and RT Associations on page 332](#)
- [Generating XML Customer Reports on page 335](#)
- [Viewing VPN Routing Reports on page 337](#)



The information in this chapter applies only to units that have licenses for both the BGP protocol and the VPN protocol.

About VPN Routing

The BGP/MPLS VPN, described in RFC 4364, is the most common form of VPN service provider managed. The edge routers of a VPN customer (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 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 destination. The resulting packet is re-encapsulated so that it can be tunneled appropriately over the backbone to the destination 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 4364, a single mesh of tunnels is required between the PE routers. 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 problems with BGP routes can affect normal Internet connectivity.

To manage a large-scale deployment of VPNs in a robust manner, it is important to integrate protocol diagnostics with VPN service metrics such as reachability and participation. The VPN protocol module includes features:

- A VPN topology overlay that lets you visualize the VPN topology on a per-customer basis.
- Summary and detailed views of reachability for advertised prefixes and status of the PE routers.
- Reports that signal problems in the VPN.
- Integrated VPN and BGP routing diagnostics 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.

Understanding the Reachability and Participation Index

Dynamic tracking is provided for every prefix that is advertised from each customer on every VPN. PE routers that participate in each VPN are also tracked.

Reachability and participation metrics normally remain stable in customer networks; however, these metrics change continually in service provider networks. Changes can be caused by periodic addition of new customer sites or VPN prefixes added to existing sites, addition of new PE routers to the network, or 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 VPN stability, a baseline is established with 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. When establishing the baseline, the system looks at routes that have been up for more than 80% of the time over the course of 7 days. (Before a route reaches the 7-day mark, its baseline is determined on a day-to-day basis, such as 80% of 24 hours, 80% of 48 hours.) This number is assigned a stability index of 100. As the number of prefixes or routers change, the corresponding index number changes accordingly.



If you begin recording new routes for an existing database, the system continues to consider the baseline history of routes stored in that database. In the case of PEs, however, historical data is not considered; each time recording is started, the process of determining a baseline begins again.

The system 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 [Viewing VPN Routing Reports](#) on page 337 for information about the available reports.

Creating Customer and RT Associations

Because the MPLS labels of the VPN 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 appliance in the network. See the “Configuration and Management” chapter in the *HP Route Analytics Management System Administrator Guide* for information about how to enable VPN when establishing peering.

However, if you want 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 Routing Reports window.

To configure numerous customer/RT associations at once, it is easier to copy and paste a comma-separated value (CSV) file.

Specify one of the following 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 appliance 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.

Before creating customer and route target associations, you must enable queries on the VPN client. In a deployment with Route Recorders and a centralized Modeling Engine, consider the following recommendations when you enable queries:

- For network-wide information, enable queries on the centralized Modeling Engine.
- For information local to a recorder’s area or protocol, enable queries on the Route Recorder.

To enable queries, perform the following steps:

- 1 Open the web application and choose **Administration**.
- 2 Click **Queries** on the left navigation bar.
- 3 Select **Enable queries**.
- 4 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.
- 5 Click **Update**.

To set up customer/RT associations manually, perform the following steps:

- 1 Open the client application and choose **Administration** → **VPN Customer Configuration** to open the VPN Customer Configuration window (Figure 119).
- 2 Click **Import** and enter customer data using the format

```
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, type each association on a separate line.

- 3 After entering all of the required customer/RT associations, click **Import**.

The new associations appear in the table. 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 window containing the complete list.

The screenshot shows a window titled "VPN Customer Configuration". At the top, there is a "Filter by:" dropdown menu set to "Any", and two buttons: "Show" and "Hide". Below this is a table with three columns: "Name", "Definition", and "Enable Customer Reports". The table contains 18 entries, each with a customer name, a route target (RT) definition, and a checked checkbox in the "Enable Customer Reports" column. At the bottom of the window, there is a status bar showing "128 entries" and four buttons: "Show Enabled", "Auto-Configure", "Import", and "Close".

Name	Definition	Enable Customer Reports
AMD	RT:100:50	<input checked="" type="checkbox"/>
ATT	RT:100:28	<input checked="" type="checkbox"/>
Acer	RT:100:48	<input checked="" type="checkbox"/>
Alibaba	RT:100:5	<input checked="" type="checkbox"/>
Allstate	RT:100:42	<input checked="" type="checkbox"/>
Amazon	RT:100:10	<input checked="" type="checkbox"/>
Apple	RT:100:39	<input checked="" type="checkbox"/>
BT	RT:100:16	<input checked="" type="checkbox"/>
Bell Canada	RT:100:21	<input checked="" type="checkbox"/>
Bestbuy	RT:100:11	<input checked="" type="checkbox"/>
Bloomberg	RT:100:44	<input checked="" type="checkbox"/>
BostonCommunications	RT:100:23	<input checked="" type="checkbox"/>
Broadcom	RT:100:53	<input checked="" type="checkbox"/>
COLA	RT:65470:1	<input checked="" type="checkbox"/>
Charter Communications	RT:100:20	<input checked="" type="checkbox"/>
ChinaTelecom	RT:100:54	<input checked="" type="checkbox"/>

Figure 119 VPN Customer Configuration Configuration Table



If the appliance does not have a VPN Customer Reports license, the Enable Customer Reports column is hidden.

To set up customer/RT associations automatically, perform the following steps:

- 1 Open the client application and choose **Administration** → **VPN Customer Configuration** to open the VPN Customer Configuration window.
- 2 Click **AutoConfigure** (you may need to scroll to see this button).

The AutoConfigure feature uses heuristics to identify a collection of route targets that could plausibly be associated with a single customer. The route targets are selected from the received VPN routes, and the identified customers are named with a “Customer_RT:” prefix.

After the Autoconfig process has finished, the edit option allows customer names to be edited, and the set of associated route targets to be adjusted as needed.

To set up associations by copy and pasting a file, perform the following steps:

- 1 Create a text file with customer data in the following format:

```
cust_id,rt
```

where `cust_id` is a customer identifier, and `rt` is the route target you want to associate with that customer.

To type 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
```

- 2 Copy the contents of the file.
- 3 Open the client application and choose **Administration** → **VPN Customer Configuration** to open the VPN Customer Configuration window.
- 4 Paste the text into the text box near the bottom of the window.
- 5 Click **Submit**.

The new associations are added to the table in the lower portion of the pane.

Generating XML Customer Reports



This feature is available only if the appliance has a VPN Customer Reports license.

The system can generate a set of reports through an XML-RPC interface, which you can make available through a web reports portal for your customers. By default, the ingress PE and egress PE of a particular VPN customer flow are specified as the source and destination customer site for computing site-related statistics.

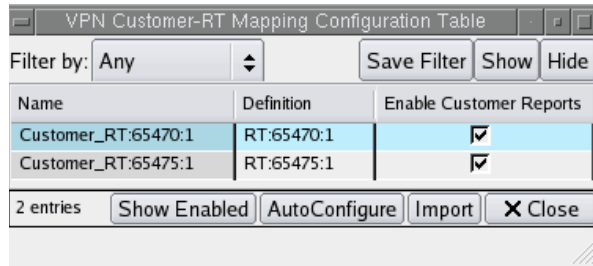
You can change this definition from the web portal and communicate it to the Flow Analyzer and the Modeling Engine through the XML-RPC interface.

You can generate reports for up to 100 customers using this mechanism. The reports are available on the Flow Analyzer or Modeling Engine.

For more information about the XML RPC queries used for the customer reports, see the “VPN Customer Traffic API” chapter in the *HP Route Analytics Management System Administrator Guide*.

To make the XML reports available, perform the following steps:

- 1 Open the client application and choose **Admin** → **VPN Customer Configuration** to open the VPN Customer_RT Mapping Configuration table.



Name	Definition	Enable Customer Reports
Customer_RT:65470:1	RT:65470:1	<input checked="" type="checkbox"/>
Customer_RT:65475:1	RT:65475:1	<input checked="" type="checkbox"/>

Figure 120 VPN Customer_RT Mapping Configuration Table

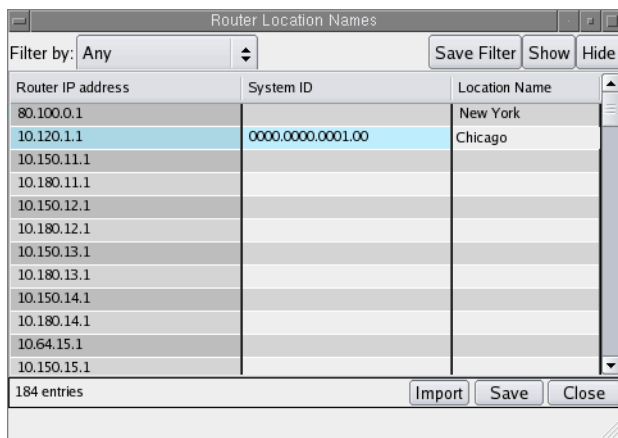
- 2 Perform any of these tasks:
 - Select check boxes for the reports that you want to generate.
 - Click **Show Enabled** to list only the customers for which reports are enabled.
 - Click **Show All** to list all entries in the table.
- 3 Click **Close**.

You can also add names to selected routers to make the customer reports more meaningful. The names are included in the XML file along with the IP addresses.

To add router location names for XML customer reports, perform the following steps:

- 1 Open the client application and choose **Admin** → **Router Location Names**.

- 2 Choose a router from the list and click in the Location Name column.
- 3 Type the location name.
- 4 Click **Save**.



Router IP address	System ID	Location Name
80.100.0.1		New York
10.120.1.1	0000.0000.0001.00	Chicago
10.150.11.1		
10.180.11.1		
10.150.12.1		
10.180.12.1		
10.150.13.1		
10.180.13.1		
10.150.14.1		
10.180.14.1		
10.64.15.1		
10.150.15.1		

Figure 121 Router Location Names

Viewing VPN Routing Reports

In a deployment with multiple Route Recorders and a centralized Modeling Engine, we recommend that you obtain reports from the Modeling Engine. Reports from the Modeling Engine return network-wide information and are faster to obtain than reports obtained directly from Route Recorders.

To access the VPN report pages, perform the following steps:

- 1 Open the client application and choose **Reports** → **Routing Reports**.
The Routing Reports window opens (Figure 122).

The screenshot shows the 'Routing Reports' window with the following data:

Router	IP Address	Type	Protocol	Hardware	Software	State	Area ID	System ID	Area or A
[-] 0100.640									
[-] 0100.640	--	L2 Internal	IP			Up	27.0001	0100.6401	PACKETD
[-] 0100.640									
[-] 0100.640	--	L2 Internal	IP			Up	27.0001	0100.6401	PACKETD
[-] 0101.031									
[-] 0101.031	--	L2 Internal	IP			Up	49.0001	0101.0313	PACKETD
[-] 0101.031	--	L1 Internal	IP			Up	27.0001	0101.0313	PACKETD
[-] 0101.032									
[-] 0101.032	--	L1 Internal	IP			Up	27.0001	0101.0320	PACKETD
[-] 0101.032									
[-] 0101.032	--	L2 Internal	IP			Up	49.0001	0101.0321	PACKETD
[-] 0101.032	--	L1 Internal	IP			Up	27.0001	0101.0321	PACKETD
[-] 0101.032									
[-] 0101.032	--	L2 Internal	IP			Up	49.0001	0101.0321	PACKETD
[-] 0101.032	--	L1 Internal	IP			Up	27.0001	0101.0321	PACKETD
[-] 0200.200									
[-] 0200.200	--	L1 Internal	IP			Up	27.0001	0200.2002	PACKETD
[-] 0300.300									
[-] 0300.300	--	L2 Internal	IP			Up	49.0001	0300.3003	PACKETD
[-] 10.71.2.2									
[-] 10.71.2.2	10.71.2.20	Internal R	IP			Up			PACKETD
[-] 10.71.2.2									
[-] 10.71.2.2	10.71.2.21	Internal R	IP			Up			PACKETD

48 top level entries, 169 total entries

Figure 122 Routing Reports Window

2 Choose individual reports from the tree menu on the left side of the window. The remaining sections in this chapter describe the reports.

Modifying the Report Table

You can modify the report table by right-clicking in the column header and selecting from the following options:

- **Sort**—Sort on the selected column. Click the column header to change the sort order.
- **Group or UnGroup**—Combine elements of the same values in the selected column into a single group, or remove a grouping.
- **Collapse All/Expand All**—Hide all the elements in the groups created in the column, or show all the elements.

- **Hide**—Hide the selected column.
- **Show**—Show a column that was previously hidden.

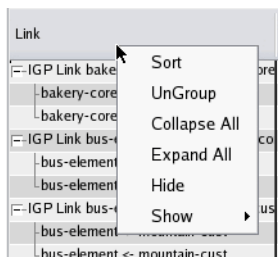


Figure 123 Modifying Report Tables

VPN Summary Report

Choose **Reports** → **Routing Reports** → **VPN** → **Summary** in the client application to open the VPN Summary report (Figure 124). The report displays the following information.

- At the top of the pane, the report contains 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).



See [Chapter 11, “Alerts,”](#) for information about VPN alerts.

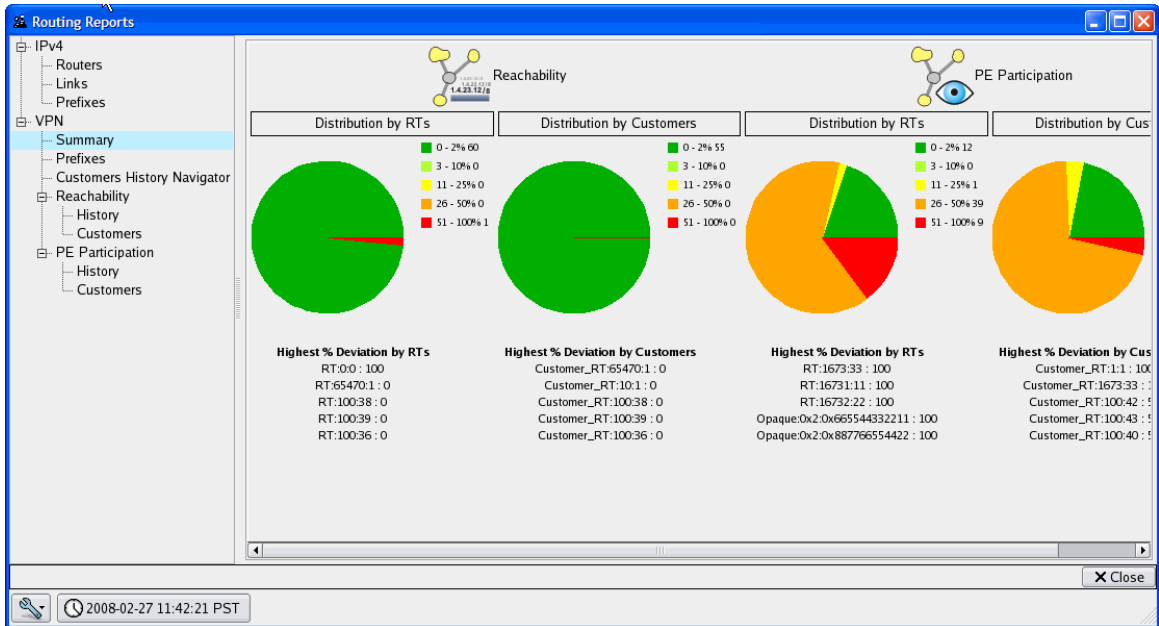


Figure 124 VPN Summary Report

VPN Prefixes Report

Choose **Reports** → **Routing Reports** → **VPN** → **Prefixes** in the client application to open the VPN Prefixes report (Figure 125).

The report lists all prefixes advertised by VPNs in the network with the associated router, attributes, state, and area or AS.

The Filter By menu lets you filter the report to include only the information you want to see. See [Using Filters](#) on page 195. You can resort data by clicking any column heading in the report. Click again to change the sort order (descending/ascending).

Prefix	Router/Net	Attributes	State	Area or AS
65470:1.10.70.102.1/32 468	10.120.1.1	AS Path: 65470 (IGP) Local-Pref: 200 MED: 0 Communities: 22526:20 Originator ID: 10.120.1.6 Cluster List: 10.120.1.1 Ext Communities: RT:65470 MP Reachability Next Hop:	Up/B	PACKETDESIGNLABNETM
65470:1.10.70.103.1/32 467	10.120.1.1	AS Path: 65470 (IGP) Local-Pref: 200 MED: 0 Communities: 22526:20 Originator ID: 10.120.1.6 Cluster List: 10.120.1.1 Ext Communities: RT:65470 MP Reachability Next Hop:	Up/B	PACKETDESIGNLABNETM
65470:1.10.70.104.1/32 466	10.120.1.1	AS Path: 65470 (IGP) Local-Pref: 200 MED: 0 Communities: 22526:20 Originator ID: 10.120.1.6 Cluster List: 10.120.1.1 Ext Communities: RT:65470	Up/B	PACKETDESIGNLABNETM

283 top level entries, 566 total entries

Figure 125 VPN Prefixes Reports

VPN Customers History Report

Choose **Reports** → **Routing Reports** → **VPN** → **Customers History Navigator** in the client application to open the VPN Customers History Navigator report (Figure 126).

This report lists all customer and route target associations. It also includes a mini-History Navigator area at the bottom of the page. A limited set of History Navigator functions is available. For a description of these functions, see [Chapter 4, “The History Navigator”](#)

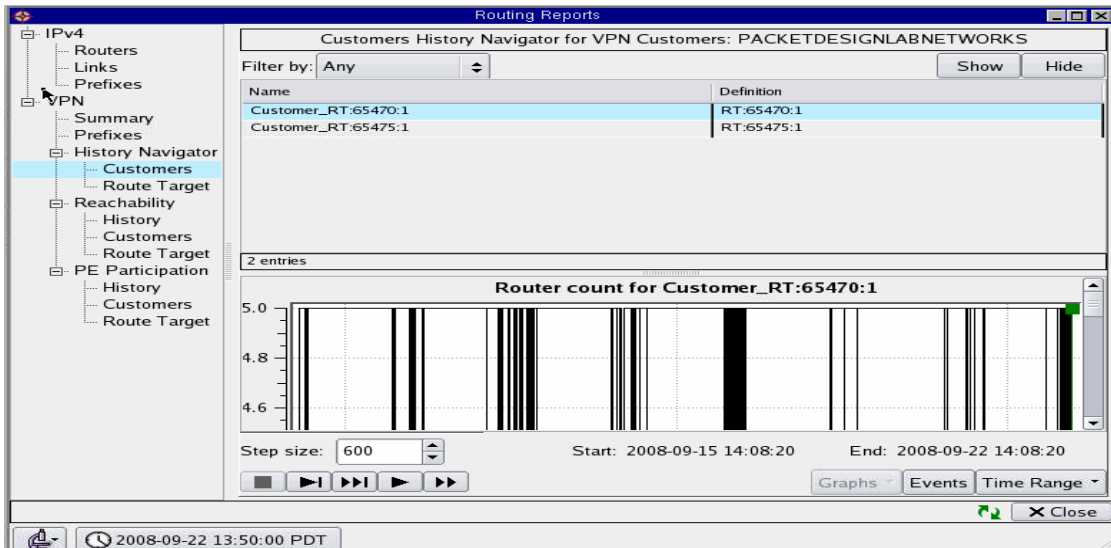


Figure 126 VPN Customers History

VPN Reachability History Report

Choose **Reports** → **Routing Reports** → **VPN** → **Reachability** → **History** in the client application to open the VPN Reachability History report (Figure 127).

The graphs in this report show deviation from the baseline by RT and by customer. The x axis is time and the y axis is percentage of deviation. A limited set of History Navigator functions is available. For a description of the functions, see [Chapter 4, “The History Navigator”](#)

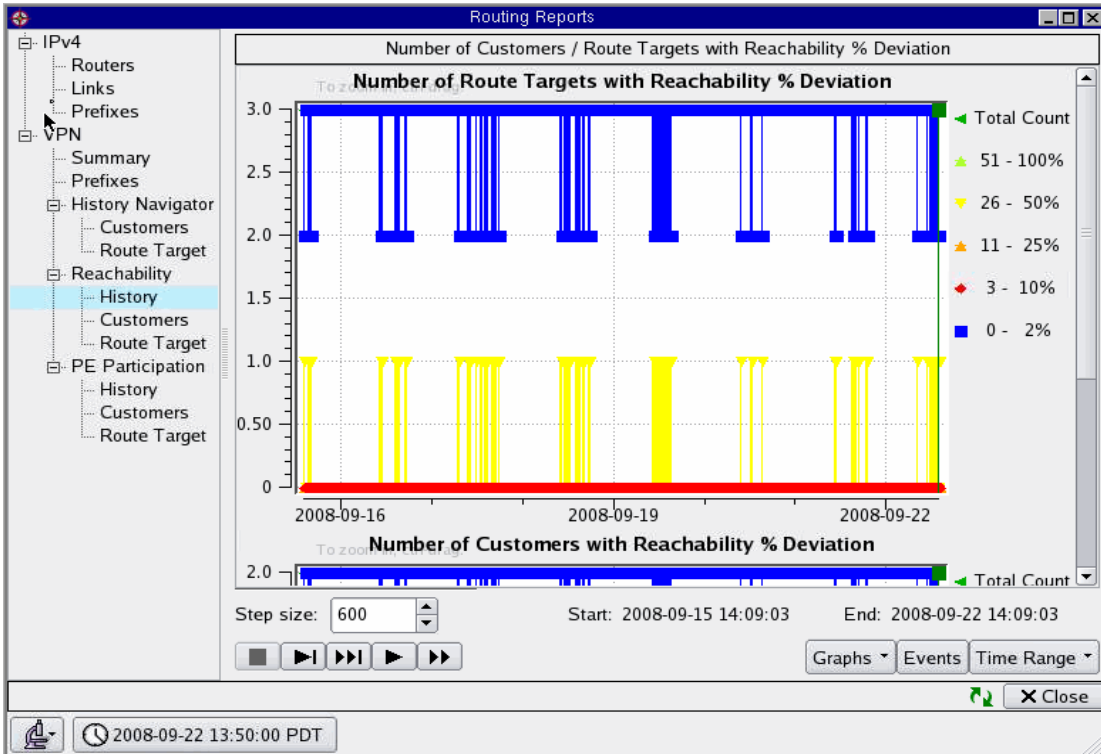


Figure 127 VPN Reachability History Report

VPN Reachability Customers Report

Choose **Reports** → **Routing Reports** → **VPN** → **Reachability** → **Customer** in the client application to open the VPN Reachability Customers report (Figure 128). The VPN Reachability Customers report displays reachability information by individual customer/RT association.

