Cisco Service Path Analyzer User Guide

Release 1.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-12860-01

Cisco Service Path Analyzer User Guide

CONTENTS

Preface xix

Overview xix

Audience xix

Organization xx

Chapter-Level Organization xxi

Related Documentation xxi

Additional Technical References xxii

OSPF Technical Information xxii

BGP Technical Information xxiii

Support for Alarm Trigger Exporting xxiii

Open Source License Acknowledgements xxiv

OpenSSL/Open SSL Project xxiv

Obtaining Documentation, Obtaining Support, and Security Guidelines xxv

CHAPTER 1 **Getting Started** 1-1

Getting Started with Path Analyzer 1-1

Monitor Routing Activities Within Domains 1-1

Monitor Routing Activities Between Domains 1-2

View Routing Data in the Path Analyzer Management Console 1-2

Simultaneous, Multi-User Monitoring and Administration 1-2

Complete Set of System Administration Tools 1-3

Starting Path Analyzer 1-3

Start Path Analyzer in Microsoft Windows 1-4

Start **Path Analyzer** in a Supported Unix-Based Operating System 1-4

Log in to **Path Analyzer** 1-4

Verify Your Connection 1-5

Additional Taskbar Indicators 1-6

Collector Status Indicators 1-6

Features of the Management Console 1-7

Path Analyzer Taskbar 1-7

Select a Module 1-8

A Real-time View of Your Network 1-12

Monitor Service Paths 1-14

Monitor Routing Changes in OSPF or BGP Event Logs 1-15

Query for Specific Events 1-17
Set and Monitor Alarms and their Triggers 1-17
Create Reports and Charts 1-17
Replay and View Historical Events 1-17
Navigating in the Path Analyzer Management Console 1-17
Move and Resize Windows and Dialog Boxes 1-18
Manage Windows and Sessions 1-19
Minimize Open Windows 1-21
Restore a Minimized Window 1-21
Change between Real-time and Historical Sessions 1-21
Select a Module Window 1-22
Log out of Path Analyzer 1-23
Exit Path Analyzer 1-23
Move or Copy Information 1-23
Set Preferences 1-24
Select Topology Viewer Settings 1-25
Select Preferences for Router Names 1-29
Set the Formatting of Dates and Times 1-32
Set Automatic Completion of Fields 1-33
Set Modules to Start Automatically 1-34
Set the Amount of Time to Keep Charts, Reports, and Schedules 1-35
Using Help 1-36
View an Online Manual 1-36

CHAPTER 2 **Monitoring Your Network's Topology** 2-1
Viewing Your Network Topology in Detail 2-1
Structure of Your Network in Cisco Service Path Analyzer 2-1
Exchanges of Routers Between Autonomous Systems 2-1
Topology Viewer Shows Your Network's Topology 2-2
Open Investigative Event Log to Query for Related Events 2-3
Starting the Topology Viewer 2-4
Start the Flat Topology Viewer 2-4
Start the Hierarchical Topology Viewer 2-4
Start the Service Viewer 2-5
Start the Topology Browser 2-5
Start the Investigative Topology Browser Wizard 2-5
Viewing Your Network Topology 2-6
View the Flat Topology Viewer 2-6
View the Hierarchical Topology Viewer 2-7

View Exploratory Paths 2-8
How Path Anaylzer Generates the Network Topology 2-12
Viewing Changes of Status 2-13
Identifying Topology Viewer Elements 2-14
Autonomous Systems 2-19
Areas 2-20
Routers 2-21
OSFP Routes and Advertisements 2-25
BGP Routes, Prefixes, and Prefix Families 2-28
BGP Filtering 2-28
Networks and Subnets 2-29
Interfaces and Links 2-30
Navigate Using the Overview Frame 2-33
Move Topology Viewer Elements 2-37
Expand and Collapse Topology Elements 2-37
Limit and Expand Your View of the Topology 2-38
Change Location from an Area Node 2-40
Change the Layout of the Topology Viewer 2-41
Save a Topological Layout 2-42
Remove a Topological Layout 2-42
Apply a Topological Layout 2-43
Hide and Show Routers and Topology Elements 2-43
When to Hide Edge Routers 2-44
Viewing Services in the Service Viewer 2-45
Getting Detailed Information About Topology Viewer Elements 2-45
Link to Additional Information 2-47
Navigating in Topology Browser Dialog Boxes 2-48
Viewing Metrics and Attributes 2-54
Pivoting to the Event Log 2-64
Investigate Events 2-64
Using the Topology Filter Wizard for BGP Entities 2-65
BGP Query Types and Constraints 2-66
BGP Filtering Example: VPN Route List 2-67
Data Entry Format for BGP Topology Filter Constraints 2-80
Making Routing Information Base (RIB) Comparisons for BGP Routes 2-81
RIB Comparison Example: IPv4 Routes for VRFs 2-81
Querying for Network Elements (for OSPF Entities) 2-82
Issue a Fast Query 2-83
Query for an OSPF Interface 2-84

Query for a Route Advertisement 2-85
Query for OSPF Interfaces 2-85
Specify Additional OSPF Interface Query Constraints 2-89
Query for an OSPF Route Advertisement 2-90
Specify Additional Advertisement Query Constraints 2-93
Use a Query as a Template for a New Query 2-94
Previewing and Printing a Topology 2-95
Related Forms 2-96
Topology Viewer 2-96
Topology Viewer Toolbar 2-97
Topology Browser Dialog Boxes 2-99