The report includes the customer identifier or RT identifier and the numbers of active PE participants, active routes, baseline routes, down routes, new routes, and the deviation from the baseline.



The Route Target column in the Reachability Summary for Route Targets report may occasionally contain an entry that is a type of extended community other than a Route Target. Use the Show RT communities only configuration option to display only the extended communities that are interpreted as Route Targets in reports and graphs for MPLS VPN networks. See [Miscellaneous](#) on page 71 for a description of the option.

The Filter By menu lets you filter the report to include only the information you want to see. See [Using Filters](#) on page 195. You can resort data by clicking any column heading in the report. Click again to change the sort order (descending/ascending).

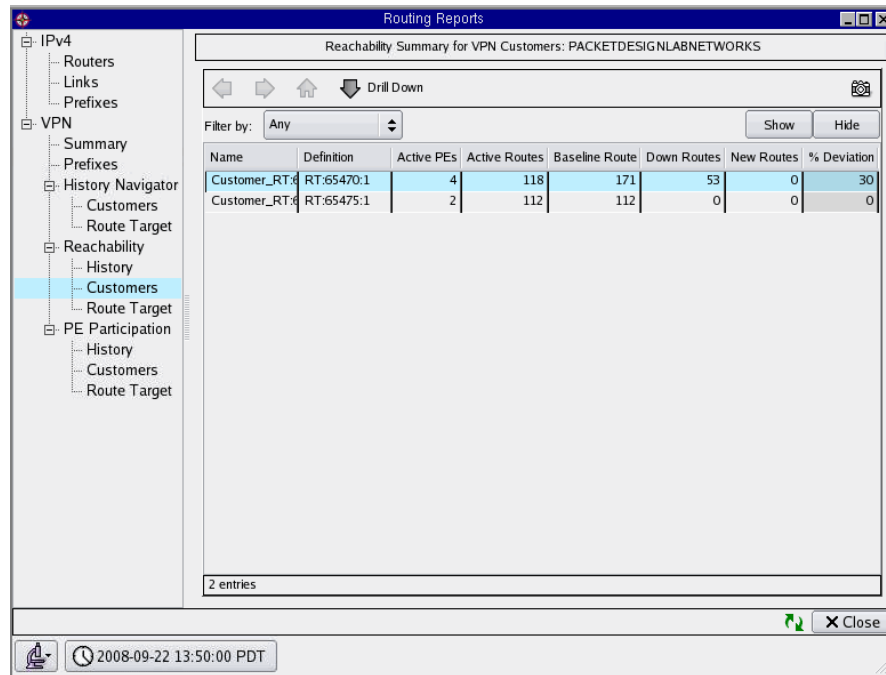


Figure 128 VPN Reachability History Report

VPN PE Participation History Report

Choose **Reports** → **Routing Reports** → **VPN** → **Reachability** → **Customer** in the client application to open the VPN Reachability Customers report (Figure 129).

The graphs in this report show deviation from the baseline by RT and by customer. The x axis is time and the y axis is percentage of deviation. A limited set of History Navigator functions is available. For a description of the functions, see Chapter 4, “The History Navigator”

A limited set of History Navigator functions is available. For a description of the functions, see Chapter 4, “The History Navigator”

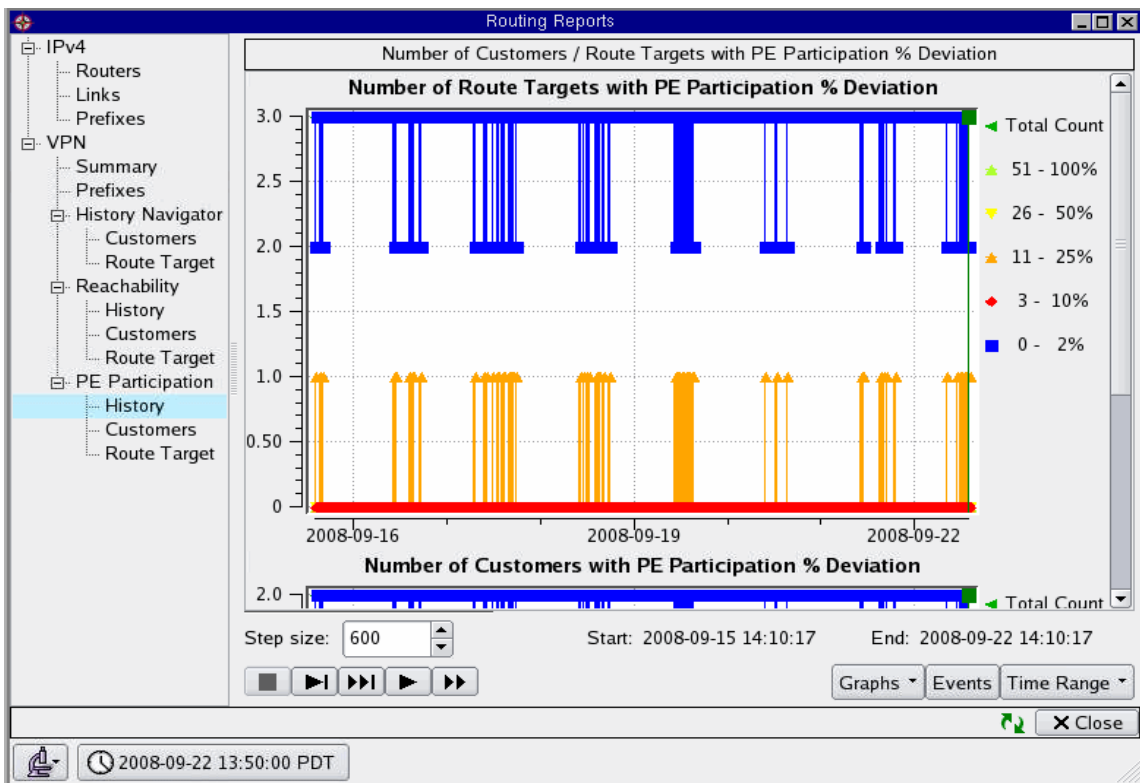


Figure 129 VPN PE Participation Report

VPN PE Participation Customers Report

Choose **Reports** → **Routing Reports** → **VPN** → **Reachability** → **Customer** in the client application to open the VPN Reachability Customers report (Figure 130).

The report displays PE participation information by individual customer/RT association.

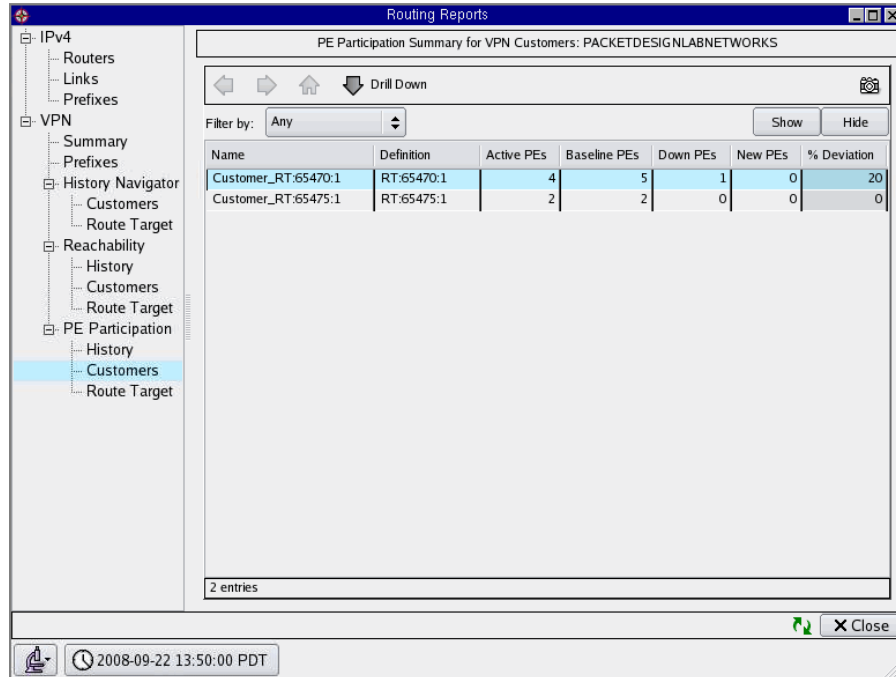


Figure 130 VPN PE Participation Report

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.



The Route Target column in the Reachability Summary for Route Targets report may occasionally contain an entry that is a type of extended community other than a Route Target. Use the Show RT communities only configuration option to display only the extended communities that are interpreted as Route Targets in reports and graphs for MPLS VPN networks. See [Miscellaneous](#) on page 71 for a description of the option.

The Filter By menu lets you filter the report to include only the information you want to see. See [Using Filters](#) on page 195. You can resort data by clicking any column heading in the report. Click again to change the sort order (descending/ascending).

Obtaining Detailed Information

From the Reachability and PE Participation reports, you can display detailed information or focus your attention on specific RTs or customers.

To display the details of a summary report, perform the following steps:

- 1 Open the client application and choose **Reports** → **Routing Reports**.
- 2 Choose **Reachability** → **Customers** or **PE Participation** → **Customers** open the Reachability Summary report or Participation Summary report.
- 3 Right-click an entry in the report to open and choose one of the following options.
 - [Details by PE](#)
 - [List Routes](#) (displays for Reachability Customers section only)
 - [Highlight PEs](#)
 - [Show Map](#)
 - [Reachability over Time](#) (displays for the Reachability section only)
 - [PE Participation](#) (displays for the PE Participation Customer section only)
 - [History Navigator](#)

Details by PE

This option lists all PE routers associated with the selected RT or customer. For each PE router, the report includes the identifier of the PE router, IP address, type, state, and area or AS.

The Details by PE table contains the following buttons:

- **Tear Off** – Creates a new window for the Details by PE report, so you can 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.
- **Reload** – Updates the report with new data.
- **Close** – Closes the Details by PE report.

List Routes

This option lists the routes for the VPN customer. (This option displays for Reachability section only).

Highlight PEs

This option highlights the PE routers that advertise the selected RT or are associated with the selected customer VPN on the routing topology map.

Show Map

This option highlights the portion of the topology map that is utilized for a particular VPN by fading all the other nodes and links. The highlighted links can then be viewed in any of the color modes available for the full map. To return the topology map to its original setting, go to the Traffic Reports window and select the **Restore Map** button.

Reachability over Time

This option opens historical graphs displaying the number of routes associated with a customer or route target over time. You can display the Customer or Route Target graph by selecting the appropriate radio button located at the top of the Reachability Summary window.

For example, open the client application and choose **Routing Reports** → **VPN** → **Reachability** → **Customers**, and select the **Customer** radio button to open the Reachability Summary for VPN Customers window. When you right-click in a customer row, and select the Reachability over Time option, two graphs will open below the table. The top graph shows the history of four number sets over time for a particular customer:

- **Baseline + New:** The number of routes that are up but not yet in the baseline set.
- **Baseline - Down:** The number of routes that are in the baseline set but currently down.
- **Baseline:** The number of routes in the baseline.
- **Active:** The number of active routes.

All four quantities change over time as the routes get advertised and withdrawn, and the baseline computations update the baseline set.

The bottom graph displays the deviation over time (the difference between the number of routes that are up and the number in the baseline).

If you select the **Route Target** radio button in the Reachability Summary window, the Reachability Summary for VPN Customers window opens. The information that displays for the Route Target option is similar to the Customers graphs, except that the information is broken down by RTs instead of by customers.

PE Participation

This option opens a historical graph displaying the number of PE routers associated with a customer or route target over time. You make the choice of viewing either the Customer or Route Target graph by selecting the appropriate radio button, located at the top of the PE Participation Summary window.

The graphs that display provides similar information as the Reachability Summary graphs, discussed in the previous section. The difference being that these graphs display changes (a down router, for example) for a particular PE router.

IPv4 Routers Report

This report lists all IPv4 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 (see [Router List](#) on page 91) or the **List Routers** button on the Topology Map toolbar.

IPv4 Links Report

This report lists all IPv4 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 (see [Links List](#) on page 92) or the **List Links** button on the topology map toolbar.

IPv4 Prefixes Report

This report lists all IPv4 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 (see [Prefix List](#) on page 94) or the **List Prefixes** button on the topology map toolbar.

History Navigator

The VPN Customers History Navigator window is similar to the History Navigator window described in [Chapter 4](#), “[The History Navigator](#)” See that chapter for descriptions of the controls and buttons in the lower portion of the VPN Customers History Navigator window.

9 Traffic Reports

This chapter describes how to use traffic reports to monitor behavior and anticipate usage trends in the network.

Chapter contents:

- [Understanding Traffic Reports](#)
- [Accessing Traffic Reports](#)
- [Working with Traffic Reports](#)
- [Setting Interface Capacities](#)
- [Understanding Report Types](#)
- [Top Changes Report](#)
- [Aggregate Reports](#)
- [IPv4 Traffic Reports](#)
- [BGP Traffic Reports](#)
- [VPN Traffic Reports](#)

Understanding Traffic Reports

Traffic Reports allow you to monitor behavior and anticipate trends of network elements, such as routers, links, customers, and ASs. You can study network element usage, optimize network resource allocation, produce realistic network planning strategies, and troubleshoot and identify network problems.

RAMS constructs traffic reports from real time and historic data generated every few minutes (default is 5 minutes). Incremental data is used to produce hourly, daily, weekly, and monthly data and to determine averages, minimums,

maximums, and 95 percentiles. The resulting statistical and trend reports show bandwidth utilization, packet and protocol distribution, and error and outage information. Many of the reports have drill-down options.

The report data is collected and correlated from the Flow Collector and the Route Recorder and processed by the Flow Analyzer. Some data is concealed by prefix-level aggregation so that only the Flow Collector (not the Flow Analyzer) can generate reports for this concealed data.

Examples of this data include:

- Top source addresses
- Top destination addresses
- Traffic distribution per protocol
- Traffic distribution per Flow Collector

The Flow Collector generates data for the 5-minute reports. The Flow Analyzer obtains the data from multiple Flow Collectors and aggregates the data into hourly, daily, weekly, and monthly data sets. For example, you can compare utilization values of the network elements listed in the table to find over- and under-utilized links and make changes to help route traffic more evenly among the links.

Traffic data is based on the time that is displayed in the status bar at the bottom of the routing topology map window in the client application. For current data, there is typically a 30-minute delay, although data acquisition time varies based on the complexity of your network. See [Main Window Status Bar](#) on page 47 for instructions on changing the date, time, and modes.

You can view and analyze traffic distribution over the network for the following protocol families:

- IPv4
- VPN

Aggregate reports are available only when your network uses more than one protocol. All aggregate reports include data from all Flow Collectors known to the Flow Analyzer.

Right-click options are available with most data fields within the workspace. These options can duplicate or extend drill-down functionality, as described in [Understanding Report Types](#) on page 367.



Traffic data is based on the time appearing in the status bar, which you can change to review any previous data. For current data, there is typically a 20- to 30-minute delay, although data acquisition times varies based on the complexity of your network.

Accessing Traffic Reports

The following conditions are required to access traffic reports in the client application:

- You must have a license for RAMS Traffic SPI.
- The topology that you open must include a Traffic Reports database (which has a corresponding routing database).
- The Flow Collector database must be open.

To access Traffic Reports, perform the following steps:

- 1 Open the client application and choose **Reports** → **Traffic Reports** to open the Traffic Reports window (Figure 131).

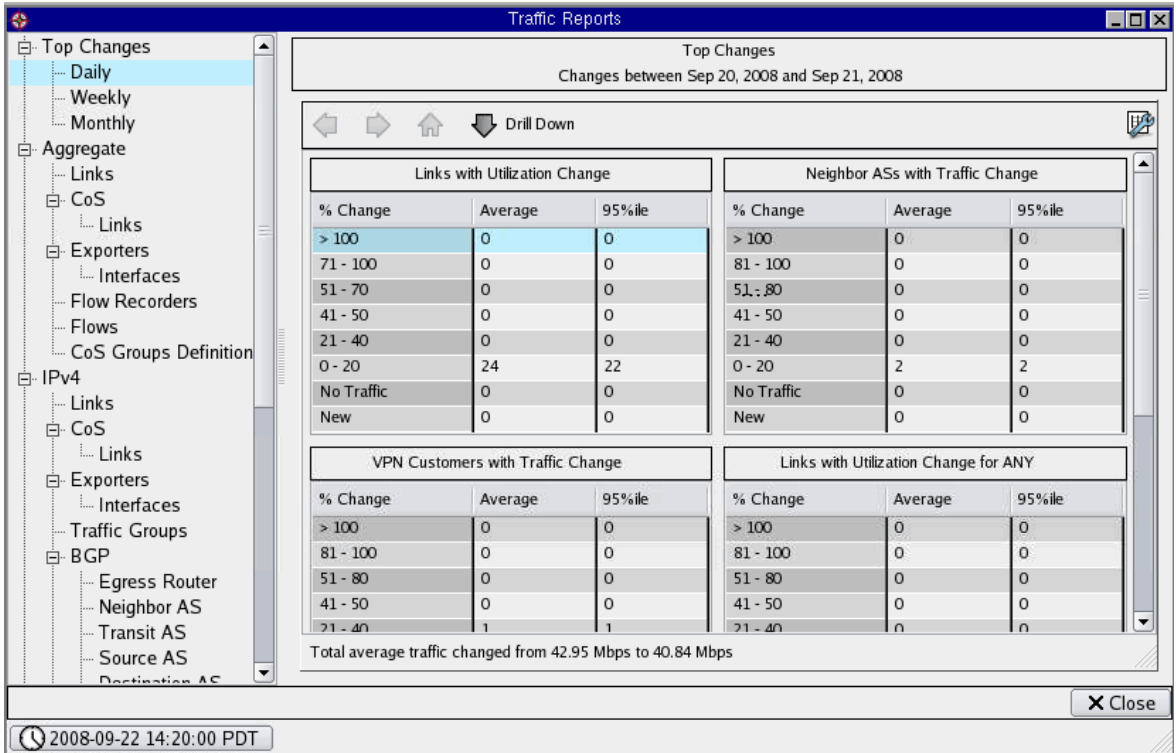


Figure 131 Traffic Reports Window

- 2 Choose individual reports from the tree menu on the left side of the window.

Navigation Tree

The navigation tree in the left pane is grouped by protocol families in your network. If your network supports multiple protocols, you will see an Aggregate category and a category for IPv4 and VPN traffic. If your network supports only one protocol there will not be an Aggregate category.

You can expand or compress any category preceded by a plus or minus symbol. Within each category are reports that contain diagnostic information.



Traffic reports for protocol families appear only if the protocol is configured and only if that specific license has been purchased.

Traffic Reports Buttons

The following buttons are available in Traffic Reports. Some of these icons are present for particular tables or conditions; those conditions are noted, below:

Table 37 Traffic Report Buttons













	Go back one drill-down	During a drill-down, goes back one drill-down level.
	Go forward one drill-down	During a drill-down, goes forward one-drill down level.
	Go back to top; undo all drill-downs	Goes to the highest point in the drill-down hierarchy, and “unrolls” the drill-down view from the window.
	Configure	Allows you to add columns or modify the data within a column using conditions and parameters. For Top Changes reports, allows you to set up ranges.
	Color Links By Traffic Volume	Each link is colored according to according to the aggregate traffic volume of all flows traversing the link. The legend indicates the correspondence between colors and levels of traffic volume. Note: This icon is present for any report or drill-down based on links.
	Advanced Filter	Allows you to define advanced filters. Refer to Understanding Report Types on page 367 and Using Filters on page 195 for more information.
Restore Map	Restore Map	Displays after the Show Map feature is evoked. This is done by right-clicking a row in a VPN traffic report that is broken down by customer.
	Snapshot	Opens a new window containing a snapshot of the current window.
	Table	Changes the workspace data to columns and rows. (This button is not always available.) This icon is present for Top Sources, Top Destinations, and Protocol reports.
	Pie Chart	Changes the workspace data to a pie chart. This icon is present for Top Sources, Top Destinations, and Protocol reports.


Table 37 Traffic Report Buttons (cont'd)

	Bar Graph	Changes the workspace data to a bar graph. This icon is present for Top Sources, Top Destinations, and Protocol reports.
	Drill-down	If available, this button allows to see finer detail within a set of data.
	Close	Closes the Traffic Reports workspace.

Working with Traffic Reports

Most reports allow you to edit, move, or add columns appearing in the report.

Columns Settings

Most traffic reports allow you to manipulate columns or customize the data in existing columns by clicking the configuration icon , which opens the Traffic Reports Columns window (Figure 132).

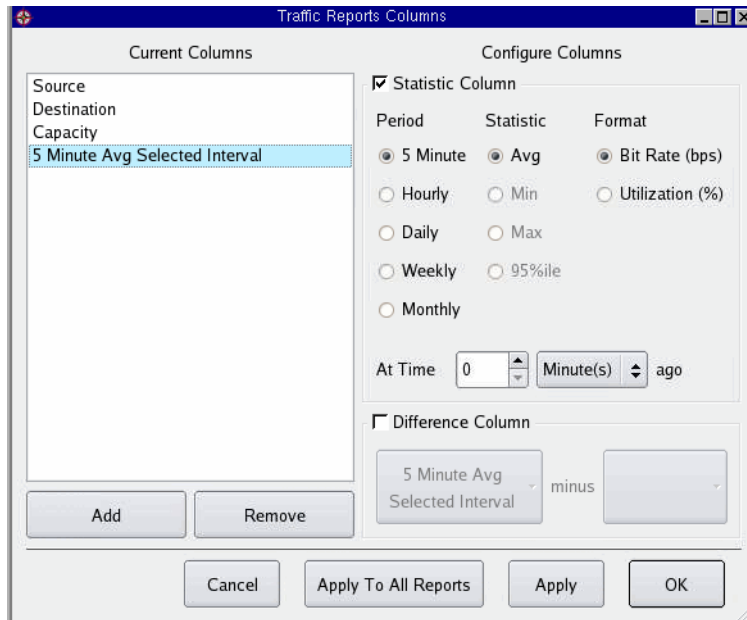


Figure 132 Traffic Reports Columns



The available Configure columns vary. You can modify the Statistic (including the default 5 Minute Average column) or Difference Column. Do not delete or change the default 5 Minute Avg Selected Interval column if you want to retain drill-down capability.

If you click **Apply to All Reports**, all statistic and difference columns in all other reports are replaced by those appearing the current Traffic Reports Columns window. This process cannot be undone.

Statistics Column Area

The Statistics Column area allows you to create additional columns defining new data parameters. Periods are based on the time appearing in the status bar. Within the available periods, you can select from the following options:

- **5 Minute** – Last 5 minutes of available data based on the standard 5-minute increments of a clock. For example, if you choose this option and the time is set between 1:30 and 1:34, data is retrieved for the period 1:25 to 1:30.
- **Hourly** – Last 1 hour of available data from the time appearing in the status bar based on the standard twelve 1-hour increments of a clock. For example, if you choose this option and the time is set for 1:30, data is retrieved for the period 12:00 to 1:00.
- **Daily** – Last full day (12:00:01 am to 11:59:59 pm) of available data from the time appearing in the status bar. For example, if you choose this option and it is Tuesday, data is retrieved for the previous Monday.
- **Weekly** – Last full week (Monday to Sunday) of available data from the time appearing in the status bar. For example, if you choose this option and it is Friday, data is retrieved for the period Monday to Sunday of the previous week.
- **Monthly** – Last calendar month of available data from the time appearing in the status bar.
- **At Time** – Specific time intervals for obtaining report data.

Within the available statistics options are:

- **Average** – Sum of all selected values divided by the total number of elements.
- **Minimum** – Lower bounds within a group of values.
- **Maximum** – Upper bounds within a group of data.
- **95 percentile** – Value equal to or greater than 95 percent of the values.

Selecting reports on links allows you to create additional columns related to the Average statistic:

- **Bit Rate (bps)** – Bit rate level that a link is reaching.
- **Utilization (%)** – Percentage of use that a link is achieving if capacity is configured.

Difference Column Area

The Difference Column area allows you to create a new column that generates data based on subtracting one statistics column from another. The applicable statistic columns appear in the drop-down lists within the Difference Column area.

Advanced Filtering

Simple filters let you choose a single operator from a list and specify one or more parameters to be matched or excluded.

Advanced filters let you choose two or more different operators from a list and specify their corresponding parameters to be matched or excluded. From a Filter workspace, select the drop-down list in the Filter by field and choose **Advanced**. The Composing Advanced Filter window opens.



Figure 133 Composing Advanced Filter



Advanced filtering may not be enabled for all reports.

See [Using Filters](#) on [page 195](#) for more information.

Minute Data Granularity

You can reset the clock to retrieve data based on minute granularity. This can be useful information if you need to determine the environment at a specific moment. However, depending on the amount of data involved, retrieving

granular data can be a resource-intensive process and require additional time in retrieving and displaying the data. This type of information automatically creates a 5 Min Avg Current Time column in the report.

Drill-Down Capabilities

A measure is a metric or a performance indicator used to determine how well routing and traffic are operating. The aggregated data you need to examine are called measures — numeric values that are measurable and additive. You can also examine measures under certain conditions called “dimensions.”

Dimensions are often time-based, such as by day, week, or month. Dimensions can have a hierarchy that allows you to perform drill down functions on the data.

Traffic Reports contains measures (data) organized by different dimensions to provide faster retrieval and drill-down capability. Drill-down allows you breakdown data into finer detail. Many report measurements offer the ability to take summary information and drill-down through a hierarchy to show the detailed data used to develop the summary data. Drill-down capability is not available for all measures, either because finer detail is not stored or you have already reached the finest detail. The values you see when you drill-down can vary, depending on the drill-down selections you have made.



You can select multiple rows to drill-down by selecting Ctrl + Shift keys, and then selecting the rows you want to drill-down.

When the **Drill-Down** button appears, you can gain additional detail for any of the following:

- **Community**—displays how much traffic each community receives in bits.
- **CoS**—displays the class of service for the traffic flow.
- **CoS Group**—displays a user-defined CoS group name.
- **Customer**—displays the user-defined customer ID.
- **Destination AS**—identifies the name or AS number of the final AS.
- **Egress PE**—identifies the router from which flow exits the current AS.
- **Egress Router**—identifies the router from which flow exits the current AS in a VPN topology.

- **Exit Router**—identifies the name or IP address of the exit router used to reach a peer. This information is obtained from the router name repository prioritized by router names, DNS names, IP address, and system IDs. For more information regarding the router name repository, see [Assigning Router Names](#) on page 88.
- **Exit Router-Next Hop**—identifies the IP address of next hop.
- **Exporter**—identifies the name or IP address of the peer from which flow information was received.
- **Exporter Interface**—identifies the interface of the peer from which flow information was received.
- **Interfaces**—identifies the name or IP address of peer from which flow information on the interface it exited from.
- **Flow Collector**—identifies each Flow Collector on the network.
- **Flows**—displays the details of each traffic flow.
- **History**—Displays detailed routing history for the network using graphs and trending. For more information about this feature, see [Drill-Down History Option](#) on page 363.
- **Ingress PE**—identifies the name or IP address of peer from which flow information was received.
- **IPv4 Flows**—displays details of each IPv4 traffic flow
- **Link**—displays how much traffic each link is carrying.
- **Neighbor AS**—identifies the name or AS number of directly connected AS to which traffic is being sent.
- **Source AS**—identifies the name or AS number of the AS from which the flows originated.
- **Traffic Group**—displays a user-defined group name. For more information about creating traffic groups, see [Creating Groups Using the Menu](#) on page 104.
- **Transit AS**—displays the name or AS number of each transit AS used in delivering data to a destination.
- **VPN Flows**—displays the details of each VPN traffic flow.

Viewing the summary data helps show the general utilization of your network elements, while dividing the data into more specific segments can help you analyze and troubleshoot your network elements more accurately.



Depending on the amount of data involved, drilling down can be a resource-intensive process and may

The following example displays the drill-down from the BGP Flows report to show the links for specified flows.

The screenshot shows the 'Traffic Reports' window with the 'Flows -> Links' view. The left navigation pane is expanded to 'BGP' > 'Flows'. The main area displays a table of flow data and a drill-down table.

Flow Source	Flow Destination	Exporter	Traffic Group	CoS Group	5 Minute Avg Current Time
10.120.1.1/32	10.64.14.0/24	10.120.1.13:2	Other	exp0	273.00 Kbps

Link Source	Link Destination	5 Minute Avg Current Time
CORE-ROUTER13	CORE-ROUTER13.02	273.00 Kbps
CORE-ROUTER13.02	ROUTER10	273.00 Kbps
ROUTER10	SF-CORE-ROUTER2.04	273.00 Kbps
SF-CORE-ROUTER2.04	SF-CORE-ROUTER2	273.00 Kbps
SF-CORE-ROUTER2	10.64.14.0/24	273.00 Kbps

Figure 134 Example of Drill-Down to Identify BGP Flows on a Link

Drill-Down History Option

The History option delivers ways for you to obtain graphical representation of past traffic trends, enabling you to anticipate and plan for future traffic needs. To access this option, select a report type from the left navigation pane, and then select the element you wish to view traffic data for. Next, select **Drill-Down>History**.

The History window opens.

Several features within this option provide you with more tools to examine traffic data:

The **Trend** drop-down menu opens the Trending window (shown below). This feature provides a way for you to project and estimate traffic statistics at the selected future date and time. Either a Linear or Exponential model can be used for this estimation. Your organization can use this information to allocate your future traffic needs.

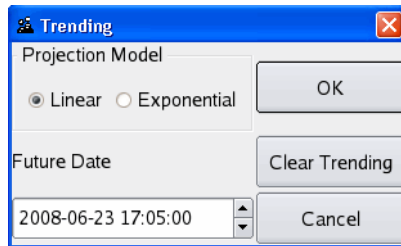


Figure 135 Trending

- The **Graphs** drop-down menu displays, by default a “best fit” (in other words, the best traffic data available) graphical representation of past traffic data for the selected network element(s). The **Graphs** drop-down menu provides the option to show/hide other graphs, including the default graph. There is one graph for each of the reports that displays in the top level report.



The default time range for the graphs is seven days.

- The **Time Range** drop-down menu provides a selection of time periods (including a custom time frame) to confine the graph to.

Columns in the History window enable you to select the reports to be shown simultaneously. For more information about Columns in Traffic Reports, see [Columns Settings](#) on page 357.

Setting Interface Capacities

In order to compute percentage utilization across the links, RAMS Traffic must be able to determine the capacity of link interfaces. Some protocols (ISIS with TE enabled or EIGRP) allow the system to determine the capacity directly, and capacity can also be determined through static data collection.

To accommodate other situations and also permit additional capacity adjustments, RAMS Traffic allows you to configure interface capacities manually. This is useful for situations in which the capacity is not automatically discovered or there are conflicts in the capacities that are reported for different protocols or physical links.

The following use cases may arise:

- Multiple physical links between the same two routers—The system automatically sums the capacities for the different physical links.
- Multiple protocols over a single physical link. If the individual protocols are reporting capacities, then the following rules are automatically applied to determine default capacity:
 - If the same capacity is reported for different multiple protocols, that capacity is used by default.
 - If different capacities are reported for the multiple protocols (or only some capacities are reported), then the largest reported capacity is used by default.
 - If the capacities are not known, then it is necessary to assign capacities manually.

In all of these cases, you can adjust capacity on a per-interface basis by directly setting the capacity. If you configure a capacity for protocol instance on a physical link, that configured capacity supersedes all of the discovered capacities for that physical link.

For IGP interfaces, the system provides the option of configuring a reference bandwidth, which is used with an automatically-generated metric to determine the capacity according to the formula (capacity = reference bandwidth / metric).

To set interface capacities, perform the following steps:

- 1 Open the client application and choose your database to open the routing topology map.
- 2 Choose **Monitoring Mode** or **Analysis Mode**. You cannot set interface capacities in Planning mode.
- 3 Choose **Administration** → **Set Interface Capacities** to open the configuration options window.

The window presents information in a hierarchy, with the top level entry identifying a router-router link and each sub-entry representing an individual protocol. A top level entry has multiple sub-entries if there are multiple protocols running over a single physical link or multiple physical links running in parallel between routers.

After you modify capacities at the sub-entry level, the system can consolidate the results to generate a capacity for the overall link (top level entry).

The screenshot shows a window titled "Set Interface Capacities" with a table of network links. The table has columns for Source, Destination, Interface, Area, Discovered Capacity (bps), Configured Capacity (bps), and Metric. The first row is expanded to show sub-entries. Annotations with arrows point to the first row as the "Top level entry" and the first sub-row as the "Sub-entry".

Source	Destination	Interface	Area	Discovered Capacity (bps)	Configured Capacity (bps)	Metric
Static Link SF-PE2-ROUTER8.packetdes...						
└ SF-PE2-ROUTER8.packetdesign.com	10.74.1.0/24	10.74.1.8	PDI.Static/snmp	100.00M	100.00M	
└ SF-PE1-ROUTER6.yourdomain.com	30.30.30.0/24	30.30.30.6	PDI.Static/snmp	100.00M	100.00M	
└ SF-PE1-ROUTER6.yourdomain.com	10.70.1.0/30	10.70.1.1	PDI.Static/snmp	100.00M	100.00M	
└ SF-PE1-ROUTER6.yourdomain.com	10.78.1.5	10.78.1.6	PDI.Static/snmp	1.54M	100.00M	
└ Core-Router14.packetdesign.c...						
└ Core-Router14.packetdesign.com	10.77.1.0/24	10.77.1.14	PDI.Static/snmp	10.00M	100.00M	
└ LA-CORE-RTR5	10.64.15.0	10.64.15.5	PDI.Static/snmp	100.00M	100.00M	
└ LA-CORE-RTR5	192.168.0.0/24	192.168.0.5	PDI.Static/snmp	100.00M	100.00M	
└ LA-CORE-RTR5 -> 192.168.0.0/24	192.168.0.0/24	192.168.0.5	PDI.Static/snmp	100.00M	100.00M	
└ LA-CORE-RTR5	10.71.6.0/24	10.71.6.5	PDI.Static/snmp	100.00M	100.00M	
└ OSPF-SITE-CE-RTR21.packetdesign.c...						
└ OSPF-SITE-CE-RTR21.packetdesign.c...	10.71.1.0/24	10.71.1.21	PDI.Static/snmp	100.00M	100.00M	
└ SF-CORE-ROUTER2 -> 10.64.14.0/24	10.64.14.0/24	10.64.14.2	PDI.Static/snmp	100.00M	100.00M	
└ SF-CORE-ROUTER2	10.64.14.0/24	10.64.14.2	PDI.Static/snmp	100.00M	100.00M	
└ ROUTER11 -> 167.130.1.5	167.130.1.5	167.130.1.6	PDI.Static/snmp	1.54M	100.00M	
└ ROUTER11	167.130.1.5	167.130.1.6	PDI.Static/snmp	1.54M	100.00M	
└ ROUTER11 -> 192.168.122.0/24	192.168.122.0/24	192.168.122.50	PDI.Static/snmp	10.00M	100.00M	
└ ROUTER11	192.168.122.0/24	192.168.122.50	PDI.Static/snmp	10.00M	100.00M	
└ ROUTER32.packetdesign.com						
└ ROUTER32.packetdesign.com	10.71.7.0/24	10.71.7.32	PDI.Static/snmp	10.00M	100.00M	
└ SF-CORE-RTR1.packetdesign...						

Figure 136 Set Interface Capacities Window

- 4 Choose a desired filtering option, if needed, to display the entries of interest.
- 5 Choose one of the following options:
 - To change the capacity for a single sub-entry, click the **Configured Capacity** column and enter the value. The default units are bits per second (bps). You must enter K, M, or G to specify Kbps, Mbps, or Gbps.
 - To modify the capacities for the full table, choose **Change** → **All**.
 - To configure the capacity for multiple rows, select the sub-entry rows and choose **Change** → **Selected**.
- 6 If you choose one of the **Change** options, the Change Interface Capacity window opens.

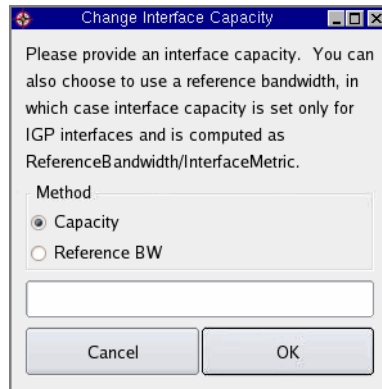


Figure 137 Setting Interface Capacity

- 7 Choose one of the following options:
 - Select the **Capacity** button and enter the desired capacity. If you choose this option, no additional metric is calculated.
 - (ISIS and OSPF only) Choose the **Reference BW** button and enter the bandwidth. ISIS and OSPF have a mechanism that allows the system to compute a metric according to the link's actual capacity (metric=reference bandwidth/capacity).



The default units are bits per second (bps). You must enter K, M, or G to specify Kbps, Mbps, or Gbps.

8 Click **OK**.

The window closes, and the Set Interface Capacities window displays the changes.

9 Choose one of the following actions:

- Click **Apply** to apply the values in the Configured Capacity column to the working topology model. (**Apply** is automatically performed when you click **OK** in the Change Interface Capacity window, as described in step 8.) If you enter a value in the Configured Capacity column and then close the window without saving or applying, the change is lost.
- Click **Save** to perform an **Apply** operation and then save new values to the database. You must choose this option to keep the applied changes after closing the topology.
- Click **Cancel** to remove any unsaved changes made to the table since it was opened, whether or not those changes have been applied. If you make a change, click **Apply** or **Save**, and then close the table and reopen it, the change will be visible and Cancel will not remove it
- Click **Import** to reload all configured capacities from the database (global).

Understanding Report Types

There are four categories of report types available within Traffic Reports:

- Flow Analyzer reports contain history, period (5 minute, hourly, weekly, monthly), statistical data (average, minimum, maximum, and 95th-percentile). These are reports that include the **Columns** button.
- Flow Collector reports contain data from the last 5 minutes. These are the IPv4 Top Source Address, IPv4 Top Destination Address, and IPv4 Protocols reports.
- Reports with no history that are created on-the-fly. These are the Aggregate Flows, BGP Community, IPv4 Flows, and VPN Flows reports.

- General information reports that contain configuration information and do not change based on any time change. This type of report is represented by the Traffic Groups Definition report.

The navigation tree contains only those protocols identified on your network, have been loaded and opened, and for which you have purchased a license. This section provides a list of all default measures and dimensions within each report. This list is presented alphabetically and does not match the flow within the navigation tree. Your configuration may differ. Following the descriptions of each default report are suggestions for other useful measures.

The following diagram is intended to help clarify the content that appears within Traffic Reports by defining terms. All reports are based on your administrative domain being the central location.

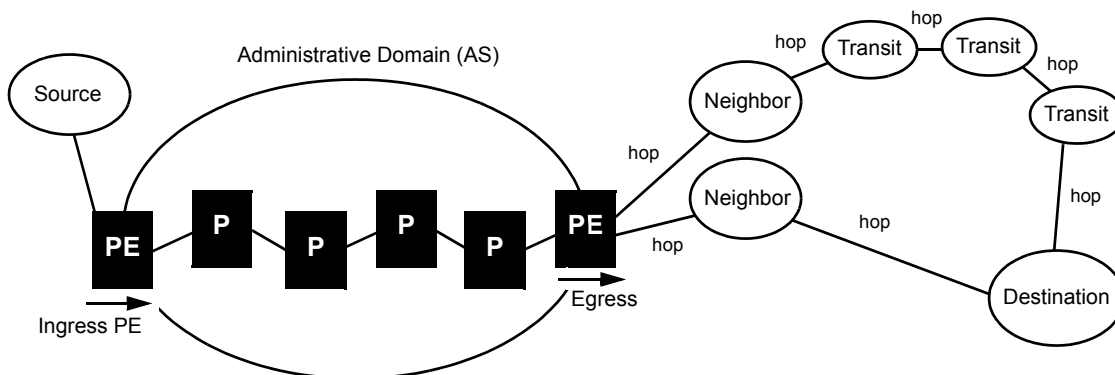


Figure 138 Graphical Representation of Networking Concepts


Note the following observations:

- Each source, neighbor, transit, and destination AS is an administrative domain. Administrative domains are based on perspective; for example, a transit is also a destination, neighbor, and source in relation to other administrative domains.
- Each administrative domain is connected to multiple administrative domains. Typically there are multiple entry and exit points for data flow within an administrative domain.
- Multiple Provider Edge (PE) routers can be connected to the Provider (P) routers. Only two PE routers are shown in Figure 138 for the ingress (data coming in) and egress (data going out) examples.


Top Changes Report

Top Changes Report highlights the top traffic changes across the entire network. Choose the daily, weekly, or monthly time frame, as shown in [Figure 139](#).



If CoS groups are not configured, a message is shown in red at the bottom of the window when you open any of the Top Changes reports (Table 37). To include reports on CoS groups, click the configuration icon  in the Top Changes window and select the desired CoS groups under the Link Utilization by CoS menu option (see next procedure). When you apply your changes, a new table is added to the Top Changes report for each of the CoS groups. For information on creating definitions of CoS groups see the “Administration” chapter in the *HP Route Analytics Management System Administrator Guide*.