CHAPTER 3 **Monitoring Unicast and Multicast Services** 3-1
Monitoring Data Between Endpoints 3-1
Differentiating Unicast and Multicast Services 3-1
Monitoring Unicast Services 3-2
Branches of a Unicast Service 3-2
Visual, Real-time Traceroute on Multiple, Simultaneous Flows 3-2
Starting Service Monitor 3-3
Monitoring the Flow of Business-Critical Data 3-4
How Data is Displayed in Service Monitor 3-4
Unicast Service Paths: Endpoints of a Service 3-4
Creating Unicast Services and Related Service Paths 3-7
Required Information for Creating a Unicast Service or Service Path 3-7
Create Uni-Directional or Bi-Directional Service Paths for a Unicast Service 3-7
Interpreting Service Data for Unicast Services 3-15
Viewing Unicast Services Graphically 3-19
Viewing the Root Cause of Unicast Service Path Issues 3-23
View the Root Cause of a Change to a Unicast Service Path 3-23
Viewing Details of Unicast Services and Unicast Service Paths 3-24
View Details of a Unicast Service 3-24
View Details of a Service Path 3-24
Managing Baselines of Service Paths 3-25
Resetting and Removing Baselines 3-25
Managing Unicast Services and Service Paths 3-26
Enabling and Disabling Unicast Services and Service Paths 3-31
Disable a Unicast Service 3-31
Disable a Service Path 3-31

Enable a Unicast Service 3-32
Enable a Service Path 3-32
Setting Alarms on Unicast Services and Service Paths 3-32
Replaying Historical Services 3-33
Related Forms 3-33
Details of a Unicast Service 3-33
Details of a Unicast Service Path 3-33
Details of Service Path Branches Dialog Box 3-34
Monitoring Multicast Services 3-35
Branches of a Multicast Service 3-36
Visual, Real-time Traceroute on Multiple, Simultaneous Flows 3-36
Starting Service Monitor 3-37
Start Service Monitor 3-37
Monitoring the Flow of Business Critical Data 3-38
How Data is Displayed in Service Monitor 3-38
Viewing SSM Multicast Service Groups 3-40
Viewing Details of Multicast Services and SSM Multicast Service Groups 3-41
Creating Multicast Services and Related SSM Multicast Service Groups 3-43
Required Information for Creating a Multicast Service or SSM Multicast Service Group 3-43
Interpreting Service Data on a Multicast Service 3-48
View the List of Multicast Services and Related Distribution Trees 3-50
Viewing Multicast Services Graphically 3-53
Display Graphical Multicast Service 3-58
Display Graphical Multicast Tree 3-59
Remove a Graphical Multicast Service 3-60
Remove a Graphical Multicast Tree 3-61
Viewing the Root Cause of Multicast Services Issues 3-61
Viewing Details of Multicast Services and SSM Multicast Service Groups 3-62
Managing Baselines of Multicast Service and SSM Multicast Service Groups 3-63
Reset the Baseline of a Selected SSM Multicast Service Group 3-63
Remove the Baseline of an SSM Multicast Service Group 3-63
Reset the Baseline of an SSM Multicast Service Group 3-64
Remove Baselines of an SSM Multicast Service Group 3-64
Managing Multicast Services and SSM Multicast Service Groups 3-64
Remove a Single Multicast Service 3-65
Remove Multiple Multicast Services 3-65
Add SSM Multicast Service Groups 3-66
Remove a Single SSM Multicast Service Group 3-67

Remove Multiple SSM Multicast Service Groups 3-67
Reconfigure a SSM Multicast Service Group 3-68
Enabling and Disabling Multicast Services and SSM Multicast Service Groups 3-70
Disable a Multicast Service 3-70
Disable an SSM Multicast Service Group 3-70
Enable a Multicast Service 3-71
Enable an SSM Multicast Service Group 3-71
Setting Alarms on Multicast Services and SSM Multicast Service Groups 3-71
Replaying Historical Services 3-72
Related Forms 3-72
Root Cause Dialog Box 3-72
Details of a Multicast Service 3-72
Details of a SSM Multicast Service Group 3-73
Details of SSM Multicast Service Group Branches Dialog Box. 3-74

CHAPTER 4 **Monitoring Changes in Routing** 4-1
Tracking Changes, Investigating Events 4-1
View of Real-time Events 4-1
Event Log Capabilities 4-1
Starting the Event Log 4-2
Start the Event Log 4-2
Viewing Events 4-3
Changes that Generate Events 4-3
Enterprise Events 4-4
How Events Are Displayed in the Event Log 4-5
Displaying OSPF Events 4-5
Displaying BGP Events 4-7
Working with Events 4-11
View Enterprise Events 4-12
View BGP Events 4-12
View OSPF Events 4-12
Scroll through Events 4-13
Browse Backward through Events 4-13
Browse Forward through Events 4-13
Refresh the Event Log 4-14
View the Beginning of the Event Log 4-14
Change the Number of Events Displayed 4-14
Finding Events 4-15

Find Events by ID 4-15
Find Events that Occurred in a Selected Timeframe 4-15
Filtering OSPF Events 4-16
Starting the Filter Wizard 4-16
Choosing a Predefined Filter 4-18
Customizing Filters 4-19
Changing the Filter Name 4-19
Saving the Filter 4-20
OSPF Filtering Example 4-20
Filtering BGP Events 4-20
Select BGP Events to Filter 4-21
BGP Filtering Example 1: IPv4 Unicast Events 4-21
BGP Filtering Example 2: IPV4 VPN Events 4-28
Working with Filters 4-36
Apply a Filter 4-36
Edit a Filter 4-37
Remove a Filter 4-37
Related Forms 4-38
Event Log Toolbar 4-38

CHAPTER 5 **Monitoring Network Activity** 5-1
Viewing Network Activity and Projecting Trends 5-1
View Most Active Routers 5-1
Use Event Monitor with Event Log 5-1
Viewing OSPF Convergence Activity 5-2
Start the Event Monitor 5-2
Viewing Network Activity 5-2
Set Data Normalization 5-3
Exponential Smoothing of Data 5-8
Event Monitor Toolbar 5-11
Graph Network Activity 5-12
View the Most Active Routers in a Domain 5-13
The OSPF Convergence Log 5-14

CHAPTER 6 **BGP Tagging** 6-1
Creating BGP Tags 6-1
Tagging Basics 6-1
Sample Tag Formats 6-3

Working with BGP Tags 6-9
Importing BGP Tags 6-10
Viewing BGP Tags 6-12
Exporting BGP Tags 6-14
Deleting BGP Tags 6-14
Purging BGP Tags from the Path Analyzer Database 6-15