Traffic Reports
Top Changes
Changes between Sep 20, 2008 and Sep 21, 2008

← → ⏪ ⏩ Drill Down 

Links with Utilization Change			Neighbor ASs with Traffic Change		
% Change	Average	95%ile	% Change	Average	95%ile
> 100	0	0	> 100	0	0
71 - 100	0	0	81 - 100	0	0
51 - 70	0	0	51 - 80	0	0
41 - 50	0	0	41 - 50	0	0
21 - 40	0	0	21 - 40	0	0
0 - 20	24	22	0 - 20	2	2
No Traffic	0	0	No Traffic	0	0
New	0	0	New	0	0

VPN Customers with Traffic Change		
% Change	Average	95%ile
> 100	0	0
81 - 100	0	0
51 - 80	0	0
41 - 50	0	0
21 - 40	1	1

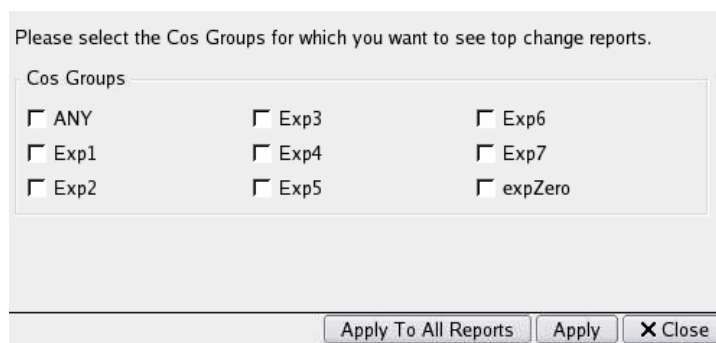
Total average traffic changed from 42.95 Mbps to 40.84 Mbps

2008-09-22 14:20:00 PDT **No Cos Groups selected for Link Utilization by Cos Reports** Close

Figure 139 Top Changes Report Window

To modify the information presented in the display, perform the following steps:

- 1 Open the client application and choose **Reports** → **Traffic Reports** to open the Traffic Reports window (Figure 9-1).
- 2 Click the **Configure** button to open the Configure Traffic Change Reports window (Figure 140).
- 3 Choose one of the following categories to modify:
 - **Link Utilization**—Select to compute the traffic changes for each link found in the network.
 - **Neighbor A bitrate**—Select to compute change in traffic traveling to each Neighbor AS.
 - **VPN Customer bitrate**—Select to compute traffic changes per VPN customer.
 - **Link Utilization by CoS**—Select to compute the traffic changes for the selected CoS links found in the network.



- 4 Enter ranges for the top changes, where each entry represents the upper bound of a range. For example, the ranges shown in Figure 140 correspond to ranges 0-20, 20-40, 40-60, 60-80, and 80-100.

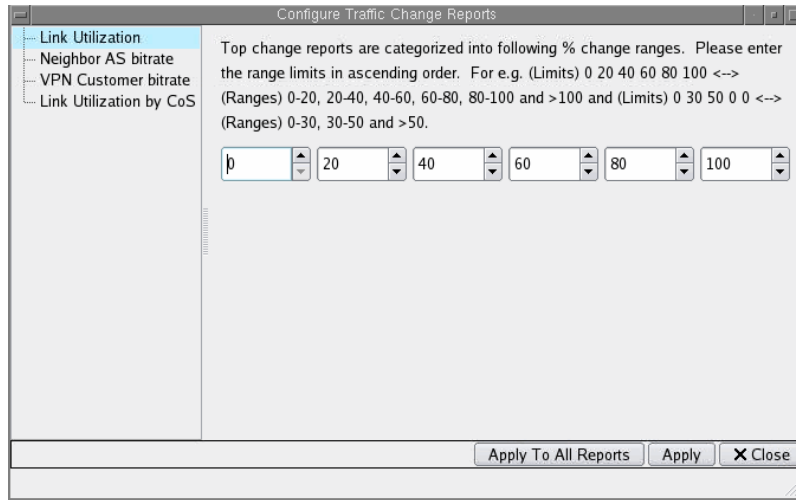


Figure 140 Configure Traffic Change Report Window

- 5 Click **Apply**.

Aggregate Reports

Aggregate Reports are available only when your network uses more than one protocol family. All aggregate reports include data from all Flow Collectors known to the Flow Analyzer. You cannot dynamically change the set of Flow Collectors. The Aggregate reports always shows a network view that is as complete as possible. By default, these reports cover the most recently recorded five minutes of traffic activity.

Aggregate – Links

The Links report shows the combined total of all IPv4 and VPN traffic links in the network, and allows you to color links on the topology map based on traffic volume. The default fields for the Links report are shown in the following table.

Table 38 Aggregate – Links

Measure	Description
Source	Source router ID of an identified pair.
Destination	Destination router ID of an identified pair.
Capacity	The amount of Egress traffic the link is capable of handling, in bits per second (bps).
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.



Color by Links is enabled only if the **5 Minute Avg Selected Interval** column is present in the window.

Drill-down options for the Links report include the following:

- Link
- Exporters
- Exporter Interface
- Flow Collector
- Flows
- IPv4 Flows
- VPN Flows
- CoS Group
- History

Aggregate—CoS

This report displays the total of all IPv4 and VPN traffic seen with a particular CoS group.

Table 39 Aggregate - CoS

Measure	Description
CoS Group	User-defined name for the Class of Service group.
5-Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the CoS report include the following:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Egress Router
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- Ingress PE
- Egress PE
- Flows
- IPv4 Flows
- VPN Flows
- Link
- Traffic Group
- Customer
- History

Aggregate—CoS Links

The Links report shows the combined total of all IPv4 and VPN traffic links associated with a particular CoS in the network.

Table 40 Aggregate - CoS Group

Measure	Description
Exporter	Name or IP address of peer from which flow information was received.
5-Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the CoS Links report include the following:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Egress Router
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- Ingress PE
- Egress PE
- Flows
- IPv4 Flows
- VPN Flows
- Link
- Traffic Group
- Customer
- History

Aggregate – Exporters

This report lists the total of all IPv4 and VPN Exporters traffic on the network. The default fields for the Exporters report are shown in the following table.

Table 41 Aggregate – Exporters

Measure	Description
Exporter	Name or IP address of peer from which flow information was received.
5-Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Exporters report include the following:

- Link
- Flow Collectors
- Traffic Group
- Egress Router
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- Customer
- Ingress PE
- Egress PE
- Flows
- IPv4 Flows
- VPN Flows
- Exporter Interface



If an Exporter is not present in the topology, the **Exporter** column is listed as unknown.

Aggregate – Exporters Interfaces

This report lists each router used for obtaining traffic data. The default fields for the Interfaces report are shown in the following table.

Table 42 Aggregate – Exporter Interfaces

Measure	Description
Exporter: Interface Index	Identifies a network interface on the exporting router by its SNMP interface index.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Interfaces report include:

- Link
- Flow Collector
- Flows
- IPv4 Flows
- VPN Flows
- History

Aggregate – Flow Collectors

This report lists each Flow Collector on the network. The default fields for the Flow Collectors report are shown in the following table.

Table 43 Aggregate – Flow Collectors

Measure	Description
Flow Collector	The ID of each Flow Collector on the network.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Flow Collectors report include:

- Link
- Exporter
- Exporter Interface
- Traffic Group
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- Destination AS
- Community
- Ingress PE
- Egress PE
- Flows
- IPv4 Flows
- VPN Flows
- History

Aggregate – Flows

This report provides details for the all IPv4 and VPN flows on the network. The default fields for the Flows report are shown in the following table.

Table 44 Aggregate – Flows

Measure	Description
Flow Source	Source router ID of an identified pair.
Flow Destination	Destination router ID of an identified pair.
Exporter	Name or IP address of peer from which flow information was received.
Traffic Group	User-defined group name. See Creating Groups Using the Menu on page 104 for more information.
CoS Group	User-defined group name for the Class of Service.

Table 44 Aggregate – Flows (cont'd)

Egress PE	Router from which flow exits the current AS.
VRF Label	Label assigned to VRF.
5 Minute Average Current Time	Average amount of traffic during the most recent 5 minutes of time.

Drill-down options for the Flows report include:

- Link
- Flow Collector

Right-click options for the Flows report include the drill-down options and the following:

- Link
- Flow Collector
- Show flow-records
- Show prefixes
- Show paths

Aggregate – CoS Groups Definition

This report lists the currently defined CoS groups. See the “Administration” chapter in the *HP Route Analytics Management System Administrator Guide* for information on creating CoS definitions.

Table 45 Aggregate - CoS Groups Definition**Table 46**

Measure	Description
Name	CoS group name.
EXP	EXP value or values of the CoS group. This column is available only if you have a valid MPLS VPN license.
DSCP or TOS	DSCP or TOS value for the CoS group. This is based on the mode used for CoS definitions.

IPv4 Traffic Reports

IPv4 is the dominant network layer protocol on the Internet. It is a best effort protocol in that it does not guarantee delivery, does not make any guarantees on the correctness of the data, and it can result in duplicated packets and/or packets out-of-order.

IPv4 Traffic reports include data from all Flow Collectors specific to IPv4 traffic. The IPv4 Traffic reports always shows a view that is as complete as possible. By default, these reports cover the most recently recorded five minutes of traffic activity.

IPv4 Traffic – Links

This report shows how much IPv4 traffic each link is carrying, and allows you to color links on the topology map based on traffic volume. The default fields for the Links report are shown in the following table.

Table 47 IPv4 Traffic – Links

Measure	Description
Source	Source router ID of an identified pair.
Destination	Destination router ID of an identified pair.
Capacity	User-defined capacity level.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the IPv4 Links report include:

- Link
- Source AS
- Exporter
- Destination AS
- Exporter Interface
- Community
- Flow Collector
- IPv4 Flows

- Egress Router
- Neighbor AS
- Transit AS
- Traffic Group
- CoS Group
- History

IPv4 Traffic – CoS

This report lists the total amount of IPv4 traffic seen with each CoS group.

Table 48 IPv4 Traffic - CoS

Measure	Description
CoS Group	User-defined name of Class of Service Group
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the CoS report include the following:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Egress Router
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- Ingress PE
- Egress PE
- Flows
- IPv4 Flows
- VPN Flows
- Link
- Traffic Group
- Customer
- History

IPv4 Traffic - CoS Links

This report shows how much IPv4 traffic each CoS link is carrying.

Table 49 IPv4 Traffic - CoS Links

Measure	Description
CoS Group	User-defined name of Class of Service Group
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the CoS Links report include the following:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Egress Router
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- Ingress PE
- Egress PE
- Flows
- IPv4 Flows
- VPN Flows
- Link
- Traffic Group
- Customer
- History

IPv4 Traffic – Exporters

This report lists each router used for obtaining traffic data. The default fields for the Exporters report are shown in the following table.

Table 50 IPv4 Traffic – Exporters

Measure	Description
Exporter	Name or IP address of Flow Collector peer that is exporting Net Flow data.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Exporters report include:

:

- Link
- Flow Collector
- Traffic Group
- Egress Router
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- IPv4 Flows
- Exporter Interface
- History

IPv4 Traffic – Interfaces

This report lists each interface used for obtaining traffic data. The default fields for the Interfaces report are shown in the following table.

Table 51 IPv4 Traffic – Interfaces

Measure	Description
Exporter: Interface Index	Identifies a network interface on the exporting router by its SNMP interface index.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Interfaces report include:

- Link
- Flow Collector
- Traffic Group
- Egress Router
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- IPv4 Flows
- History

IPv4 Traffic – Traffic Groups

This report shows the details of each user-defined traffic group. The default fields for the Traffic Groups report are shown in the following table.

Table 52 IPv4 Traffic – Traffic Groups

Measure	Description
Traffic Group	User-defined group name. See Creating Groups on the Topology Map on page 98 for more information.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Traffic Groups report include:

- Exporter
- Exporter Interface
- Flow Collector
- Transit AS
- Source AS
- Destination AS
- Community
- IPv4 Flows
- Link
- Neighbor AS
- Exit Router - Next Hop

IPv4 Traffic – Top Sources

This report shows the top 100 source addresses per Flow Collector generating the most traffic. Advanced filtering is enabled. The default fields for the Top Sources report are shown in the following table.

Table 53 IPv4 Traffic – Top Sources

Measure	Description
Prefix	Top 100 source IP addresses with the highest amount of traffic.
Average Traffic (bps)	Average amount of traffic for each IP address.

There is no drill-down option for this report. Graphing capabilities are provided.

Right-click options for the Top Sources report include:

- Show flow-records
- Show flow record browser

IPv4 Traffic – Top Destinations

This report shows the top 100 destination address prefixes that receive the most traffic. Advanced filtering is enabled. The default fields for the Top Destinations report are shown in the following table.

Table 54 IPv4 Traffic – Top Destinations

Measure	Description
Prefix	Top 100 destination IP addresses with the highest amount of traffic.
Average Traffic (bps)	Average amount of traffic for each IP address.

There is no drill-down option for this report. Graphing capabilities are provided.

Right-click options for the Top Destinations report include:

- Show flow-records
- Show flow record browser

IPv4 Traffic – Protocols

This report shows the Flow Collector traffic breakdown by IP protocol. The default fields for the Protocols report are shown in the following table.

Table 55 IPv4 Traffic – Protocols

Measure	Description
Protocols	All IP protocols. UDP and TCP protocols include the source and destination ports.
Average Traffic (bps)	Average amount of traffic for each protocol.

There is no drill-down option for this report. Graphing capabilities are provided.

Right-click options for the Protocols report include:

- Show flow-records
- Show flow record browser

IPv4 Traffic – Flows

This report shows the details of each traffic flow. The default fields for the Flows report are shown in the following table.

Table 56 IPv4 Traffic – Flows

Measure	Description
Flow Source	Within a flow, the prefix of the starting point.
Flow Destination	Within a flow, the prefix of the ending point.
Exporter	Name or IP address of peer from which flow information was received.

Table 56 IPv4 Traffic – Flows (cont'd)

Traffic Group	User-defined group name. See Creating Groups on the Topology Map on page 98 for more information.
CoS Group	User-defined group name.
5 Minute Avg Current Time	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Flows report include:

- Link
- Flow Collector
- Egress Router
- Neighbor AS
- Transit AS
- Source AS
- Destination AS

Right-click options for the Flows report include the drill-down options and the following:

- Show flow-records
- Show prefixes
- Show paths

IPv4 Traffic – Traffic Groups Definition

This report allows you to see the current definition of each traffic group. The default fields for the Traffic Groups Definition report are shown in the following table.

Table 57 IPv4 Traffic – Traffic Groups Definition

Measure	Description
Priority	User-defined order of groups.
Name	User-defined group name. See Creating Groups on the Topology Map on page 98 for more information.
Source Prefixes	Source address of an identified pair.
Destination Prefixes	Destination address of an identified pair.
Source and/or Destination Ports	UDP and TCP protocols include the source and destination ports.
Protocols	All IP protocols.
CoS Groups	User-defined identification assigned to a Class of Service group.

There is no drill-down option for this report.

BGP Traffic Reports

The Border Gateway Protocol (BGP) maintains a table of IP networks or prefixes that designate network reachability among ASs. An AS is a collection of IP networks and routers frequently under the control of one company that presents a common routing policy to the Internet. BGP makes routing decisions based on path, network policies, and rulesets. BGP traffic is a subset of IPv4 traffic.

BGP Traffic reports include data from all Flow Collectors specific to BGP traffic. You cannot dynamically change the set of Flow Collectors. The BGP Traffic reports always shows a view that is as complete as possible. By default, these reports cover the most recently recorded five minutes of traffic activity.

BGP Traffic – Egress Router

This report shows the amount of traffic exiting the customer network through a given router at a single point in time. Traffic exiting at this router may go to many different BGP next hops. A next hop address usually corresponds to a peering link. The default fields for the Egress Router report are shown in the following table.

Table 58 BGP Traffic – Egress Router

Measure	Description
Egress Router	Name or IP address of the exit router used to reach a peer. This information is obtained from the Router Name repository prioritized by router names, DNS names, IP address, and system IDs.
Next Hop	IP address of next hop.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Egress Router report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- IPv4 Flows
- Traffic Group
- History

BGP Traffic – Neighbor AS

This report shows how much traffic a neighbor AS is receiving. This information can help ensure a peering relationship is meeting expected levels. The default fields for the Neighbor AS report are shown in the following table.

Table 59 BGP Traffic – Neighbor AS

Measure	Description
Neighbor AS	Name or AS number of directly connected AS to which traffic is being sent.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Neighbor AS report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Neighbor AS
- Transit AS
- Source AS
- Destination AS
- Community
- IPv4 Flows
- Traffic Group
- History

BGP Traffic – Transit AS

This report lists each transit AS used in delivering data and how much data each transit was transmitting. The default fields for the Transit AS report are shown in the following table.

Table 60 BGP Traffic – Transit AS

Measure	Description
Transit AS	Name or AS number of each transit AS used in delivering data to a destination.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Transit AS report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Neighbor AS
- Destination AS
- Egress Router
- Community
- IPv4 Flows
- Traffic Group
- History
- Source AS

BGP Traffic – Source AS

This report shows how much traffic is being received from each source AS. The default fields for the Source AS report are shown in the following table:

Table 61 BGP Traffic – Source AS

Measure	Description
Source AS	Name or AS number of the source AS.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Source AS report include:

- Link
- Exporter
- Exporter Interface
- Traffic Group
- Egress Router
- Neighbor AS
- Transit AS
- Destination AS
- Community
- IPv4 Flows
- History

BGP Traffic – Destination AS

This report shows how much traffic each destination AS is receiving. The default fields for the Destination AS report are shown in the following table.

Table 62 BGP Traffic – Destination AS

Measure	Description
Destination AS	Name or AS number of the final AS.
5 Minute Avg Current Time	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Destination AS report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Neighbor AS
- Transit AS
- Egress Router
- Community
- IPv4 Flows
- Traffic Group
- History
- Source AS

BGP Traffic – Community

This report shows how much traffic each community receives in bits per second (bps) by the first and second 2 octets (groupings of 8 bits). The default fields for the Community report are shown in the following table.

Table 63 BGP Traffic – Community

Measure	Description
First 2 Octets	The first two AS numbers for the given community.
Second 2 Octets	The second two AS numbers for the given community.
5 Minute Avg Current Time	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Community report include:

- Link
- Exporter
- Transit AS
- Source AS

- Exporter Interface
- Destination AS
- Traffic Group
- IPv4 Flows
- Neighbor AS

VPN Traffic Reports

A virtual private network (VPN) is a communications network tunnelled through another network and dedicated for a specific network. VPNs can be used to separate the traffic of different user communities over an underlying network with strong security features.

All VPN Traffic reports include data from all Flow Collectors specific to VPN traffic. The VPN Traffic reports always shows a view that is as complete as possible. By default, these reports cover the most recently recorded five minutes of traffic activity.

VPN Traffic – Links

This report shows how much VPN traffic each link is carrying, and allows you to color links on the topology map based on traffic volume. The default fields for the Links report are shown in the following table.

Table 64 VPN Traffic – Links

Measure	Description
Source	Source router ID of an identified pair.
Destination	Destination router ID of an identified pair.
Capacity	User-defined capacity level.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Links report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Customer
- Ingress PE
- Egress PE
- VPN Flows
- CoS Group
- History

VPN Traffic – Class of Service (CoS)

This report displays the total amount of VPN traffic seen with each CoS. The fields for the CoS report are shown in the following table.

Table 65 VPN Traffic – Class of Service (CoS)

Measure	Description
CoS Group	User-defined name of Class of Service groups.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the CoS report include:

- Exporter
- Exporter Interface
- Flow Collector
- Ingress PE
- Egress PE
- VPN Flows
- Link
- Customer
- History

VPN Traffic – Class of Service (CoS) Links

This report displays the total amount of VPN traffic per link at each class of service. The default fields for the CoS Links report are shown in the following table.

Table 66 VPN Traffic – Class of Service (CoS) Links

Measure	Description
Source	Displays the source address for the link.
Destination	Displays the destination address for the link.
Capacity	Displays the capacity value for the link.
CoS Group	User-defined name of Class of Service groups.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the CoS Links report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Ingress PE
- VPN Flows
- Egress PE
- Customer
- History

VPN Traffic – CoS Customers

This report displays the total amount of traffic per customer for each class of service. The default fields for the CoS Customers report are shown in the following table.

Table 67 VPN Traffic – CoS Customers

Measure	Description
Customer	User-defined customer ID. See Creating Customer and RT Associations on page 332 for more information.
CoS Group	User-defined Class of Service for a group.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the CoS Customers report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Ingress PE
- Egress PE
- VPN Flows
- History

VPN Traffic – Customers

This report displays traffic for each VPN customer and allows you to view the customer on the topology map. The default fields for the Customers report are shown in the following table.

Table 68 VPN Traffic – Customers

Measure	Description
Customer	User-defined customer ID. See Creating Customer and RT Associations on page 332 for more information.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Customers report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- Ingress PE
- Egress PE
- VPN Flows
- CoS Group
- History

The right-click option for the Customers report is the feature Show Map. The Show Map highlights the portion of the topology map that is utilized for a particular VPN by fading all the other nodes and links. The highlighted links can then be viewed in any of the color modes available for the full map. To return the topology map to its original setting, go to the Traffic Reports window and select **Restore Map** button.

VPN Traffic – Ingress PE

The Ingress PE report shows how much VPN traffic each link is carrying, and allows you to color links on the topology map based on traffic volume. The default fields for the Ingress PE report are shown in the following table.