CHAPTER 7 **MP-BGP Instrumentation** 7-1
Multiprotocol BGP Extensions (MP-BGP) 7-1
MP-BGP Defined 7-1
Path Analyzer MP-BGP VPN Instrumentation 7-1
Creating VRF XML Files 7-4
Sample VRF XML File 7-4
Explanation of Sample File 7-5

CHAPTER 8 **Setting and Monitoring Alarms** 8-1
Setting and Receiving Notifications of Real-time Changes 8-1
Changes that Trigger Alarms 8-1
Persist Alarms 8-1
View Real-time Alarms 8-2
Alarm Triggers in the Trigger Log 8-2
Export Alarm Triggers Your NMS 8-2
Alarm Configuration Wizards 8-2
View the Root Cause of Service Path Alarms 8-2
Starting Alarm Monitor 8-3
Start Alarm Monitor 8-3
Configuring Alarms 8-4
Configure a BGP Alarm 8-4
Configure an OSPF Alarm 8-19
Configure a Service Alarm 8-42
Set the Alarm Export Options 8-54
Viewing and Managing Alarms 8-55
Differences Between SNMP Polls and Path Analyzer Alarms 8-57
Supported Alarms 8-57
Wildcard alarms: Alarms on All Changes to All Selected Entities 8-61
Severity Values of Alarms 8-61
Indicators of Triggered Alarms 8-61
Time Window for Alarm Triggering 8-63
Clear All Alarm Triggers 8-63

Globally Enable or Disable All Alarms 8-64
Disable a Selected Alarm 8-65
Enable a Selected Alarm 8-65
Remove an Alarm 8-66
Start the Trigger Log 8-66
Working in the Trigger Log 8-68
Browse through the Trigger Log 8-68
Refresh the List of Alarm Triggers 8-69
Change the Number of Triggers Displayed in Trigger Log 8-70
Related Forms 8-71
Alarm Monitor 8-72
Alarm Monitor Toolbar 8-73
BGP Alarm Configuration Wizard 8-74
BGP Alarm Configuration, Advertisement Alarms 8-75
BGP Alarm Configuration, Threshold per Router Alarms 8-77
BGP Alarm Configuration, Route Alarms 8-78
BGP Alarm Configuration, Threshold per AS Alarms 8-79
BGP Alarm Configuration, Next Hop 8-80
OSPF Alarm Configuration Wizard 8-81
OSPF Alarm Configuration, Interface Alarms 8-82
OSPF Alarm Configuration, Router Alarms 8-84
OSPF Alarm Configuration, Transit Network Alarms 8-85
OSPF Alarm Configuration, Advertisement Alarms 8-87
OSPF Alarm Configuration, Route Alarms 8-88
OSPF Alarm Configuration, Threshold Alarms 8-90
OSPF Alarm Configuration, Error Alarms 8-91
Service Alarm Configuration Wizard 8-92
Unicast Service Alarm Configuration, Service Alarms 8-92
Unicast Service Alarm Configuration, Service Path Alarms 8-93
Multicast Service Alarm Configuration, Service Alarms 8-94
Multicast Service Alarm Configuration, SSM Multicast Group Alarms 8-95
Last 10 Triggers Dialog Box 8-95
Trigger Log 8-96

CHAPTER 9 **Generating Reports** 9-1

Generating Reports Showing Network Changes and Trends over Time 9-1
Reports and Charts 9-1
Customized Reports 9-1
Report Manager Tasks 9-2

Starting Report Manager 9-2
Start Report Manager 9-2
Creating Reports 9-2
Start the Report Wizard 9-2
Select a Report 9-2
Select an Autonomous System 9-3
Select Time Period 9-5
Managing Reports 9-6
View a Report 9-7
Cancel a Report 9-7
Delete a Report 9-8
Print a Report 9-8
Save a Report 9-8
Load a Report 9-9
Managing Charts from Report Manager 9-9
Derive a Chart 9-10
View a Chart 9-10
Cancel a Chart 9-11
Delete a Chart 9-12
Scheduling a Report 9-12
Pick Up Reports 9-15
Types of Reports 9-15
Enterprise Routing Stability 9-15
Service Stability 9-17
Enterprise Route Availability 9-19
Network Activity Hotspot Analysis 9-21
OSPF (Non-External) Advertisement Hotspot Analysis 9-22
BGP/External Advertisement Hotspot Analysis 9-24
Transit/Stub Route Redundancy Analysis 9-25
External Route Redundancy Analysis 9-27
OSPF (Non-External) Route Reachability Analysis 9-28
BGP/External Route Reachability Analysis 9-29
Related Forms 9-31
Report Manager Toolbar 9-31
Chart Toolbar 9-32
Chart Detail Window 9-33

CHAPTER 10 **Generating Charts** 10-1
Using Charts to Investigate Network Changes 10-1

Chart Manager Tasks 10-1
Chart Manager Details 10-1
Starting Chart Manager 10-1
Start Chart Manager 10-2
Determining the Type of Chart to Generate 10-2
Select a Basic or Advanced Chart 10-3
Select the Type of Chart to Generate 10-3
Select the Mode of the Chart 10-4
Generating a Basic Chart 10-6
Start the Wizard 10-6
Select the Chart 10-6
Select an Autonomous System and Domain 10-7
Select the Period of Time 10-8
Select the Mode 10-10
Cancel a Chart During Processing 10-11
Generating an Advanced Chart 10-11
Start the Wizard 10-11
View Charts 10-12
Select Data Set 10-12
Select Entities 10-14
Select an Autonomous System and Domain 10-15
Select Entity Types 10-16
Select the Time Period 10-17
Select the Name, Mode, and Type of Chart 10-18
Select the Time Divisions of a Trending Chart 10-20
Select the Aggregators and Entities of a Classification Chart 10-21
Preview the Chart 10-22
Generating a Derived Chart 10-23
Start the Wizard 10-23
Viewing Generated Charts 10-24
Chart Detail 10-24
Chart Tab 10-25
View a Chart 10-25
Raw Data Tab 10-26
Properties Tab 10-26
Managing Charts 10-27
Delete a Chart 10-27
Print a Chart 10-27
Save a Chart 10-28

Load a Chart 10-28
Scheduling a Chart 10-29
Picking up a Chart 10-29
Descriptions of Charts 10-29
Enterprise Charts 10-29
Topology Charts 10-30
Routing Update Charts 10-34
Service Charts 10-41
Descriptions of Advanced Charting Charts 10-44
Chart Types Associated with Data Sets 10-45
Select Entities 10-46
Related Forms 10-48
Chart Manager Toolbar 10-48
Chart Wizard Pages for Advanced Charting 10-50
Choose Entities for Routers 10-53
Entity Types to be Included for Routers 10-54
Choose Entities for Transit Network 10-54
Entity Types to be Included for Transit Networks 10-55
Choose Entities for Stub Routes 10-55
Entity Types to be Included for Stub Routes 10-56
Choose Entities for Unnumbered Point-to-Point Interfaces 10-56
Entity Types to be Included for Unnumbered Point-to-Point Interfaces 10-57
Choose Entities for Numbered Point-to-Point Interfaces 10-58
Entity Types to Be Included for Numbered Point-to-Point Interfaces 10-58
Choose Entities for Transit Interface 10-59
Entity Types to be Included for Transit Interface 10-60
Choose Entities for Transit and Stub Route 10-60
Entity Types to be Included for Transit and Stub Route 10-60
Choose Entities for External Route 10-61
Entity Types to be Included for External Route 10-61
Choose Entities for BGP Route 10-62
Entity Types to be Included for BGP Route 10-62
Choose Entities for T3 Summary 10-63
Entity Types to be Included for T3 Summary 10-63
Choose Entities for T4 Summary 10-64
Entity Types to be Included for T4 Summary 10-65
Choose Entities for External Advertisement 10-65
Entity Types to be Included for External Advertisement 10-66
Choose Entities for BGP Route Advertisement 10-66

Entity Types to be Included for BGP Route Advertisement 10-67
Choose Entities for Service 10-68
Entity Types to be Included for Service 10-68
Choose Entities for Service Path 10-68
Entity Types to be Included for Service Path 10-69

CHAPTER 11 **Scheduling Reports and Charts** 11-1
Managing Scheduled Tasks with Path Analyzer Schedule Manager 11-1
Schedule Manager Tasks 11-1
Schedule Manager Details 11-1
Starting Schedule Manager 11-2
Start Schedule Manager 11-2
Scheduling Reports 11-2
Schedule One-Time Reports 11-2
Schedule Recurring Reports 11-7
Scheduling Charts 11-9
Schedule One-Time Charts 11-9
Schedule Recurring Charts 11-14
Scheduling Advanced Charts 11-17
Schedule One-Time Advanced Charts 11-17
Start the Schedule Advanced Chart Wizard 11-17
Schedule Recurring Advanced Charts 11-27
Managing Scheduled Reports, Charts, and Advanced Charts 11-32
Schedule Manager 11-32
Related Forms 11-42
Schedule Manager Toolbar 11-42
Schedules 11-44
Completed Tasks 11-45

CHAPTER 12 **Web-Based Report Management** 12-1
Accessing Generated Charts and Reports from the Web 12-1
Web Schedule Manager Details 12-1
Starting the Path Analyzer Web Schedule Manager 12-1
Start the Web Schedule Manager 12-2
Log In 12-3
Navigating in the Web Schedule Manager 12-4
Viewing Current Schedules and Completed Tasks 12-5
View Scheduling Information of All Users 12-5

Refresh Page Values 12-6
Managing Schedules 12-7
View Schedules 12-7
Search for Schedules 12-9
Reset Search Fields 12-11
Delete Schedules 12-12
Managing Completed Tasks 12-13
View Generated Charts or Reports in the Completed Tasks Screen 12-13
Search for Completed Tasks 12-15
Reset Task Search Fields 12-17
Delete Completed Tasks 12-18
Manage Your Own Schedule and Tasks 12-19
View Your Tasks 12-19
Search for Your Schedules 12-20
Search for Your Tasks 12-20
Reset Search Values 12-21
Delete Your Schedules and Tasks 12-21

CHAPTER 13 **Replaying Your Network's History** 13-1
Watching Historical Events Replay 13-1
Uses for Replaying Events 13-1
Full Use of Path Analyzer Modules 13-1
Viewing Past Events: Like Watching a Movie 13-2
Like Using a Media Player 13-2
Historical Session Tasks 13-2
Starting a Historical Session 13-3
Start a Historical Session 13-3
Select an Autonomous System 13-3
Select a Period of Time 13-4
Select Services to View Historically 13-6
Using Controls of Historical Sessions 13-7
Set the Delay Between Routing Update Messages 13-8
Navigating Between Historical Sessions and the Realtime Console 13-8
Using the Context Switcher to Switch Sessions 13-8
Select a Module Window 13-10
Analyzing Previous Network Conditions 13-11
Start a Module in a Historical Session 13-11
Review the Historical Topology 13-12
Find Information about Historical Service Paths 13-13

Review Previous Events 13-14
View Historical Configurations and Domain Naming Assignments 13-15

Preface

After installing, connecting, and configuring Cisco Service Path Analyzer appliances and software, you can use Cisco Service Path Analyzer (hereafter referred to as Path Analyzer) to monitor, identify, and resolve routing issues that occur in instrumented routing domains of your network. The *Cisco Service Path Analyzer User Guide* describes and explains how to use all the features of the Cisco Service Path Analyzer.

For information about initially installing and connecting your Path Analyzer appliances, see the *Cisco Service Path Analyzer Appliance Installation Guide* under Related Documentation, page xxi.

For information about configuring your Path Analyzer system, managing user accounts, reconfiguring your Listeners and Collectors, and removing components, see the *Cisco Service Path Analyzer System Administration Guide* under Related Documentation, page xxi.

Overview

Path Analyzer enhances your current network management solution by adding the ability to identify, diagnose, and quickly resolve routing faults, increasing the reliability and performance of your network.