Table 69 VPN Traffic – Ingress PE

Measure	Description
Ingress PE	Displays each Ingress PE router found on the network.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Ingress PE report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- CoS Group
- Customer
- Egress PE
- VPN Flows
- History

VPN Traffic – Exporters

This report lists each router used for obtaining traffic data. The default fields for the Exporters report are shown in the following table.

Table 70 VPN Traffic – Exporters

Measure	Description
Exporter	Name or IP address of peer from which flow information was received.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Exporters report include:

- Link
- Flow Collector
- CoS Group
- Customer
- Ingress PE
- Egress PE
- VPN Flows
- Exporter Interface
- History

VPN Traffic – Interfaces

Each row in this report represents a router interface where VPN traffic was seen and exported over the network. The default fields for the Interfaces report are shown in the following table.

Table 71 VPN Traffic – Interfaces

Measure	Description
Exporter: Interface Index	Identifies a network interface on the exporting router by its SNMP interface index.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Interfaces report include:

- Link
- Flow Collector
- Customer
- Ingress PE
- Egress PE
- VPN Flows
- History

VPN Traffic – Egress PE

This report shows the amount of traffic leaving the PE routers. The default fields for the Egress PE report are shown in the following table.

Table 72 VPN Traffic – Egress PE

Measure	Description
Egress PE	Router from which flow exits the current AS.
5 Minute Avg Selected Interval	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Egress PE report include:

- Link
- Exporter
- Exporter Interface
- Flow Collector
- CoS Group
- Customer
- Ingress PE
- VPN Flows
- History

VPN Traffic – Flows

This report shows the details of each traffic flow. The default fields for the Flows report are shown in the following table.

Table 73 VPN Traffic – Flows

Measure	Description
Flow Source	Source router ID of an identified pair.
Flow Destination	Destination router ID of an identified pair.
CoS Group	User-defined Class of Service group.
Exporter	Address of the exporting router.

Table 73 VPN Traffic – Flows (cont'd)

Egress PE	Router from which flow exits the current AS.
VRF Label	Label assigned to VRF.
5 Min Avg Current Time	Average amount of traffic during the most recent 5 minutes of the selected time.

Drill-down options for the Flows report include:

- Link
- Customer
- Flow Collector
- Ingress PE

Right-click options for the Flows report include the drill-down options and the following:

- Show flow-records
- Show prefixes
- Show paths

10 Path Reports

This chapter describes how to use path reports to analyze network connectivity and optimize routing performance.

Chapter contents:

- [Understanding Path Reports](#) on page 404
- [Accessing the Path Reports Window](#) on page 404
- [Using the Path Reports Window](#) on page 407
- [Viewing Path Analysis Reports](#) on page 408
- [Network Element Analysis](#) on page 418
- [Failure Analysis](#) on page 424

Understanding Path Reports

Network connectivity is the ability of a router to reach all other routers in the network by sending packets of data along paths between source and destination routers. Each path consists of one or more links. Links are associated with a metric value, which is used to calculate the cost of the path.

The Path Reports tool computes and provides a summary of paths between routers in a selected topology, and allows you to break down the summary by area of interest, such as asymmetric links, unused links, and source routers. The reports are organized by analysis type. For example, you can view an analysis of all paths in the selected topology, or you can choose to view only asymmetric paths.



Path Reports are disabled in Monitoring mode.

Accessing the Path Reports Window

You can access path reports from the client application.

To access the Path Reports window, perform the following steps:

- 1 Start the client application and open the desired topology.
- 2 Choose **Reports** → **Path Reports**.

The Select Topologies and Routers for Path Analysis window opens.

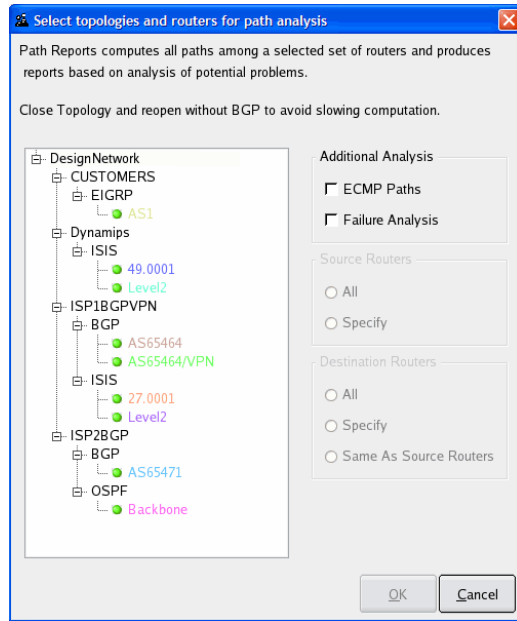


Figure 141 Path Reports - Select Topology

- 3 Choose one or more databases from the list.

You can choose any combination of databases 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.



When you open a topology for path analysis, avoid selecting BGP data when only IGP paths are of interest. Selecting BGP data may significantly increase the amount of time required to generate reports, as compared to non-BGP data. In general, computation of path reports for a 300-node, non-BGP topology can take up to 2 minutes to process, while a 300-node BGP topology can take 30-60 minutes to process.

- 4 If desired, select one or both of the following check boxes:

- **ECMP Paths:** Select this check box to enable the Equal Cost Multi-Path (ECMP) analysis option, which finds and lists multiple paths of the same cost. See [ECMP Paths Analysis](#) on page 414 for more information. If you do not select this check box, a single path is computed for each router pair, rather than multiple paths.
- **Failure Analysis:** Select this check box to cause the links in the selected database to fail, one link at a time. This can help determine which link failures are the most costly. See [Failure Analysis](#) on page 424 for more information.



Enabling failure analysis, increases computation time significantly compared to reports that are generated without failure analysis. For example, when you enable failure analysis for a 300-node, non-BGP topology, you can add up to 8 minutes to the computation time.

- 5 Choose the source routers to include in the path analysis :
 - **All:** Every source router in the selected database are included in the analysis.
 - **Specify:** Choose which routers to include in the path analysis.
When you click **Specify**, the system presents a list of available source routers. You can filter the list of routers by entering a regular expression in the RegEx text box at the top of the window. Select one or more routers from the Available Routers column, then click the arrow to move the specified routers to the Selected Routers column. Click **OK**.
- 6 Select the destination routers to include in the path analysis:
 - **All:** Every destination router in the selected databases will be included in the analysis.
 - **Specify:** Choose the routers to include in the path analysis, as described in Step 5.
 - **Same as Source Routers:** Destination routers included in the analysis will be the same as the source routers you chose in Step 5.
- 7 Select the routed protocols to include in the path analysis:
 - **IP:** Route Resolution for IP Prefixes.
 - **ISO OSI:** Route Resolution for OSI Prefixes.



If OSI ISIS is not detected, the options in Step 7 will not display.

- 8 Click **OK** to begin generating reports.

You can cancel the report generation at any time. Partial results are displayed in the Path Reports window.

Using the Path Reports Window

The Path Reports window displays reports in the following categories:

- [Viewing Path Analysis Reports](#) on page 408
- [Network Element Analysis](#) on page 418
- [Failure Analysis](#) on page 424, included only if you select the **Failure Analysis** check box when opening the report.

The screenshot shows a window titled "orksBGP/BGP" with a subtitle "Analysis of Paths: LabNetworksBGP/BGP". The window contains a table with the following data:

Source Router	Destination Router	Destination Prefix	Paths	Hops	Metric	
10.150.1.2	Core-Router14	10.120.1.14/32		1	14	71
10.150.2.2	Core-Router14	10.120.1.14/32		1	14	71
10.150.3.2	Core-Router14	10.120.1.14/32		1	14	71
10.150.4.2	Core-Router14	10.120.1.14/32		1	14	71
10.150.5.2	Core-Router14	10.120.1.14/32		1	14	71
10.150.6.2	Core-Router14	10.120.1.14/32		1	14	71
10.150.7.2	Core-Router14	10.120.1.14/32		1	14	71
10.150.8.2	Core-Router14	10.120.1.14/32		1	14	71
10.150.9.2	Core-Router14	10.120.1.14/32		1	14	71
10.150.10.2	Core-Router14	10.120.1.14/32		1	14	71
DC-PE2-ROUTER9	Core-Router14	10.120.1.14/32		1	13	70
Core-Router14	DC-PE2-ROUTER9	10.120.1.9/32		1	13	70
10.150.1.2	SF-PE1-ROUTER6	10.120.1.6/32		1	12	61
10.150.1.2	CORE-ROUTER13	10.120.1.13/32		1	12	61
Core-Router14	10.150.1.2	10.150.1.2/32		1	14	61
Core-Router14	10.150.2.2	10.150.2.2/32		1	14	61
Core-Router14	10.150.3.2	10.150.3.2/32		1	14	61
Core-Router14	10.150.4.2	10.150.4.2/32		1	14	61
Core-Router14	10.150.5.2	10.150.5.2/32		1	14	61

Figure 142 Path Reports Window

The following icons appear in the Path Reports window. Not every icon appears in every table.



Color paths — Highlight paths on the routing topology map. Click a particular row in the Path Reports table and the corresponding path(s) between the selected source and destination routers is highlighted on the map, as shown in [Figure 143](#).



Show paths — View a table listing all paths between the selected source and destination router pair. The paths are broken down by hop or link.



Color by ... — Color elements on the routing topology map. For example, click the **Color by ...** icon in the Hot Nodes table to color all hot nodes on the routing topology map. A second Legend panel is displayed on the topology map to describe each colored element. Click the icon again to uncolor the highlighted elements.



Tear off — Opens the table in a new window.



Put back — Puts the table you opened in a new window back into the original window.



Show detailed path statistics — View more details about the paths originating or ending with a selected router. For example, in [Figure 144](#), clicking this icon opens an Analysis of Paths table in the lower half of the Path Reports window. You can also right-click a router in the table and choose **Show Detailed Path Statistics** from the pop-up menu to achieve the same result.

Viewing Path Analysis Reports

This section describes the following path analysis options, which are available from the Path Reports window (see [Accessing the Path Reports Window](#) on page 404):

- [Path Statistics Report](#) on page 409

- [ECMP Paths Analysis](#) on page 414
- [Single \(Non-ECMP\) Path Analysis](#) on page 415
- [Asymmetric Paths Analysis](#) on page 416

Path Statistics Report

The Path Statistics report lists every path between router pairs in the selected database. If you chose specific source and destination routers to analyze, as described in [Accessing the Path Reports Window](#) on page 404, only those routers appear in the Path Statistics table.

The Path Statistics table allows you to identify where connectivity has been lost. For example, if Router A cannot reach Router D, then Path Not Found is listed in the **Paths** column of the table. In addition, the Path Statistics table lists paths from highest metric value to lowest, making the costliest paths immediately evident.

The Path Statistics table includes the following columns:


- **Source Router** — Router where the path originates.
- **Destination Router** — Name of the router where the path ends. Since a router may advertise multiple prefixes, a destination prefix is used as the destination IP address for the path.
- **Destination Prefix** — A prefix unique to each router is used for the destination router. For example, if a node advertises 20 prefixes, the system isolates one prefix that is advertised by no other router, and uses this prefix as the address of the destination router. If multiple unique prefixes are found, the following rules determine the destination:
 - a. Select a unique prefix with lowest metric value.
 - b. If the metrics of all unique prefixes are equal, select the prefix with the longest length.
 - c. If the metrics of all unique prefixes are equal, and all are of the same length, select the prefix with the smallest IP address.

If none of the prefixes advertised by a router is unique, then non-unique prefixes are considered. However, if a destination prefix cannot be determined, then no paths to the destination router are computed. All such routers are included in the Down Nodes report as described in [Down Nodes](#) on page 423.

- **Paths** — Number of paths found between the source router and the destination router. Unless you have chosen to compute ECMP paths, this number is 1.

If a path between the source and destination router cannot be computed, one of the following messages is displayed:

- **Destination Not Reached** — The final hop of the path is not the destination router. This can occur if the destination prefix used to reach the destination router (Router B) is also being advertised by another router (Router C). If the final hop is Router C rather than Router B, the path cannot be computed.
- **Path Not Found** — No path is found between the source and destination router.
- **Loop Detected** — The number of hops between the source and destination router exceeds 30. a loop is detected that prevents the path from being computed properly.
- **Hops** — Number of hops between the source router and destination router. If a range of values is displayed in this column, the range represents the minimum and maximum number of hops for the paths between the source and destination router. For example, if there are 3 paths between Router A and Router B, with a range of 4-9 hops, Path 1 is made up of 4 hops, Path 2 is made up of 5 hops, and Path 3 is made up of 9 hops.
- **Metric** — The metric value of a path is calculated by adding up the link metric values along the path. For example, a path between Router A and Router B consists of two hops. Hop 1 has a link metric value of 10, and Hop 2 has a link metric value of 20. The total metric value of the path is 30. If a range of metrics is displayed in the column, the range represents the minimum and maximum metric for paths found between the source and destination routers.

To drill down further and view path details for a specific row in the table, highlight the row, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Paths menu item. The List of Paths table appears in the lower half of the Path Reports window.

Each path between the highlighted source and destination routers is listed in a separate row, broken down by link (Hop 1, Hop 2 ...). For example, if four paths are found between Router A and Router B, each of the four paths and the associated hops are listed along with the following information:

- **Path** — Path(s) corresponding to the row you selected in the upper half of the window. If more than one path is found between the source and destination router, the paths are labeled Path 1, Path 2 ... and so on. A collapsible list of the hops for each path appears in this column as well.
- **Source Router** — Router where the link originates.
- **Destination Router** — Router where the link ends.
- **Metric** — Metric value for the link.
- **Protocol** — Routing protocol associated with the link.

To view path information on the routing topology map, click the corresponding row in the table. The path, link, or node is highlighted on the routing topology map as shown in [Figure 143](#).

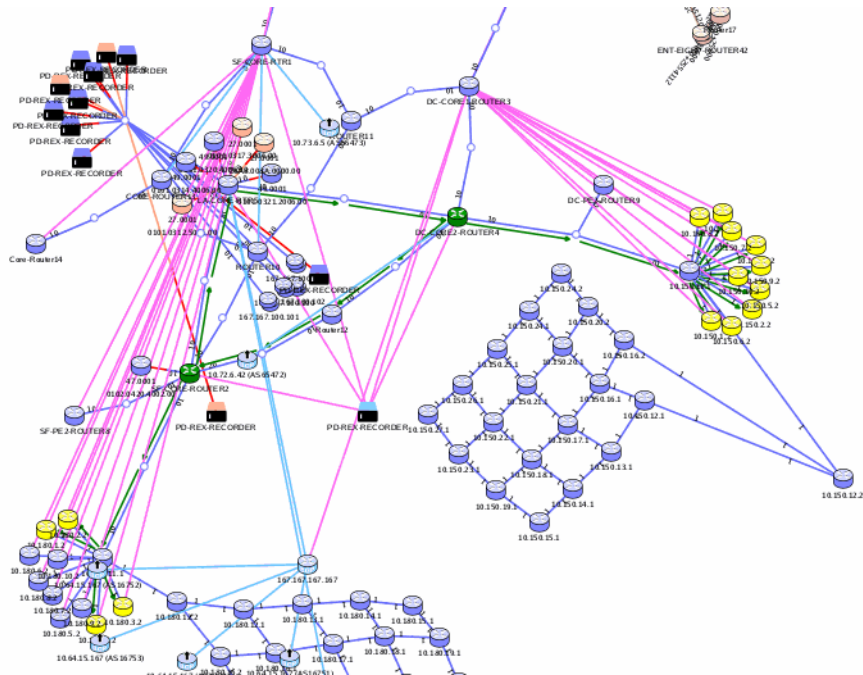



Figure 143 Path Highlighted on the Routing Topology Map

Path Statistics by Source

To view the number of paths reachable by each source router, click **By Source** in the left pane to organize data accordingly. The following information is displayed in the table:

- **Source Router** — Router where a path originates.
- **Reachable Destinations** — Number of routers that the source router can reach.
- **Paths** — Range of paths to all reachable destinations. For example, 1-5.
- **Hops** — Number of hops along the path between the selected node and a corresponding destination router. If a range of numbers is displayed, this column reflects the minimum and maximum number of hops for the set of paths originating with the source router.
- **Metric** — The metric value for the path(s) originating with the selected node. If a range of values is displayed, this column reflects the minimum and maximum metric value for the set of paths originating with the source router.

To drill down further and view detailed path statistics for a source router in the Paths by Source table, highlight the source router, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Detailed Path Statistics menu item. The Analysis of Paths table appears in the lower half of the Path Reports window as shown in [Figure 144](#).

NetworksBGP/BGP

All Paths by Source: LabNetworksBGP/BGP

Filter by: Any


Show Hide

Source Router	Reachable Destinations	Paths	Hops	Metric
167.167.167.167	None	NA	NA	NA
10.150.1.2	29	1	3 - 14	2 - 71
10.150.2.2	29	1	3 - 14	2 - 71
10.150.3.2	29	1	3 - 14	2 - 71
10.150.4.2	29	1	3 - 14	2 - 71
10.150.5.2	29	1	3 - 14	2 - 71
10.150.6.2	29	1	3 - 14	2 - 71
10.150.7.2	29	1	3 - 14	2 - 71
10.150.8.2	29	1	3 - 14	2 - 71
10.150.9.2	29	1	3 - 14	2 - 71
10.150.10.2	29	1	3 - 14	2 - 71
10.180.1.2	29	1	3 - 12	2 - 61
10.180.2.2	29	1	3 - 12	2 - 61
10.180.3.2	29	1	3 - 12	2 - 61
10.180.4.2	29	1	3 - 12	2 - 61
10.180.5.2	29	1	3 - 12	2 - 61
10.180.6.2	29	1	3 - 12	2 - 61
10.180.7.2	29	1	3 - 12	2 - 61
10.180.8.2	29	1	3 - 12	2 - 61

21 PST

X Close

Figure 144 All Paths by Source with Analysis of Paths Table


To view details for each of the paths listed in the Analysis of Paths table, click the **Show Paths** icon  as described in [Path Statistics Report](#) on page 410.


Path Statistics by Destination

To view the number of paths reachable by each destination router, click **By Destination** in the left pane to organize data accordingly. The following information is displayed in the table:

- **Destination Router** — Node where a path ends.
- **Reachable by** — Number of routers that can reach the specified destination router.
- **Paths** — Range of paths whose destination is the specified node.
- **Hops** — Number of hops along the path between the selected node and a corresponding source router. If a range of numbers is displayed, this column reflects the minimum and maximum number of hops for the set of paths ending with the source router.

- **Metric** — The metric value for the path(s) ending with the selected node. If a range of values is displayed, this column reflects the minimum and maximum metric value for the set of paths ending with the source router.

To drill down further and view detailed path statistics for a destination router in the Paths by Destination table, highlight the destination router, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Detailed Path Statistics menu item. The Analysis of Paths table appears in the lower half of the Path Reports window as shown in [Figure 144](#).


To view details for each of the paths listed in the Analysis of Paths table, click the **Show Paths** icon  as described in [Path Statistics Report](#) on [page 410](#).

ECMP Paths Analysis

The Analysis of ECMP Paths table lists the paths between source and destination router pairs that are of equal cost. This information helps identify the amount of redundancy in the network and allows you to make adjustments accordingly. For example, if there are two equal-cost paths between Router A and Router B, you might determine that two paths do not provide enough redundancy. As a result, you might increase the number of equal-cost paths between Router A and Router B. The opposite is also true: if you do not want equal-cost paths in your network, you can use the Analysis of ECMP Paths table to find and eliminate such paths.

- **Source Router** — Router where the path originates.
- **Destination Router** — Name or ID of the router where the path ends. Since a router may advertise multiple prefixes, a destination prefix is used as the destination IP address for the path.
- **Destination Prefix** — A prefix unique to each router is used as the destination for the destination router. For more information about destination prefixes, see [Path Statistics Report](#) on [page 409](#).
- **Paths** — Number of equal-cost paths between the source and destination routers.
- **Hops** — Number of hops making up each equal-cost path. If a range of values is displayed, this column reflects the minimum and maximum number of hops for the set of paths.
- **Metric** — Total metric value of the path.

To view the Analysis of ECMP Paths table by source or destination router, click **By Source** or **By Destination** in the left pane to organize data accordingly, then see [Path Statistics by Source](#) on page 412 and [Path Statistics by Destination](#) on page 413 for more information.

To drill down further and view path details for a specific row in the By Source or By Destination table, highlight the row, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Detailed Path Statistics menu item. The Analysis of ECMP Paths table appears in the lower half of the Path Reports window.


Single (Non-ECMP) Path Analysis

The Analysis of Single Paths table lists paths between source and destination router pairs for which there is not another path of equal cost. This table can help identify a lack of redundancy between vital routers. The Analysis of Single Paths table is displayed only when the **ECMP Paths** check box is selected on the Select Topologies dialog box, as described in [Accessing the Path Reports Window](#) on page 404.

The Analysis of Single Paths table has the following columns:

- **Source Router** — Router where the path originates.
- **Destination Router** — Name or ID of the router where the path ends. Since a router may advertise multiple prefixes, a destination prefix is used as the destination IP address for the path.
- **Destination Prefix** — A prefix unique to each router is used as the destination for the destination router. For more information about destination prefixes, see [Path Statistics Report](#) on page 409.
- **Paths** — Number of paths between the source and destination routers whose cost is not equal to any other path between the source and destination router.
- **Hops** — Number of hops making up each path.
- **Metric** — Total metric value of the path.