Popular network management solutions model the physical infrastructure of a network for incidental events and faults, such as a disconnected cable or damaged power supply. Path Analyzer delivers a new level of proactive maintenance by monitoring the IP level of the network for routing events and faults.

Audience

Network administrators and operators who manage, maintain, and troubleshoot large, distributed, geographically dispersed networks can use the *Cisco Service Path Analyzer User Guide* to find information about the following topics:

- Initial configuration
- Viewing events
- Viewing your network topology
- Viewing and finding paths between source and destination nodes
- Generating real-time and historical data about the state of your network
- Administering new versions of software and maintaining versions

Organization

This guide is organized into the following chapters:

Chapter Number	Chapter Title	Description
Chapter 1	Getting Started	Path Analyzer network management and the Management Console environment.
Chapter 2	Monitoring Your Network's Topology	Using the Topology Viewer for proactive fault management.
Chapter 3	Monitoring Unicast and Multicast Services	Creating and monitoring services—collections of business-critical data from essential applications and resources.
Chapter 4	Monitoring Changes in Routing	Viewing, finding, and filtering BGP and OSPF events in the Event Log; querying for specific events in the Investigative Event Log.
Chapter 5	Monitoring Network Activity	Using the Event Monitor to track routing activity on your network.
Chapter 6	BGP Tagging	Tagging BGP events for identification within the Event Log. Chapter includes reasons for tagging, methods for importing and exporting tags via XML, tag deletion and purging.
Chapter 7	MP-BGP Instrumentation	Explains Path Analyzer MP-BGP VPN instrumentation. Includes instructions for creating and using VRF XML files.
Chapter 8	Setting and Monitoring Alarms	Using Alarm Monitor to set alarm notifications to identify the events that cause changes to paths, routers, transit interfaces, and other network entities.
Chapter 9	Generating Reports	Generating reports: collections of charts that show trends and top performers in your network.
Chapter 10	Generating Charts	Using Path Analyzer charting features to develop customized or pre-defined charts and tables that depict trends in network conditions over time and top performers on your network.

Chapter Number	Chapter Title	Description
Chapter 11	Scheduling Reports and Charts	Using the Schedule Manager to schedule chart or report generation and printing.
Chapter 12	Web-Based Report Management	Using the Web Schedule Manager to view and manage schedules and tasks related to charts and reports from a Web browser.
Chapter 13	Replaying Your Network's History	Running a historical sequence of events as a Historical Session; reviewing earlier network conditions in the Topology Viewer, Service Monitor, and Event Monitor.
Glossary	Glossary	Glossary of terms used within the Cisco Service Path Analyzer User Guide.

Chapter-Level Organization

Each chapter is structured to provide you with the information you need to complete network management tasks using Path Analyzer.

- **Background and conceptual information**—Background information about the tasks you need to complete and the purpose of these tasks.
- **Procedures**—Step-by-step procedures for completing each task.

Related Documentation

The *Cisco Service Path Analyzer User Guide* is accompanied by the following documentation:

- *Cisco Service Path Analyzer Installation Guide*—Provides information about the following topics:
  - Prerequisites for installation
  - Loading Cisco Service Path Analyzer software.
  - Initial system configuration tasks.
  - Database backup and restore
- *Cisco Service Path Analyzer System Administration Guide*—Provides detailed information about the following topics:
  - Initial configuration of your Path Analyzer system, including the following configuration tasks:
  - Assigning the Path Analyzer Server IP address, subnet mask, gateway, and other related information using the Server Configuration Tool.
  - Installing the Path Analyzer Management Console.
  - Configuring Listeners and Collectors.
  - Assigning an IP address and subnet mask to each Listener.
  - Administering and maintaining your Path Analyzer system:

  - Adding, removing, and changing Listeners and Collectors.
  - Adding, removing, and modifying user accounts.
  - Upgrading, registering, and licensing your Path Analyzer software.
  - Exporting the Path Analyzer database and system logs.
  - Restarting your Path Analyzer Server.
- Setting up user accounts or multi-user access to the Management Console.
- Configuring names for autonomous systems and routing domains, adding static routes, and setting up forwarding resolution.

- *Cisco Service Path Analyzer Alarm Reference*—Explains the syntax and significance of alarms in the Alarm Monitor.
- *Cisco Application Deployment Engine 1010 and 2120 Appliance Hardware Installation Guide*—Provides information about the following topics:
  - Product overview
  - Installation preparation
  - Installation instructions
  - Cable specifications
  - Site log
- *Cisco Application Deployment Engine 2130 and 2140 Appliance Hardware Installation Guide*—Provides information about the following topics:
  - Product overview
  - Installation preparation
  - Installation instructions
  - Cable specifications
  - Site log
- *Release Notes for Cisco Service Path Analyzer 1.0*—Provide information about the following topics:
  - Compatible hardware and software platforms.
  - System requirements.
  - Known and fixed software and documentation issues.

Additional Technical References

The Path Analyzer supports networks that run the Open Shortest Path First (OSPF) protocol version 2 and Border Gateway Protocol (BGP) version 4.

OSPF Technical Information

For detailed information about the OSPF protocol, see the following Internet Engineering Task Force (IETF) documents:

- RFC 1584—Describes Type 6, Multicast, Link State Advertisements (LSAs). See http://www.ietf.org/rfc/rfc1584.txt
- RFC 1587—Describes Type 7 LSAs. See http://www.ietf.org/rfc/rfc1587.txt
- RFC 1850—Defines attributes of the OSPF Management Information Base (MIB). See http://www.ietf.org/rfc/rfc1850.txt
- RFC 2328—Defines Type 1 through 5 LSAs in the most recent RFC for OSPF version 2. See http://www.ietf.org/rfc/rfc2328.txt
- RFC 2740—Describes features and attributes of OSPF for Internet Protocol (IP) version 6. See http://www.ietf.org/rfc/rfc2740.txt
- RFC 1774, *BGP-4 Protocol Analysis*—Provides further information about how BGP satisfies IETF protocol requirements, including key features and algorithms, scalability and performance, link bandwidth and CPU utilization, memory requirements, and security considerations. See http://www.ietf.org/rfc/rfc1774.txt

BGP Technical Information

For detailed information about BGP, see the following IETF documents:

- RFC 4271, A Border Gateway Protocol 4—Provides a comprehensive review of the draft standard protocol. Download a text version at: ftp.rfc-editor.org/in-notes/rfc4271.txt
- RFC 3345, *Border Gateway Protocol (BGP) Persistent Route Oscillation Condition*—discusses the two types of persistent route oscillation, when these conditions occur, and provides network design guidelines to avoid introducing these occurrences. See http://www.ietf.org/rfc/rfc3345.txt
- RFC 1771, *A Border Gateway Protocol*—Describes the initial version of the BGP. See http://www.ietf.org/rfc/rfc1771.txt
- RFC 1772, *Application of the Border Gateway Protocol in the Internet*—Describes how to apply BGP in a network comprised of multiple autonomous systems, such as the Internet. See http://www.ietf.org/rfc/rfc1772.txt
- RFC 1773, *Experience with the BGP-4 Protocol*—Provides further information about how BGP satisfies IETF protocol requirements, including operational experience, vendor implementations, and migration. See http://www.ietf.org/rfc/rfc1773.txt

Support for Alarm Trigger Exporting

The Path Analyzer supports Alarm Trigger Exporting to syslog hosts and Simple Network Management Protocol (SNMP) agents running SNMP v.1, v.2c, or v.3. For details, see Chapter 12, Alarm Trigger Exporting in the *Cisco Service Path Analyzer System Administration Guide*.

Syslog

For detailed information about the syslog protocol, see the syslog man pages and RFC 3164 from the IETF:

- syslog (3)
- syslog.conf (5)
- syslogd (8)

- RFC 3164—The BSD Syslog Protocol, which defines the protocol. See http://www.ietf.org/rfc/rfc3164.txt.

Simple Network Management Protocol (SNMP)

For detailed information about the SNMP, see Stallings, William. *SNMP, SNMPv2, and SNMPv3, and RMON 1 and 2, 3rd ed.* Boston: Addison-Wesley. 1999. ISBN: 0-201-48534-6.

Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

© 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Getting Started

Getting Started with Path Analyzer

Cisco Service Path Analyzer (hereafter referred to as Path Analyzer) is the industry's first multi-user, multi-domain solution for automated fault, root-cause, and service management across autonomous systems and routing domains of enterprise-wide Internet Protocol (IP) networks.

Enterprise networks are divided into individual administrative domains, referred to as *autonomous systems*. Within an autonomous system, routers use guidelines provided by Interior Gateway Protocols (IGP's) to forward data from router to router (hop to hop) toward a destination. Common IGP's include:

- Router Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Intermediate System-Intermediate System (IS-IS)
- Interior Border Gateway Protocol (iBGP)

Autonomous systems may be further partitioned into routing domains, which may contain more lower-level domains. For example, an autonomous system may be divided into one or more BGP domains and two or more OSPF domains, called *areas*.

For information about how Path Analyzer presents the hierarchy of your network in modules of the Management Console, see Structure of Your Network in Cisco Service Path Analyzer on page 2-1.

Monitor Routing Activities Within Domains

Path Analyzer components, called Listeners, aggregate messages exchanged between routers over OSPF and iBGP protocols. These messages enable routers to set up an adjacency, an initial line of communication, over which they exchange updates to the routes recorded in their routing tables. Updates enable the routers to forward data over the shortest or lowest cost path toward the intended destination.

OSPF Listeners collect the Link State Advertisements (LSAs), which are routing messages and route updates that OSPF routers exchange in and between logical subdivisions, or areas, of an autonomous system. OSPF routers also receive summarized descriptions of changes in other areas and external autonomous systems.

Monitor Routing Activities Between Domains

Between autonomous systems, routers pass data over Exterior Gateway Protocols (EGP's), of which the most commonly used protocol is the Exterior Border Gateway Protocol (eBGP). In an OSPF/BGP configuration of Path Analyzer, BGP Listeners collect and process BGP update messages, which include routing updates between autonomous systems.

View Routing Data in the Path Analyzer Management Console

Listeners collect messages in real time from adjacent routers and send the accumulated information to the Path Analyzer Server.

The Path Analyzer Server handles collected data as managed objects in its database, then sends a visual display of the information to the Path Analyzer Management Console. You can run the Management Console in real time to view the current state of your network. You can also replay a previous network state.

For information about starting the Path Analyzer Management Console in real time, see Starting Path Analyzer on page 1-3. For information about starting the Management Console in an historical state, see Replaying Your Network's History on page 13-1.

For information about basic navigation in the Management Console, see Navigating in the Path Analyzer Management Console, page 1-17.

Simultaneous, Multi-User Monitoring and Administration

Path Analyzer allows multiple network administrators and operators to log in and monitor the network simultaneously. You decide how to delegate work among your staff. Tasks include:

- Monitoring your network using the visual topology and event descriptions.
- Setting and receiving notifications of changes in your network.
- Creating and monitoring important, business-critical services.

From modules in the Management Console, you and your team can:

- Use the Topology Viewer and Topology Browser to view information about your network's routing topology and changes in routing paths.
- Create visual displays of your important, business-critical services—including applications, departments, and data flow
  - Use Service Monitor to track service-related data as it travels from a source to a destination endpoint through your network.
- Use the Investigative Topology Browser Query to search for specific OSPF or BGP route advertisements and OSPF interfaces.
- View, filter, and query from the complete set of events that occurs on your network.
  - Events are visual notifications of changes in the network, such as the advertisement, withdrawal, or change to a router, interface, or route. In Path Analyzer, all events are displayed in the Event Log.
- Use BGP Route Tagging to identify significant events in the Event Log.
- Use the Alarm Monitor to set alarms against potential routing changes. View, query

- Use the Alarm Log to identify the root cause of service and service path alarms.
- Use Chart Manager, Report Manager, and Schedule Manager to:
  - Generate data charts showing trends and top performers.
  - Create detailed reports.
  - Schedule charts and reports to run once or periodically.
  - Access and edit charts and reports from outside of Path Analyzer using Web-Based Reporting.