To view the Analysis of Single Paths table by source or destination router, click **By Source** or **By Destination** in the left pane to organize data accordingly, then see [Path Statistics by Source](#) on page 412 and [Path Statistics by Destination](#) on page 413 for more information.

To drill down further and view path details for a specific row in the By Source or By Destination table, highlight the row, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Detailed Path Statistics menu item. The Analysis of Single Paths table appears in the lower half of the Path Reports window.

Asymmetric Paths Analysis

An asymmetric path can exist when the “forward” cost of a path between two routers differs from the “reverse” cost of a path between the same two routers. In other words, if the cost of a path from Router A to Router B is 20, and the cost of a path from Router B to Router A is 40, the paths are asymmetric. In addition, a path may be asymmetric if the number of forward hops differs from the number of reverse hops; if the forward and reverse hops themselves differ; or if the number of forward paths differs from the number of reverse paths. Identifying asymmetric paths can help isolate network misconfigurations.

The Analysis of Asymmetric Paths window is shown in [Figure 145](#).

The Analysis of Asymmetric Paths table has the following columns:

- **Source Router** — Node where the path originates.
- **Destination Router** — Node where the path ends.
- **Forward Paths** — Number of paths from the source router to the destination router.
- **Reverse Paths** — Number of paths from the destination router to the source router.
- **Forward Hops** — Number of hops taken along the path from the source router to the destination router.
- **Reverse Hops** — Number of hops taken along the path from the destination router back to the source router.
- **Forward Metric** — Metric value, or cost, of the path from the source router to the destination router.
- **Reverse Metric** — Metric value, or cost, of the path from the destination router back to the source router.

- Metric Difference** — Difference between the metric values of the forward path and the reverse path between the source and destination routers. For EIGRP protocol routers, this value represents the difference in bandwidth plus the difference in delay.

Asymmetric path reports do not include ECMP paths. For more information about ECMP paths, see [ECMP Paths Analysis](#) on page 414.

The screenshot shows a window titled 'Analysis of Asymmetric Paths: LabNetworksBGP/BGP'. The window contains a table with the following columns: Source Router, Destination Router, Forward Paths, Reverse Paths, Forward Hops, Reverse Hops, Hop Difference, Forward Metric, Reverse Metric, and Metric Difference. The table lists 20 rows of data, each representing a path between two routers. The 'Hop Difference' column shows values ranging from 0 to 11, and the 'Metric Difference' column shows values ranging from 10 to 50. The window also includes a 'Filter by: Any' dropdown and 'Show Hide' buttons.

Source Router	Destination Router	Forward Paths	Reverse Paths	Forward Hops	Reverse Hops	Hop Difference	Forward Metric	Reverse Metric	Metric Difference
10.150.1.2	ROUTER10	1	1	10	10	0	51	41	10
10.150.1.2	SF-PE1-ROUTER	1	1	12	12	0	61	51	10
10.150.1.2	SF-CORE-ROUTE	1	1	8	8	0	41	31	10
10.150.1.2	DC-CORE1-ROUT	1	1	6	6	0	31	21	10
10.150.1.2	DC-PE1-ROUTER	1	1	8	8	0	41	31	10
10.150.1.2	SF-PE2-ROUTER	1	1	10	10	0	51	41	10
10.150.1.2	DC-PE2-ROUTER	1	1	4	4	0	21	11	10
10.150.1.2	CORE-ROUTER1	1	1	12	12	0	61	51	10
10.150.1.2	Core-Router14	1	1	14	14	0	71	61	10
ROUTER10	DC-CORE2-ROUT	1	1	7	7	0	30	40	10
SF-PE1-ROUTER	DC-CORE2-ROUT	1	1	9	9	0	40	50	10
SF-CORE-ROUTE	DC-CORE2-ROUT	1	1	5	5	0	20	30	10
DC-CORE1-ROUT	DC-CORE2-ROUT	1	1	3	3	0	10	20	10
DC-CORE2-ROUT	DC-PE1-ROUTER	1	1	5	5	0	30	20	10
DC-CORE2-ROUT	SF-PE2-ROUTER	1	1	7	7	0	40	30	10
DC-CORE2-ROUT	DC-PE2-ROUTER	1	1	3	3	0	20	10	10
DC-CORE2-ROUT	CORE-ROUTER1	1	1	9	9	0	50	40	10
DC-CORE2-ROUT	Core-Router14	1	1	11	11	0	60	50	10

Figure 145 Analysis of Asymmetric Paths Table

Asymmetric Paths by Path


The Analysis of Asymmetric Paths: By Paths table lists paths that are asymmetric due to a mismatch in forward and reverse hops. Click **By Path** in the left pane to organize data accordingly.


Asymmetric Paths by Metric

The Analysis of Asymmetric Paths: By Metric table lists paths that are asymmetric due to a mismatch in forward and reverse metrics. Click **By Metric** in the left pane to organize data accordingly.

Asymmetric Paths by Source


To view the Analysis of Asymmetric Paths table by source router, click **By Source** in the left pane to organize data accordingly. See [Path Statistics by Source](#) on page 412 for a description of this table.


To drill down further and view detailed path statistics for a router in the Asymmetric Paths by Source table, highlight the router, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Detailed Path Statistics menu item. The Analysis of Asymmetric Paths table appears in the lower half of the Path Reports window.

To view details for each of the paths listed in the Analysis of Asymmetric Paths table, click the **Show Paths** icon  as described in [Path Statistics Report](#) on page 410.

Asymmetric Paths by Destination

To view the Analysis of Asymmetric Paths table by destination router, click **By Destination** in the left pane to organize data accordingly. See [Path Statistics by Destination](#) on page 413 for a description of this table.

To drill down further and view detailed path statistics for a router in the Asymmetric Paths by Destination table, highlight the router, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Detailed Path Statistics menu item. The Analysis of Asymmetric Paths table appears in the lower half of the Path Reports window.

To view details for each of the paths listed in the Analysis of Asymmetric Paths table, click the **Show Paths** icon  as described in [Path Statistics Report](#) on page 410.

Network Element Analysis

Determining which network elements play too large a part in network routing and which are playing no part at all is required for network performance optimization. Hotspots are routers or links that are used more frequently than

other elements in the network. For example, if Router A is used in 20 paths, all 20 of those paths will be affected should the router fail. Conversely, coldspots are network elements that are under-utilized. If Router B is not used in any paths, you can optimize performance by making better use of Router B, and relieving Router A of some of the load.

This section describes the following network element analysis options, which are available from the Path Reports window (see [Accessing the Path Reports Window](#) on page 404):

- [Router Hot Spots](#) on page 419
- [Link Hot Spots](#) on page 420
- [Unused Links](#) on page 421
- [Down Nodes](#) on page 423
- [Down Links](#) on page 423
- [Asymmetric Link Metrics](#) on page 424

Router Hot Spots

This table is sorted by the routers that are used most frequently in paths on the network.

The Router Hot Spots window is displayed in [Figure 146](#).

The Hot Nodes table has the following columns:

- **Node** — Name or ID of the “hot” router.
- **Paths** — Number of source and destination router pairs that include the “hot” router.


Hot Nodes: LabNetworksBGP/BGP


Filter by: Any

Node	Paths
DC-CORE2-ROUTER4	504
SF-CORE-ROUTER2	502
ROUTER10	227
DC-CORE1-ROUTER3	226
LA-CORE-RTR5	174
CORE-ROUTER13	158
SF-CORE-RTR1	89
10.180.2.2	60
SF-PE2-ROUTER8	60
10.150.1.2	60
10.180.1.2	60
10.150.10.2	60
10.150.9.2	60
10.150.8.2	60
Core-Router14	60
10.150.7.2	60
10.150.3.2	60
10.150.2.2	60
10.150.6.2	60

Close

Figure 146 Router Hot Spots Table

To drill down further and view detailed path statistics for a router in the Hot Nodes table, highlight the router, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the **Show Detailed Path Statistics** menu item. The Analysis of Paths table appears in the lower half of the window.

To view details for each of the paths listed in the Analysis of Paths table, click the **Show Paths** icon  as described in [Path Statistics Report](#) on page 410.

Link Hot Spots

Similar to the Router Hot Spots table, the Link Hot Spots table is sorted by the links that are most frequently used in paths. The more frequently a link is used in a path, the more paths will be affected if that link fails.

The Hot Links window is displayed in [Figure 147](#).

The Hot Links table has the following columns:

- **Link** — The address of the “hot” link.
- **Paths** — The number of source and destination router pairs that use the “hot” link in their paths.

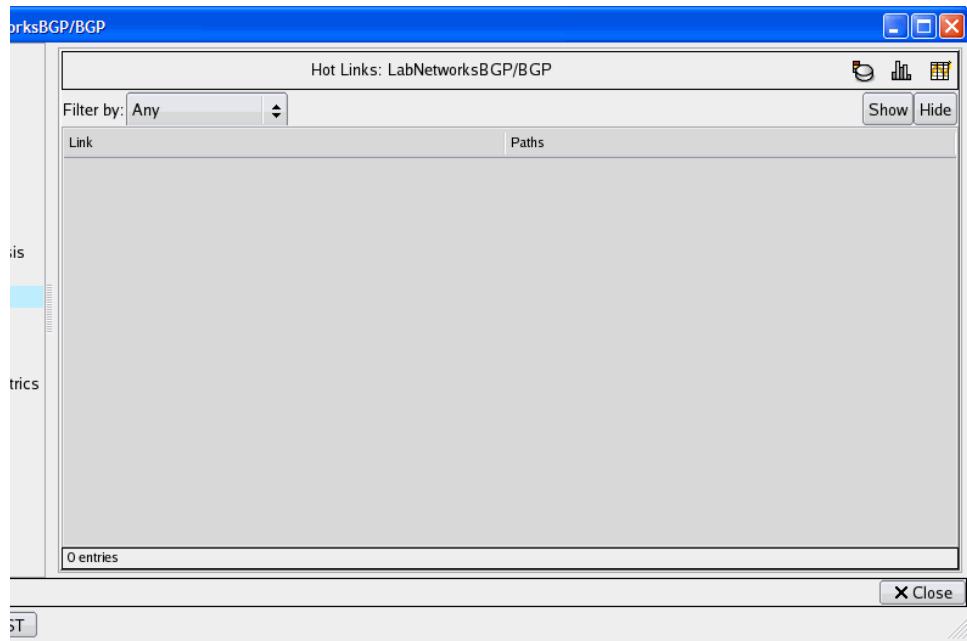




Figure 147 Link Hot Spots Table

To drill down further and view detailed path statistics for a link in the Hot Links table, highlight the link, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Detailed Path Statistics pop-up menu item. The Analysis of Paths table appears in the lower half of the window.

To view details for each of the paths listed in the Analysis of Paths table, click the **Show Paths** icon  as described in [Path Statistics Report](#) on page 410.

Unused Links

This table lists all links in the network that are not being used in any paths. The Unused Links table has the following columns:

- **Link** — The unused link.
- **Source Interface** — The interface where the link originates.
- **Destination Interface** — The interface where the link ends.
- **Metric** — Metric value of the unused link.
- **State** — Indicates whether the link is up or down.
- **Area** — Location of the link.

Down Nodes

This table lists routers that are currently down, have failed, or do not have a destination prefix.

The Down Nodes table has the following columns:

- **Router** — The node that has gone down.
- **IP Address** — Address of the node that has gone down.
- **Type** — Indicates the type of router (for example, internal, area border router, AS external).
- **Protocol** — Indicates the protocol of the router.
- **State** — Indicates whether the node is down or does not have a destination prefix.
- **Area** — Location of down node.

Down Links

This table lists links that are currently down, or have failed.

The Down Links table has the following columns:

- **Link** — The down link.
- **Source Interface** — The interface where the down link originates.
- **Destination Interface** — The interface where the down link ends.
- **Metric** — Total metric value of the down link.
- **State** — Indicates that the link is down.
- **Area** — Location of down link.

Asymmetric Link Metrics

This table lists links whose forward and reverse metrics are different. The Asymmetric Link Metrics table is similar to the Asymmetric Paths table, described on [page 416](#).

The Asymmetric Links table has the following columns:

- **Link** — The address of the asymmetric link.
- **Source Interface** — The interface where the link originates.
- **Destination Interface** — The interface where the link ends.
- **Forward Metric** — The value of the metric from the source interface to the destination interface.
- **Reverse Metric** — The value of the metric from the destination interface to the source interface.
- **Metric Difference** — The difference between the forward and reverse metrics.
- **Area** — Location of the link.

Failure Analysis

When you select the **Failure Analysis** check box on the Select Topology dialog box, as described in [Accessing the Path Reports Window](#) on page 404, each link is systematically failed along every path in the selected database. The results of the simulated link failure appear in the Failure Analysis tables, which you can use to isolate the links that would be most damaging in the event of a failure.

This section describes the following failure analysis options, which are available from the Path Reports window (see [Accessing the Path Reports Window](#) on page 404):


- [Path Failure Analysis](#) on page 425
- [Link Failure Analysis](#) on page 426
- [Failure-induced ECMP Analysis](#) on page 427

Path Failure Analysis

This table lists each path that failed as part of the failure analysis.

The Path Failure Analysis table has the following columns:


- **Source Router** — Node where the path originates.
- **Destination Router** — Name or ID of the node where the path ends. Since a router may advertise multiple prefixes, a destination prefix is used as the destination IP address for the path.
- **Destination Prefix** — A prefix unique to each router is used as the destination for the destination router. For more information about destination prefixes, see [Path Statistics Report](#) on page 409.
- **Original Paths** — Number of paths discovered between the source and destination router before failure analysis.
- **Original Hops** — Range of hops discovered between the source and destination router before failure analysis.
- **Original Metric** — Metric of the path between the source and destination routers before failure analysis.
- **Worst Link Failure**— Address of the link whose failure caused path cost to increase most of all failed links.
- **Worst Metric Change**— The difference between the original metric of the path and largest metric in the List of Paths table resulting from the link failure.

To drill down further and view the effect of the link failure for a specific path in the table, highlight the row corresponding to the path, then click the **Show Effect of Link Failures** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Effect of Link Failures pop-up menu item. The Link Failure Analysis for Path table appears in the lower half of the Path Reports window. You may need to scroll down.

The Link Failure Analysis for Path table has the following columns:

- **Link** — This column lists all links whose failure had an effect on the path (for example, caused a change in the number of hops or in the metric value).
- **New Paths** — Number of paths after the link failure. Compare this value to **Original Paths** in the Path Failure Analysis table.

- **New Hops** — Range of hops after the link failure. Compare this value to **Original Hops** in the Path Failure Analysis table.
- **New Metric** — Metric value after the link failure. Compare this value to **Original Metric** in the Path Failure Analysis table.
- **Damage Metric** — The difference between the original metric of the path and the largest metric resulting from link failure.


Additionally, you can show path details for each row in the Link Failure Analysis table by clicking the **Show Paths** icon . The first entry in the List of Paths table reflects the original path, and the second entry reflects the state of the path after the link failure.


Link Failure Analysis

This table lists each failed link and the number of paths that were damaged as a result of the failure of that link. “Damaged” means the path metric, or cost, increased after the link failed.

The Link Failure Analysis table has the following columns:

- **Link** — Address of the failed link.
- **Damaged Paths** — Number of paths whose cost increased after the link failed.


To drill down further and view detailed path statistics for a link in the Link Failure Analysis table, highlight the link, then click the **Show Paths** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the row and choose the Show Detailed Path Statistics pop-up menu item. The Analysis of Paths table appears in the lower half of the window.

View the effect of the link failure for a specific path in the Analysis of Paths table, highlight the row, then click the **Show Effect of Link Failures** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the path row and choose the Show Effect of Link Failures pop-up menu item. The Link Failure Analysis for Path table appears in the lower half of the Path Reports window. This table is described in [Path Failure Analysis](#) on page 425.

Failure-induced ECMP Analysis

This table lists paths that have become equal-cost as the result of link failure. If equal-cost paths are not desired in the network, use this table to pinpoint the links whose failure would cause equal-cost paths to occur and reconfigure the network accordingly. See [ECMP Paths Analysis](#) on page 414 for more information about equal-cost paths.

The Failure Induced ECMP table contains the same information as that in the Path Statistics table, described on [page 409](#).

To drill down further and view the effect of the link failure for a specific path in the table, highlight the path row, then click the **Show Effect of Link Failures** icon  in the upper right corner of the Path Reports window. Alternatively, right-click the path row and choose the Show Effect of Link Failures pop-up menu item. The Link Failure Analysis for Path table appears in the lower half of the Path Reports window as described in [Path Failure Analysis](#) on page 425.

11 Alerts

This chapter describes how to configure and view alerts.

Chapter contents:

- [Understanding Alerts](#) on page 430
- [Viewing Alert Types](#) on page 431
- [Creating New Alerts](#) on page 434
- [Viewing Alert Status](#) on page 440
- [Creating Dispatch Specifications](#) on page 443
- [Creating Suppression Specifications](#) on page 447

Understanding Alerts

Alerts allow you to monitor network activity and obtain information about potential problems. You can obtain notification of any changes to network elements (such as routes and routers) based on configurable thresholds. Alerts can be sent as SNMP traps to an SNMP-based network management system integrated with other network operations, logged to a syslog file, sent as a simple email notification, or logged to the database for display in the GUI.

You can configure alerts for selected protocols. You can also determine whether the alerts will operate globally or only in selected areas. For example, if you are monitoring a single or multi-area OSPF network, you can configure alerts that apply to the OSPF routing events for all the OSPF areas being monitored or that apply only to the OSPF routing events in selected areas. Alerts are disabled by default.

From the Alerts menu, you can select any of the following items:

- **View Alert Status** – list all alerts generated by the system.
- **Configure Alerts** – set up alerts and view the list of configured alerts.
- **Dispatch Specifications** – the notification method used for informing you about network and traffic status, as specified in [Creating Dispatch Specifications](#) on page 443.
- **Suppression Specifications** – determine the periods when no alerts are generated, and set a rate limit on delivering alerts.

All users can view alerts; however to configure alerts you must have administrator privileges.



The descriptions within this chapter are based on a full product license and a network configuration using all protocols.

Viewing Alert Types



You must have administrator privileges to configure alerts.

Because the privilege level of the GUI in VNC display 1 is operator, and it is not possible to configure alerts using VNC display 1. Use one of the VNC displays 2-10 or an SSH/X Window connection to run the GUI when configuring alerts.

To view alert types, perform the following steps:

- 1 Open the client application and choose **Alerts** → **Configure Alerts** to open the Configure Alerts window.

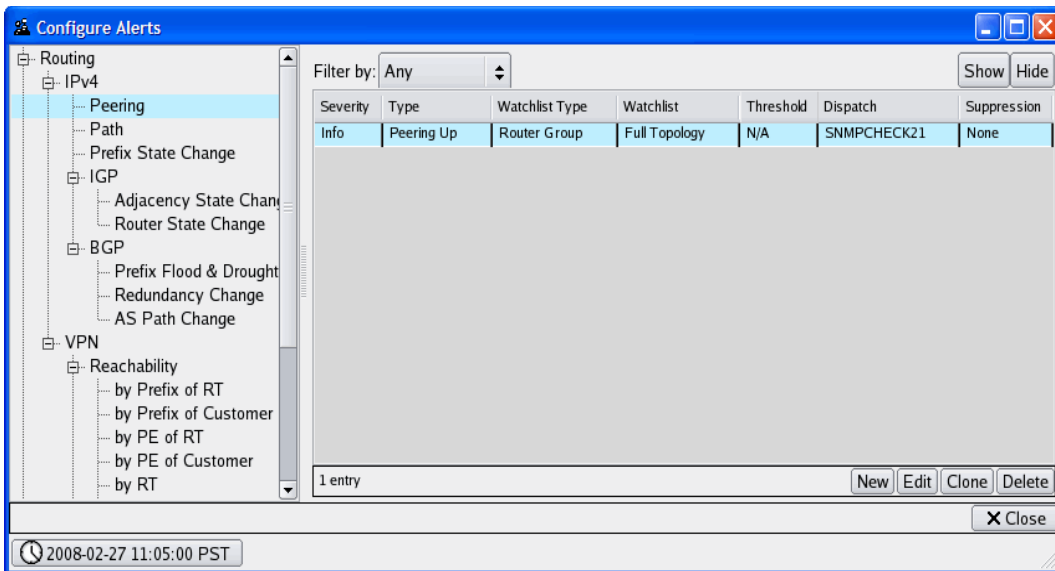


Figure 148 Configure Alerts

- 2 Choose any of the supported alert types from the side menu. See Table 74 .

Table 74 Alert Types

Alert Type	Description
IPv4 Alerts	
Peering State Change	Fired when an peering comes up, goes down or flaps, ^a depending upon the configuration selection.
Path Change	Fired when a path between a router and a prefix changes.
Adjacency State Change	Fired when a adjacency comes up, goes down or flaps, depending upon the configuration selection.
Prefix State Change	Fired when a route comes up, goes down, or flaps, depending upon the configuration selection.
Router State Change	Fired when all incoming links to a router go down or are overloaded (IS-IS only), when a router that was previously isolated is no longer isolated, or when the router flaps.
Prefix Flood & Drought	Fired when the number of prefixes heard from a BGP peer changes significantly.
Redundancy Change	Fired when the redundancy (number of next hops) for a prefix in BGP goes above or below the configured threshold.
AS Path Change	Fired when the AS path of any route in BGP changes.
VPN Alerts	
Reachability by Prefix of RT	Fired when a prefix comes up or goes down in a VPN RT.
Reachability by Prefix of Customer	Fired when a prefix comes up or goes down in a customer.
Reachability by PE of RT	Fired when number or percentage of routes gained/lost in an RT from a PE exceeds a threshold.
Reachability by PE of Customer	Fired when number or percentage of routes gained/lost in a customer from a PE exceeds a threshold.
Reachability by RT	Fired when number or percentage of routes gained/lost in an RT exceeds the threshold.