Complete Set of System Administration Tools

Use Path Analyzer User Administration features to configure administrator accounts, providing your team with privileges across the entire system. Or, you can configure power users with read-only access to applications.

Allow your accounting and product marketing teams access to the charting and reporting features of Path Analyzer, enabling them to assess routing trends and to plan for future requirements.

Path Analyzer system administration features also enable system configuration and maintenance, upgrading and reconfiguring, and troubleshooting. For more information about system administration, see the *Cisco Service Path Analyzer System Administration Guide*.

Management Console Tasks

- Starting Path Analyzer on page 1-3
- Monitoring Your Network's Topology
- Monitoring Unicast and Multicast Services on page 3-1
- Monitoring Changes in Routing on page 4-1
- Monitoring Network Activity on page 5-1
- BGP Tagging on page 6-1
- MP-BGP Instrumentation on page 7-1
- Setting and Monitoring Alarms on page 8-1
- Generating Reports on page 9-1
- Generating Charts on page 10-1
- Scheduling Reports and Charts on page 11-1
- Web-Based Report Management on page 12-1
- Replaying Your Network's History on page 13-1

Starting Path Analyzer

The following sections explain how to start and log into Path Analyzer in the following operating environments:

- Microsoft Windows
- A supported Unix-based Operating System

Start Path Analyzer in Microsoft Windows

Double-click the Path Analyzer icon on your Microsoft Windows desktop, if you installed it there.

or

Click **Start > Path Analyzer** if you installed it in the Start menu.

or

Click **Start > All Programs > Path Analyzer > Path Analyzer** if you installed it in the All Programs group.

The Path Analyzer Management Console appears.

Start Path Analyzer in a Supported Unix-Based Operating System

To start Path Analyzer in a supported Unix-based Operating System:

Step 1 Open an XTerminal window.

Step 2 Locate the directory in which you installed Path Analyzer.

Step 3 Enter the following command:

```
./Cisco_SPA
```

The Path Analyzer splash screen and Login box are displayed.

Log in to Path Analyzer

To log in to Path Analyzer:

Step 1 Click **File > Login** in the menu bar.

The Login dialog box appears.

Step 2 Enter the Path Analyzer user name and password, as provided by your system administrator, in the Username and Password fields. The Path Analyzer Server IP address and port number are provided by default.

Note Your user name and password are case sensitive.

The login will not work correctly if there are any spaces after any of the field inputs.

Step 3 Click **Login**.

A series of messages are displayed indicating that authentication processes are completed and required connections are made.

The Start button on the Path Analyzer taskbar appears in white to indicate that the Management Console is actively prepared to receive and respond to your actions.

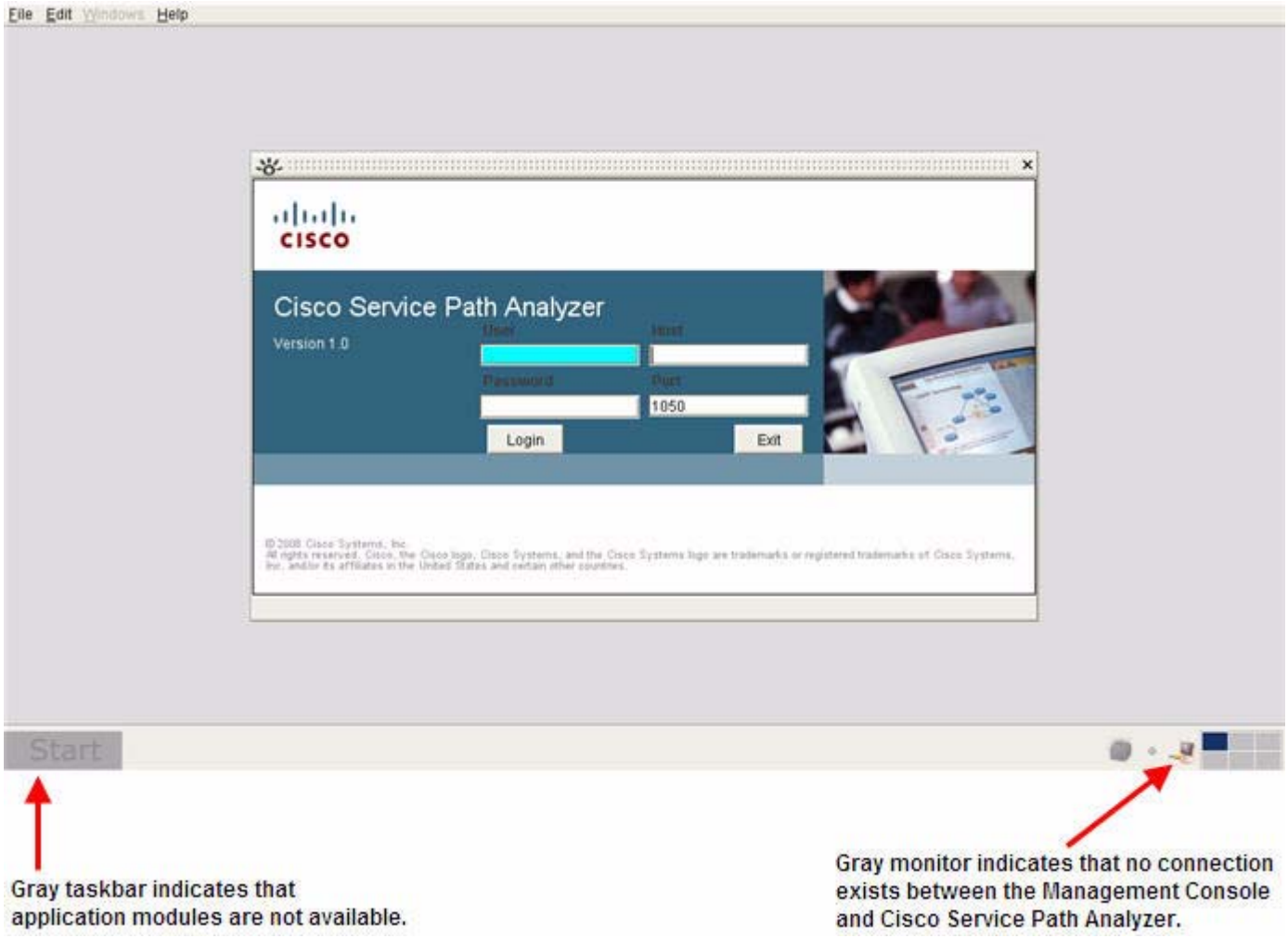
See Figure 1-2 for an image of the active taskbar.