Table 74 Alert Types (cont'd)

Alert Type	Description
Reachability by Customer	Fired when number or percentage of routes gained/lost in a customer exceeds the threshold.
PE Participation by RT	Fired when number or percentage of PEs participating in an RT exceeds the threshold ^b .
PE Participation by Customer	Fired when number or percentage of PEs participating in a customer exceeds the threshold.
Traffic Alerts	
Low Link Utilization	Fired when link utilization is below the threshold.
High Link Utilization	Fired when link utilization is above the threshold.
Link Utilization by CoS	Fired when link utilization corresponding to a specified class of service (CoS) is above the threshold.
Test Alerts	Used to verify that alerts are being sent and that all specified endpoints are able to receive the alerts.

- a. Up, down, isolated, and connected events all count as flaps. For example, if a network element goes down and comes back up, the flap count increases by 2.
- b. A PE is considered to be participating in a VPN if it announces one or more routes in that VPN (RT or Customer).

The Configure Alerts window lists any alerts that have been created, and provides a snapshot of settings for each alert. Table 75 describes the columns on the page, which may vary according to the alert type.

Table 75 Alert Attributes

Item	Description
Severity	User-assigned importance levels are info, notice, warning, error, or critical.
Type	Type of the alert (see Table 14-1).
Watchlist Type	Type of group to which this alert applies. See Creating Groups Using the Menu on page 104 for information on creating groups.

Table 75 Alert Attributes

Item	Description
Watchlist	Specific group to which this alert applies. The alert is triggered only if the affected network elements are in this group.
Threshold	Parameter level that causes an alert to fire when it is reached. For flap events, the format is count:duration. Duration is presented in seconds (adjusted as needed if the alert was configured in minutes or hours).
Dispatch	User-defined name for the dispatch specification that occurs when an alert occurs.
Suppression	User-defined name for a set of conditions that allow alerts to ignore a condition until it reaches a specified level.

Creating New Alerts

You can configure new alerts.

To create a new alert, perform the following steps:

- 1 Choose **Alerts** → **Configure Alerts**.
- 2 Click the alert type on the side menu and click **New** to display the configuration parameters.

Filter by: Show Hide

Severity	Type	Watchlist Type	Watchlist	Threshold	Dispatch	Suppression
Critical	Router State Change	Nodes Group	ROUTER_GROUP_BGP_ALL	0:0	SQA_SNMP_SYSLOG_EMAIL	None
Warning	Router State Change	Nodes Group	ROUTER_GROUP OSPF_ALL	0:0	SQA_SNMP_SYSLOG_EMAIL	None

2 entries New Edit Clone Delete

Severity:

WatchList:

Flap Count (max 20):

Duration:

Suppression Spec:

Dispatch Spec:

Save Cancel

Figure 149 Creating a New Alert

- 3 Configure settings according to the descriptions in Table 76 . The available settings depend on the alert type.

Table 76 Alert Parameters

Item	Description
Severity	User-assigned importance levels: info, notice, warning, or critical.
Watchlist	<p data-bbox="339 309 1263 371">Group name representing the set of interest. The watchlist is a group, such as a router group or prefix group, depending upon the alert.</p> <p data-bbox="339 421 1245 548">If you choose an existing watchlist group or none, the field reflects that option. If you choose a new group, the New Group window opens. See Creating Groups Using the Menu on page 104 for information on creating groups.</p> <p data-bbox="339 598 1239 756">Note: The option None is included for some alert types to specify that all objects of the relevant type should be monitored. The option None is not included for alerts where the total number of objects is large enough that monitoring all of them is not practical due to processing or storage requirements.</p> <p data-bbox="339 807 1260 965">Note: Use the RegEx field in the Add Router Group window to restrict the displayed items in the Routers and Child Groups tabs. For example, if you only want IP addresses starting with 192, type 192 in the Select (RegEx) field, click OK by the field, and then click the arrow to move the selected IP addresses from the Available Items field to the Selected Items field.</p>

Table 76 Alert Parameters (cont'd)

Item	Description
Parameters	<p>Parameter that generates an alert if specified conditions are met. Availability of the following parameter types depends upon the type of alert:</p> <ul style="list-style-type: none">•Alert condition—isolated/connected, gain/loss, up/down, flap•Flap count and duration—Number of flaps within the specified duration•Flood, Drought threshold—Percent change from a baseline number of prefixes indicating a flood or drought of prefixes•Number of next hops—Number of hops for the AS path•RT—Selected RT to match•Customer—Selected customer to match•Threshold type— Absolute/percent.•COS—Class of service <p>Note: Isolated, connected, up, and down are each counted as a flap. For example, a rule could be set to generate an alert if there is a flap 10 times (isolated and/or connected) within 100 seconds.</p>
Dispatch Specification	<p>Name of the dispatch specification that controls how the alert should be delivered (email, SNMP, or syslog). Refer to Creating Dispatch Specifications on page 443 for instructions on defining a dispatch specification.</p>
Suppression Specifications	<p>Name of an optional suppression specification to limit the rate at which the alert may be generated or to specify a time interval when the alert should be ignored. Refer to Creating Suppression Specifications on page 447 for instructions on defining a suppression specification.</p>

- 4 Click **Save** to create the new alert.

Editing, Cloning, and Deleting Alerts

You can edit and delete alerts. You can also the clone option to create a new alert from an existing one.

To edit alerts, perform the following steps:

- 1 Choose **Alerts** → **Configure Alerts**.
- 2 Choose the alert type from the side menu and click **Edit**.
The alert parameters are shown in a panel at the bottom of the window.
- 3 Modify settings as described in Table 76 .
- 4 Click **Save**.

To create a new alert from an existing one, perform the following steps:

- 1 Choose **Alerts** → **Configure Alerts**.
- 2 Choose the alert type from the side menu and click **Clone**.
The alert parameters for the original alert are displayed.
- 3 Modify settings as described in Table 76 .
- 4 Click **Save**.

To delete an alert, perform the following steps:

- 1 Choose **Alerts** → **Configure Alerts**.
- 2 Choose the alert type from the side menu and click **Delete**.



You cannot recover an alert after it is deleted.

Viewing Alert Status

Select **Alerts** → **View Alert Status** to open the Alerts report. This report lists the time, severity, network, alert type, and description of the fired alert. You can sort the data in ascending or descending alphanumeric order by clicking any of the column headings. You can also show or hide selected alerts.



Only alerts that are logged to the database (as specified in the Dispatch Specifications window) appear in the Alerts report. Any records you delete cannot be recovered.



For networks that include the BGP/MPLS VPN feature, the Network column may occasionally contain an entry in the format 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. Users who do not want to see alerts for the opaque community strings should set a watchlist (an RT Group) on the appropriate alerts to restrict to the desired RT values. Use the Show RT communities only configuration option to control whether opaque RTs are shown on the routing topology map. See [Miscellaneous](#) on page 71 for a description of the option.

For more information about VPN reports, see [Chapter 8, “VPN Routing”](#)

Time	Severity	Network	Type	Message
2008-02-27 11:14:30.526947	Info	ISIS/Level2	Adjacency Up	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:15:12.376849	Info	ISIS/Level2	Adjacency Up	10.120.1.5 -> PD-REX-RECOR
2008-02-27 11:15:12.376849	Info	ISIS/Level2	Adjacency Up	10.120.1.5 -> PD-REX-RECOR
2008-02-27 11:15:12.376849	Info	ISIS/Level2	Adjacency Flap	10.120.1.5 -> PD-REX-RECOR
2008-02-27 11:15:12.376849	Info	ISIS/Level2	Adjacency Up	10.120.1.5 -> PD-REX-RECOR
2008-02-27 11:15:16.020710	Info	ISIS/27.0000.000	Adjacency Up	10.120.1.5 -> PD-REX-RECOR
2008-02-27 11:15:16.020710	Info	ISIS/27.0000.000	Adjacency Up	10.120.1.5 -> PD-REX-RECOR
2008-02-27 11:15:16.020710	Info	ISIS/27.0000.000	Adjacency Flap	10.120.1.5 -> PD-REX-RECOR
2008-02-27 11:15:16.020710	Info	ISIS/27.0000.000	Adjacency Up	10.120.1.5 -> PD-REX-RECOR
2008-02-27 11:16:04.645416	Info	ISIS/Level2	Adjacency Down	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:16:04.645416	Info	ISIS/Level2	Adjacency Flap	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:16:56.350407	Info	ISIS/Level2	Adjacency Up	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:16:56.350407	Info	ISIS/Level2	Adjacency Up	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:16:56.350407	Info	ISIS/Level2	Adjacency Flap	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:16:56.350407	Info	ISIS/Level2	Adjacency Up	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:17:44.626004	Info	ISIS/Level2	Adjacency Down	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:17:44.626004	Info	ISIS/Level2	Adjacency Flap	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:17:57.155882	Info	ISIS/Level2	Adjacency Up	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:17:57.155882	Info	ISIS/Level2	Adjacency Up	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:17:57.155882	Info	ISIS/Level2	Adjacency Flap	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR
2008-02-27 11:17:57.155882	Info	ISIS/Level2	Adjacency Up	SF-CORE-ROUTER2 (10.120.1.5) -> PD-REX-RECOR

Figure 150 Viewing Alerts Status

Filtering Alerts

You can modify the alert list by using filtering options.

To view specific alerts using the **Filter by** option, perform the following steps:

- 1 Open the client application and choose **Alerts** → **View Alert Status**.
- 2 Make a selection from the **Filter by** drop-down list.
 - If you choose **Severity**, select the severity levels you want to include from the check boxes in the **Options** drop-down list.
 - If you choose **IPv4 Alerts**, select the types of alerts you want to include from the check boxes in the **Options** drop-down list.
 - If you choose **VPN Alerts**, select the types of alerts you want to include from the check boxes in the **Options** drop-down list.

- If you choose **Traffic Alerts**, select the types of alerts you want to include from the check boxes in the **Options** drop-down list.
 - If you choose **Network**, enter the network to match, as indicated in the Network column. For the match, you can choose **Substring**, **Exact Match**, or **Begins With**.
 - If you choose **Message**, enter the string to match the message name, as indicated in the Message column. For the match, you can choose **Substring**, **Exact Match**, or **Begins With**.
 - If you choose **Acknowledgment**, you can choose **Acknowledged** or **Unacknowledged**.
 - If you choose **Expression**, you can type a simple expression in the adjacent field. For information on using this type of filter, see [Using Filters](#) on page 195.
 - If you choose **Advanced**, enter values in the window. For information on using this type of filter, see [Using Filters](#) on page 195.
- 3 Click **Show** to list only those records you want to view. Click **Hide** to have all hidden data reappear.

Acknowledging Alerts

Within the list of alerts, you can mark the records you have reviewed. Acknowledging an alert causes it to turn grey to indicate that you have investigated the activity. To acknowledge selected alerts, highlight the alerts and choose **Acknowledge** → **Selected**. To acknowledge all alerts in the list, choose **Acknowledge** → **All**.

If you inadvertently acknowledge an alert that you have not investigated, you can select it and click **Unacknowledge** → **Selected** to return the record to its original state.

A right-click menu is also available. Select one or more alerts and right-click to acknowledge, unacknowledge, or delete the alerts. For an individual alert, you can also choose **Move time to here** to change the historical time of the routing topology map to the time of the selected alert. Doing so allows you to view the network conditions at the time that the alert was generated.

Updating Alert Status

When the Alerts table opens the page scrolls to the end (sorted by time) and will start updating every 30 seconds to add new alerts. A message indicates when the table is updating.

If you select any rows in the table, the update stops so that the current selection does not automatically change. If any new alerts occur while rows are selected, a reload icon appears left of the buttons, along with an indication of the last real time when alerts were loaded into the table. Click the reload icon to turn row selection off and continue displaying new alerts when they occur. If the table is sorted ascending by time (the default) and scrolled to the end, then it will stay at the end.

Creating Dispatch Specifications

This section describes how to create new database, SNMP, Syslog, and Email dispatch specifications. Dispatch specifications determine the notification method used to inform you about network and traffic status.

To define dispatch specifications perform the following steps:

- 1 Open the client application and choose **Alerts** → **Dispatch Specifications**.
- 2 Click **Add**.
- 3 Enter a name for the dispatch specification.
- 4 Select the **Log to DB** checkbox. This allows you to view the alerts in the GUI.
- 5 Click **OK**.

To create a new SNMP dispatch specification, perform the following steps:

- 1 Open the client application and choose **Alerts** → **Dispatch Specifications**.
- 2 Click **Add**.
- 3 Enter a name for the dispatch specification.
- 4 Click the **SNMP** tab.

View Dispatch Specification

Name(max 30 chars): SQA_SNMP_SYSLOG_EMAIL

Log to DB

SNMP SYSLOG EMAIL

Address:

Port:

Community String:

Save

Address	Port	Communication String
192.168.0.48	162	public

1 entry

Edit Delete

OK Cancel

Figure 151 Defining an SNMP Dispatch Specification

- 5 Specify the address, port, and community string.
- 6 Click **Save** to add the SNMP information.
- 7 Click **OK** to save your settings or another tab to create additional specifications.

To create a new Syslog dispatch specification, perform the following steps:

- 1 Open the client application and choose **Alerts** → **Dispatch Specifications**.
- 2 Click **Add**.
- 3 Enter a name for the dispatch specification.
- 4 Click the **SYSLOG** tab.

View Dispatch Specification

Name(max 30 chars): SQA_SNMP_SYSLOG_EMAIL

Log to DB

SNMP **SYSLOG** EMAIL

Address:

Port:

SYSLOG Facility:
(This is a global setting) local0

Save

Address	Port
192.168.0.48	514

1 entry

Edit Delete

OK Cancel

Figure 152 Defining a Syslog Dispatch Specification

- 5 Specify the address and port number for the syslog.
The SYSLOG Facility field is a global setting; that is, it is used by all alerts that specify a Syslog dispatch.
- 6 Click **Save** to add Syslog information.
- 7 You can modify existing Syslog information by selecting the address and clicking **Edit**.
- 8 Click **OK** to save your settings or another tab to create additional specifications.

To create a new Email dispatch specification, perform the following steps:

- 1 Open the client application and choose **Alerts** → **Dispatch Specifications**.
- 2 Click **Add**.
- 3 Enter a name for the dispatch specification.

- 4 Click the **EMAIL** tab.

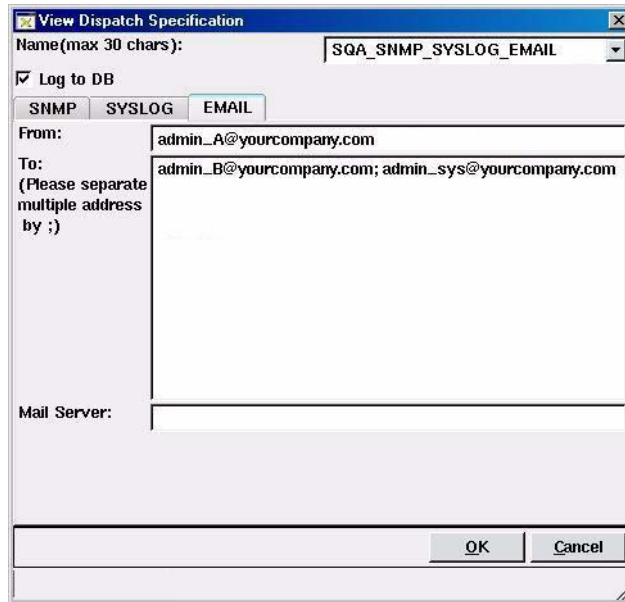


Figure 153 Defining an Email Dispatch Specification

- 5 From the **EMAIL** tab you can:
 - Set the email address that is the source for sending the dispatch notifications.
 - Create a list of destination email addresses (separated with semicolons).
 - Set the default mail server IP address or the DNS name that is used to send out the email. If left blank, the mail protocol sends email through the default mail server for that network as specified on the Mail page in the administration web pages. See “Administration” in the *HP Route Analytics Management System Administrator Guide*.
- 6 Click **OK** to save your settings or another tab to create additional specifications.

Editing, Duplicating, and Deleting Dispatch Specifications

You can edit and delete dispatch specifications. You can also use the duplicate option to create a new dispatch specification from an existing one.

To edit a dispatch specification, perform the following steps:

- 1 Choose **Alerts** → **Dispatch Specifications**.
- 2 Choose the dispatch specification and click **Edit**.
- 3 Modify settings as described in [Creating Dispatch Specifications](#) on page 443.
- 4 Click **Save**.

To create a new dispatch specification from an existing one, perform the following steps:

- 1 Choose **Alerts** → **Dispatch Specifications**.
- 2 Choose the dispatch specification and click **Duplicate**.
- 3 Modify settings as described in [Creating Dispatch Specifications](#) on page 443.
- 4 Click **Save**.

To delete a dispatch specification, perform the following steps:

- 1 Choose **Alerts** → **Dispatch Specifications**.
- 2 Choose the dispatch specification and click **Delete**.



You cannot recover an alert after it is deleted.

Creating Suppression Specifications

This section describes how to create new suppression specifications. Suppression specifications determine the periods when no alerts are generated and sets rate limits on delivering alerts.

To define suppression specifications perform the following steps:

- 1 Open the client application and choose **Alerts** → **Suppression Specifications** to open the Alerts Suppression Specifications window. This lists user-defined alert exclusions based on frequency and date/time.
- 2 Click **Add**.

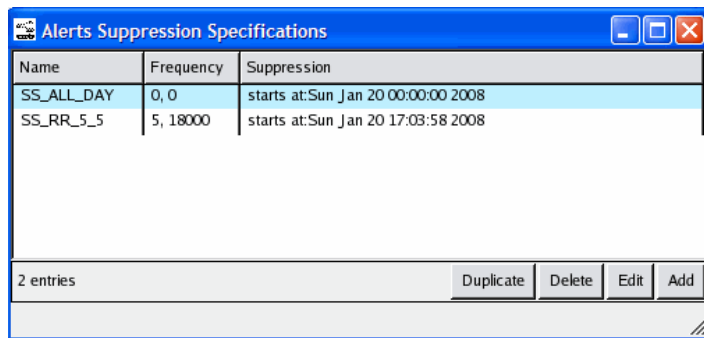


Figure 154 Suppression Specifications

- 3 Enter a name for the suppression specification.
- 4 Click the **Schedule** tab.

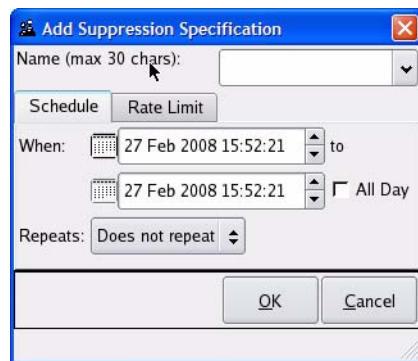


Figure 155 Suppression Specification - Schedule

- 5 Specify the schedule that determines when alerts are suppressed.
- 6 For the repeat frequency, you can choose never, daily, weekly, monthly or yearly. If this is a nonrepeating suppression, the remaining repeating frequency options do not appear.

- 7 Click the **Rate Limit** tab.

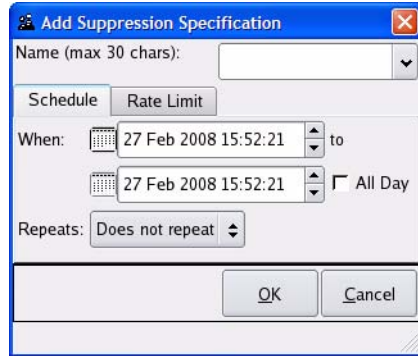


Figure 156 Suppression Specification - Schedule

- 8 From the **Rate Limit** tab you can determine the minimum acceptable count or duration.

You can specify a rate above which the alert notification is suppressed. For example, with a rate limit of 5 alerts in 10 minutes, alerts are suppressed starting with the sixth alert in that interval. The suppression applies per individual alert, not over an entire type of alert.
- 9 Click **OK** to save your settings.

Editing, Duplicating, and Deleting Suppression Specifications

You can edit and delete suppression specifications. You can also use the duplicate option to create a new suppression specification from an existing one.

To a edit suppression specification, perform the following steps:

- 1 Choose **Alerts** → **Suppression Specifications**.
- 2 Choose the suppression specification and click **Edit**.
- 3 Modify settings as described in [Creating Suppression Specifications](#) on page 447.
- 4 Click **Save**.

To create a new suppression specification from an existing one, perform the following steps:

- 1 Choose **Alerts** → **Suppression Specifications**.
- 2 Choose the dispatch specification and click **Duplicate**.
- 3 Modify settings as described in [Creating Suppression Specifications](#) on page 447.
- 4 Click **Save**.

To delete a suppression specifications, perform the following steps:

- 1 Choose **Alerts** → **Suppression Specifications**.
- 2 Choose the dispatch specification and click **Delete**.
- 3 You cannot recover an alert after it is deleted.

A Protocol Compliance

This appendix lists protocol compliance information.

- OSPF:
 - RFC 2328, OSPF Version 2
 - RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option
- ISIS
 - ISO 10589, or RFC 1142 (ISO 10589 draft), OSI ISIS Intra-Domain Routing Protocol
 - RFC 1195, Use of OSI ISIS for Routing in TCP/IP and Dual Environments
 - RFC 2763, Dynamic Hostname Exchange Mechanism for ISIS
 - RFC 3784, ISIS Extensions for Traffic Engineering
 - RFC 2966, Domain-wide Prefix Distribution with Two-Level ISIS
 - RFC 3567, ISIS Cryptographic Authentication
- BGP:
 - RFC 4271, BGP Version 4
 - RFC 2796, BGP Route Reflection
 - RFC 1997, BGP Communities Attribute
- EIGRP: Since EIGRP is a Cisco proprietary protocol, there is no RFC to specify the protocol. Documentation for EIGRP is available on the Cisco website (<http://www.cisco.com/warp/public/103/eigrp-toc.html>).

The following implementations for multi-protocol route resolution are incomplete:

- RFC2328: 16.3 (summary LSAs in transit-area)
- ISO/IEC 10589: QoS metric, virtual link

- ECMP for BGP next hops

Index

A

acknowledging, 442

Activity by AS report, 321

Activity by Peer report, 322

Activity Summary report, 320

add

- node, 222

- peering, 222

- prefix, 223

- traffic flow, 223

Administration menu, 60

aggregate flows traffic reports, 377

aggregate traffic reports, 371

alerts, 431, 442

- attributes, 433

- configuring, 431, 439, 441, 447, 449, 450

- creating, 434

- description, 430

- dispatch specifications, 443

- editing, cloning, deleting, 438

- filtering, 441

- IPv4, 432

- menu, 430

- router isolated, 181

- suppression specifications, 447

- test, 433

- traffic, 433

- types, 432

- updating status, 443

- viewing status, 440

- VPN, 432

Alerts menu, 60

all events list, 177

analysis

- event, 171

- history, 139

- options, 69

- root cause, 143, 144

Analysis mode, 24, 47, 48, 76, 137

analyze edits, 53, 59, 262

- animation, 146
 - button, 139
 - clock, 147
 - fast, 140
 - graph, 148
 - mode, 139, 148
 - playing, 148
 - saving, 150
 - window, 146
- anomalies, network, 67
- application interface, 24
- AS assignments to routers, 131
- AS names
 - assigning, 128
- AS Reachability Report, 326
- AS Reachability report, 326
- asymmetric paths, 416
- asymmetric paths analysis report, 416
- auto-hide
 - options, 74
- automatic labels, 70
- Autonomous Systems (AS) repository, 128

B

- bandwidth, 364
 - changing, 249
- bar charts and tables, 171
- Baseline AS Reachability report, 328
- Baseline Redundancy by Prefix report, 326
- baselines
 - calculating, 318, 326, 328, 331
- Before-N-After comparison, RIB, 166

BGP

- adding prefix, 230
- graphs, 142
- prefix, 244
- protocol
 - Before-N-After comparison, 167
 - RIB browser, 158
- reports, 317
 - accessing, 301, 319
 - Activity by AS, 321
 - Activity by Peer, 322
 - Activity Summary, 320
 - AS Reachability, 326
 - Baseline AS Reachability, 328
 - Baseline Redundancy by Prefix, 326
 - logical topology, 323
 - Prefix Event Detail, 323
 - Prefix Reachability, 328
 - Redundancy by Prefix, 326
 - Route Distribution Detail, 324
 - Route Flap, 322
- traffic reports, 388

BGP AS assignments, 131

BGP Reports, 25

BGP reports

- accessing, 319
- description, 320
- understanding, 318

- bitrate, changing, 249
- bounding box, 78, 81

button

- Add Node, 222
- Add Peering, 222
- Add Prefix, 223
- Add Traffic Flow, 223
- Analysis, 139, 143
- Animation, 146
- Change Prefix, 223
- Clear, 179
- Down Node, 224
- Down Peering, 224
- Down Prefix, 224
- Events, 139, 146
- Execute One Event, 179, 187
- Fast Animate, 140
- Fast Step, 139
- Go to End, 148
- Go to Start, 148
- Graphs, 139
- Hide, 164, 184
- History Navigator, 138
- List Routers, 92
- Online Update, 179
- Prefixes, 146
- Show, 164, 184
- Show Current Event, 179, 187
- Start Execution, 179, 187
- Step, 139
- Stop, 139
- Stop Execution, 179, 187
- Time Range, 139, 179, 186
- Topology Map toolbar, 49
- Update, 139

C

- capacities, setting interface, 364
- capacity, 364

capacity planning reports

- aggregate, 281
- exporter, 283
- flow collectors, 284
- IPv4, 284
- link, 281
- navigation tree, 279
- settings, 279
- VPN traffic, 291

- capacity planning reports description, 279

- CE router, 330

- Changed Metrics report, 304

- clearing events, 179

client application

- opening, 36
- opening in X-Win32, 31
- opening with VNC, 37
- viewers, 28

clock

- animation, 147
- icon, 179, 186

cloud

- expanding, 101
- menus and options, 101
- network elements, 101
- panel buttons, 102
- prefixes, 102
- routers, 102
- VPN prefixes, 103

- cluster event analysis, 171

- cold spots, 418

collector

- traffic flow, 20

- community planning reports, 274

comparison

- RIB Before-N-After, 166
- RIB Browser, 165

- compliance information
 - protocol
 - compliance, 451
- components
 - data flow, 20
 - RAMS, 19
- configuration
 - VPN, 332
- controls
 - History Navigator, 136
 - playback, 147
- CoS planning reports, 266, 269, 275
- cost, path, 118
- cursor
 - dragging to change time view, 138
 - History Navigator, 138
- customer and RT associations
 - setting up, 334
- customers planning reports, 276
- custom filter
 - adding, 86
 - deleting, 87
 - editing, 87
 - repository, 85

D

- database
 - in green letters, 40
 - recording, 40
- designated router, 77
- destination AS planning reports, 273
- diagnostics
 - topology, 121

- dispatch specifications, 443
 - creating, 443
 - editing, cloning deleting, 447
 - email, 445
 - SNMP, 443
 - syslog, 444
- distributed configuration
 - configuring route recorder in, 24
 - IGP and BGP reports for, 25
- DNS
 - displaying node name, 77

E

- ECMP paths analysis report, 414
- Edit Flows window, 223
- egress PE planning reports, 278
- egress router, 272
- egress router report, 272
- EIGRP
 - distances, mismatched, 125
 - highlighted path cost, 118
 - path cost, defined, 118
 - prefix types, 182
 - topology diagnostics, 121
 - update event, 182, 187
- enable XML RPC queries, 333

- event, 139, 146
 - adjusting time range, 185
 - analysis, 171
 - clearing, 179
 - details, 179
 - BGP, 184
 - EIGRP, 182
 - IS-IS, 179, 182
 - OSPF, 179, 181
 - execute, 187
 - executing, 179, 186
 - start, 179, 187
 - stop, 179, 187
 - filtering, 184
 - graph, 142
 - highlighting associated nodes, 184
 - list all, 177
 - listing all, 123, 177
 - matching time, 185
 - online, 123
 - prefiltering, 144, 171, 177, 185, 195
 - showing current, 179, 187
 - time interval, 171

- event graph
 - time interval, 171

- exit router, 84

- exporters reports, 266

- expression
 - definitions, 200
 - filter, 195
 - regular, 83
 - syntax, 199

F

- failure analysis
 - description, 424

- features, 18

- file upload, 194

- filter, 232, 359
 - advanced planning reports, 264
 - alerts, 441
 - custom, 85
 - definitions, 200
 - events, 184
 - expression examples, 199
 - expressions, 195
 - syntax, 199
 - using, 195

- Filter by, 232

- find
 - paths, 118

- flapping, prefix, 145

- Flapping Links report, 305

- Flow Analyzer, 20

- Flow Analyzer reports, 367

- Flow Collector, 20

- traffic reports, 376

- flow server, adding, 247

G

- graph
 - animation, 148
 - button, 139
 - displaying, 141
 - events, 142
 - History Navigator, 141
 - network events, 78, 81
 - routers, 141
 - routes, 141
 - trending, 169

- GRE tunnels, 20

- grouping nodes, 100

- groups
 - network element, 98
 - on Topology Map, 98

H

- hidden nodes, 55, 74, 78, 82
- hierarchy
 - topology, 55
- History Navigator, 25, 133
 - accessing, 135
 - and EIGRP topology errors, 121
 - button, 138
 - controls, 136
 - cursor, 138
 - displaying graphs, 141
 - example of use, 187
 - fast step, 139
 - graphs, 141
 - mode, 50, 136
 - options, 73
 - playback controls, 139
 - status bar, 138
 - switching modes, 137
 - trending, 169
 - update, 139
 - zoom timeline, 140
- history navigator
 - and VPN reports, 350
- hot spots, 418

I

- IGP
 - add prefix, 234
 - bandwidth, 364
 - protocols
 - Before-N-After comparison, 166
 - RIB browser, 158
 - reports, 299
 - Changed Metrics, 304
 - Flapping Links, 305
 - Network Churn, 306
 - Network Events Summary, 303
 - New Prefixes, 307
 - New Routers and Links, 308
 - Prefixes Withdrawn, 314
 - Prefix List, 309
 - Prefix Origination Changes, 311
 - Prefix Origination from Multiple Sources, 312
- IGP Reports, 25
- IGP reports
 - accessing, 300
 - configuring, 301
 - contents, 303
 - understanding, 300
- import
 - time series data, 193
- inaccessible routers
 - EIGRP, 123
 - list of, 121, 123
- information, viewing system, 36
- information panel, 76
 - link, 79
 - node, 77, 84
- ingress PE planning reports, 277
- interface
 - application, 24
 - status, link details, 80

- interface capacities, 364
 - metric, 366
 - setting, 364
 - specifying bandwidth, 366
 - specifying capacity, 366
 - use cases, 364
- interfaces list, 94
- invisible links, finding, 121, 128
- IPv4
 - traffic reports, 379
- IPv4 alerts, 432
- IPv4 BGP traffic planning reports, 271
- IPv4 capacity planning reports, 284
- IPv4 Links report, 350
- IPv4 planning reports, 268
- IPv4 Routers report, 350
- isolated router alert, 181

L

- layout
 - saving, 55
 - topology
 - default, 71
- Legend, 51
- legend, 43
- link
 - details, 76
 - finding invisible, 121, 128
 - hot and cold, 418
 - information panel, 79
 - interfaces list, 94
 - invisible, in EIGRP, 128
 - list all, 93, 95
- link list, 93
- Linux, 31
 - installing VNC, 34

- list
 - all events, 177
 - inaccessible routers, 121
 - mismatched distances, 121
 - paths, 118
 - topology errors, 121
- Logical Topology BGP reports, 323
- loopback, 182

M

- map
 - Routing Topology, 24
 - topology, 225
- MED, 162, 163, 189
- metric, and interface capacities, 366
- mismatched distances
 - EIGRP, 125
 - listing, 121, 125
- mode
 - Analysis, 24, 47, 48, 76, 137
 - animation, 148, 149
 - fast stepping, 149
 - History, 136
 - History Navigator, 50
 - Monitoring, 24, 48, 76, 136
 - Online, 136
 - Planning, 24, 47, 48, 137, 220, 221
 - Step, 139, 149
 - switching, 137
- Modeling Engine, 20
- modes
 - switching, 137
- Monitoring mode, 24, 48, 76, 136
- MPLS, 329
- MRTG, 193
 - file formats, 194
- multi-exit discriminator, 162, 163, 189

Multiprotocol Label Switching
 see MPLS
Multi Router Traffic Grapher, see MRTG

N

neighbor AS planning reports, 272
NetFlow, 20
network
 anomalies, 67
 events, 78
 events, graph, 81
 inventory, 91
 large, viewing, 84
Network Churn report, 306
network element analysis, 418
Network Events Summary report, 303
New Prefixes report, 307
New Routers and Links report, 308
node information panel, 84
nodes
 adding, 222
 bringing down, 224, 254
 bringing up, 255
 details, 76, 77
 displaying DNS name, 77
 hidden, 55, 74, 78, 82
 hiding failed, 56
 highlighting, 184
 information panel, 77, 115
 labels, 70
 re-hide, 78
 restoring visibility, 83
 trim, 82
 trim leaf, 55
 unhide, 82
 unhide all, 56
non-ECMP paths analysis report, 415

NSAP address, 70, 72

O

online events, 123
online update, 179
 button, 179
opaque RTs, 73
opening
 routing topology map, 40
options
 analysis, 69
 auto-hide, 74
 miscellaneous, 71
 visualization, 69
overload bit, 253
overload router, 77

P

Path Reports, 25
path reports, 403, 418
 asymmetric link metrics, 424
 asymmetric paths, 416
 down links, 423
 down nodes, 423
 ECMP paths, 414
 failure analysis, 424
 failure-induced ECMP analysis, 427
 link failure analysis, 426
 link hot spots, 420
 non- ECMP paths, 415
 path statistics, 409
 selecting topology, 404
 unused links, 421
 using window, 407

- paths, 116, 117
 - asymmetric, 416
 - cost, 118
 - finding, 118
 - hot and cold, 418
 - listing, 116, 117, 118
 - reports, 416
 - router hot spots, 419
- path statistics report, 409
- PE
 - adding VRF, 235
- peering
 - adding, 222, 227
 - bringing down, 224, 255
- PE router, 330
- planning
 - menu, 221
 - network, 219
 - toolbar, 225
- Planning menu, 58, 221
- Planning mode, 24, 47, 48, 137, 220, 221
- planning reports, 259, 272
 - advanced filtering, 264
 - aggregate, 264
 - capacity planning, 279
 - community, 274
 - CoS, 266, 269, 275
 - customers, 276
 - destination AS, 273
 - drill-down, 261
 - editing, 262
 - egress PE, 278
 - exporters report, 266
 - flow collectors, 267
 - flows report, 267, 271
 - icons, 262, 408
 - ingress PE, 277
 - IPv4, 268
 - IPv4 traffic, 271
 - links report, 265
 - navigation tree, 260
 - neighbor AS, 272
 - transit AS, 272
 - VPN flows, 278
 - VPN traffic, 274
- Planning Reports window, 25
- Planning toolbar, 225
- playback
 - animation mode, 149
 - controls, 139, 147
 - fast step, 149
 - set step, 74
 - Step mode, 149
- prefilter, 178

- prefix
 - adding, 223, 230
 - BGP, 230
 - IGP, 234
 - with filter, 231
 - bringing down, 224, 257
 - button, 146
 - changing, 223, 235
 - finding route by, 116
 - flapping, 145
 - report, 350
 - shifting, 145
 - types, EIGRP, 182
- prefixes
 - changing, 244
- Prefixes Withdrawn report, 314
- Prefix Event Detail report, 323
- Prefix List report, 309
- Prefix Origination Changes report, 311
- Prefix Origination from Multiple Sources report, 312
- Prefix Reachability report, 328
- protocol
 - link-state, 19
 - multiple, in history navigator, 136
 - supported, 19
- provider's edge (PE) router, 330
- pseudonode, 77, 80, 84

R

- RAMS
 - components of, 19
 - operation of, 19
- reachability
 - and participation index, 331

- recorder
 - NetFlow, 20
 - routing, 19
- Redundancy by Prefix report, 326
- RegEx, 83, 406
- regular expression, 83, 200, 406
- re-hide nodes, 78
- report, 419
- reports
 - BGP, 25, 317, 319
 - capacity planning, 279
 - IGP, 25, 299, 301
 - network element analysis report, 418
 - Path, 25
 - path, 403
 - Planning, 25
 - planning, 259
 - Prefixes, 350
 - selecting topology for path reports, 404
 - Traffic, 25, 351
- Reports menu, 58
- repository, router name, 88
- restore
 - nodes, 83
- RFCs, 451
- RIB
 - Before-N-After comparison dialog, 166
 - browser, 158, 175
 - visualization window, 151, 158
- root cause analysis, 143, 144
- Round Robin Database (RRDtool), 194
- route
 - finding, 84
 - finding by prefix, 116
 - redistributing, 123
 - summarization, and invisible links, 128

- Route Distribution Detail By Next Hop AS report, 325
- Route Distribution Detail By Next Hop report, 325
- Route Distribution Detail By Peer router, 325
- Route Distribution Detail By RRC report, 325
- Route Distribution Detail report, 324
- Route Flap report, 322
- router
 - CE, 330
 - exit, 84
 - finding, 84, 92
 - graph, 141
 - inaccessible, EIGRP, 123
 - isolated alert, 181
 - list all, 92
 - naming conventions, hiding by, 82
 - PE, 330
- Route Recorder, 19
- router hot spots, 419
- router names
 - assigning, 88
 - changing, 90
 - changing multiple, 90
 - repository, 88
- routers
 - BGP AS assignments, 131
- routes graph, 141
- route target (RT), 61
- routing
 - loop, 123
- Routing Information Base
 - see RIB

- Routing Topology Map, 24
 - menu, 53
 - opening, 54
 - selecting, 40, 54
 - toolbar, 49
- routing topology map
 - opening, 40
- RT
 - and customer associations, 332
 - and VPN customer mappings, 61
 - opaque, 73

S

- saving
 - animation, 150
 - topology layout, 55
 - visualization, 156
- server
 - flow, 247
- shifting, prefix, 145
- Solaris, 31
- state changes, viewing, 179
- status
 - alerts, 440, 443
- status bar
 - History Navigator, 138
 - Routing Topology Map, 47
- summarization boundaries, and EIGRP, 128
- suppression specifications, 447
 - editing, cloning deleting, 449
 - rate limit, 449
 - schedule, 448
- SVG plug-in, 35
- syntax
 - filter expression, 199
- system
 - viewing information, 36

T

test alerts, 433

time

- adjusting range, 185
- moving, 185
- setting range, 139, 179, 186

timeline, zooming, 140

time series data, 194

- correlating, 193
- importing, 193
- uploading, 194

Tools menu, 56

topology

- diagnostics, 121
 - EIGRP, 121
 - submenu, 121
- errors
 - EIGRP, 121
 - list, 121, 122
- hierarchy, 55
- map, 24
- map, colors, 70
- saving a layout, 55
- selecting, 40
- status bar, 47
- window, 49, 55, 64, 262

Topology Map, 225

- creating groups, 98
- grouping nodes
 - groups
 - from nodes, 100
- network element groups, 98

traffic

- data delay, 138, 139, 179
- loading, 143
- reports, 351

traffic alerts, 433

traffic flow

- adding, 237, 249
- changing bitrate, 249
- deleting, 250
- editing, 246, 251
- moving, 250

traffic flows

- editing, 246

Traffic Reports, 25

traffic reports

- accessing, 353
- advanced filtering, 359
- aggregate, 371
- aggregate flow, 377
- BGP, 388
- buttons, 355
- column settings, 356
- data examples, 352
- data granularity, 359
- description, 351
- difference column, 359
- drill down, 360
- drill down history, 363
- flow collectors, 376
- IPv4, 379
- navigation tree, 354
- report types, 367
- statistics column, 358
- understanding, 351
- VPN, 394
- working with, 356
- workspace and buttons, 352

traffic reports, advanced, 359

transit AS planning reports, 272

trending, 169

trim

- leaf nodes, 55
- nodes, 82

- tunnels
 - GRE, 20
 - VPN, 330

- types, 431

U

- unhide nodes, 82

- UNIX, 31

- unused links report, 421

- upload
 - to appliance, 194

- user interface
 - application, 24
 - web, 23

V

- viewer, 23

- viewers
 - options, 28
 - VNC, 32
 - Xmanager, 28
 - Xming, 28
 - Xwin-32, 28
 - X Window system, 28

- View menu, 55

- views, 28

- visualization
 - options, 69
 - RIB, 151
 - saving, 156

- VNC, 23
 - installing, 32
 - opening application, 37
 - opening client application, 37

- VNC viewer, 32

VPN

- adding customer, 242
- configuration, 332
- customer configuration, 61
- customer flow, 240
- editing traffic flows, 251
- protocol, 329
- reachability and participation index, 331
- reports
 - accessing, 337
 - history navigator, 350
 - Prefixes, 350
 - Summary, 339, 340, 341, 342, 343, 345, 346
- starting, 33
- traffic reports, 394
- tunnels, 330

- VPN alerts, 432

- VPN Customers History report, 341

- VPN flows planning reports, 278

- VPN PE Participation Customers report, 346

- VPN PE Participation History report, 345

- VPN PE-PE flow, 239

- VPN Prefixes report, 340, 350

- VPN Reachability History report, 342

- VPN reports
 - accessing, 337
 - customer and RT associations
 - about, 332
 - detailed information, 347

- VPN Summary report, 339

- VPN traffic capacity planning reports, 291

- VPN traffic planning reports, 274

VRF

- adding to PE, 235
- bringing down, 258
- editing, 254

W

web interface, 23

X

Xmanager, 28

Xming, 28

X-Win32, 29, 30

Xwin-32, 28

X Window System, 23

X Window system
using, 28

Z

zoom

History Navigator timeline, 140