See Features of the Management Console, page 1-7 for information about starting and using Management Console modules.

Verify Your Connection

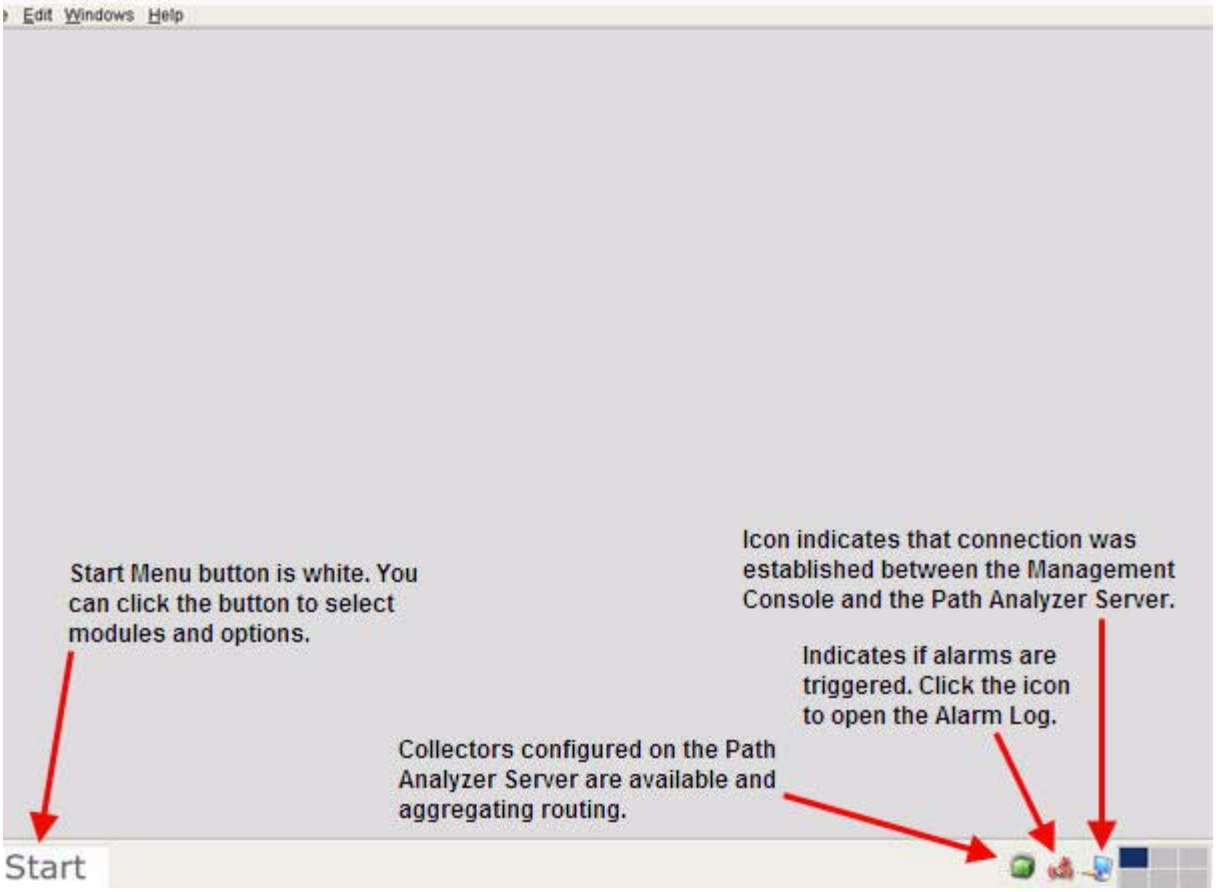
Logging in to the Path Analyzer Management Console (**File > Login**) establishes a connection between the Management Console and the Path Analyzer Server. Before login, the Management Console displays a gray taskbar in Figure 1-1.

Figure 1-1 Path Analyzer Management Console Before Login



As shown in Figure 1-2, after logging in, the Management Console button turns white and the other icons appear in color.

Figure 1-2 Path Analyzer Management Console After Login



Additional Taskbar Indicators

In addition to the Start button changing from gray to white, the taskbar shows icons that indicate the status of other Path Analyzer components.

Collector Status Indicators

Cube-shaped indicators change color from green to red to indicate the status of Collectors configured on your Listener. The indicator is green when all Collectors are available and aggregating routing data. The indicator changes to red if a collector becomes unavailable, as shown in Figure 1-3.

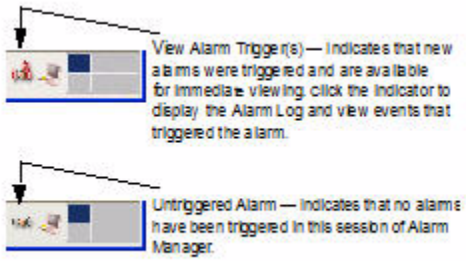
Figure 1-3 Collector Status Indicators

For information about configuring Collectors, see Chapter 6, Configuring Listeners and Collectors, in the *Cisco Service Path Analyzer System Administration Guide*.

Alarm Indicators

Alarm indicators show the status of alarms you set during your previous Path Analyzer session, as shown in Figure 1-4.

Figure 1-4 Alarm Indicators



For information about setting Path Analyzer alarms, see Setting and Monitoring Alarms on page 8-1.

Session Indicators

Path Analyzer supports one real-time session and up to five historical sessions at the same time. The taskbar provides session indicators to track current sessions. For information, see Change between Real-time and Historical Sessions, page 1-21.

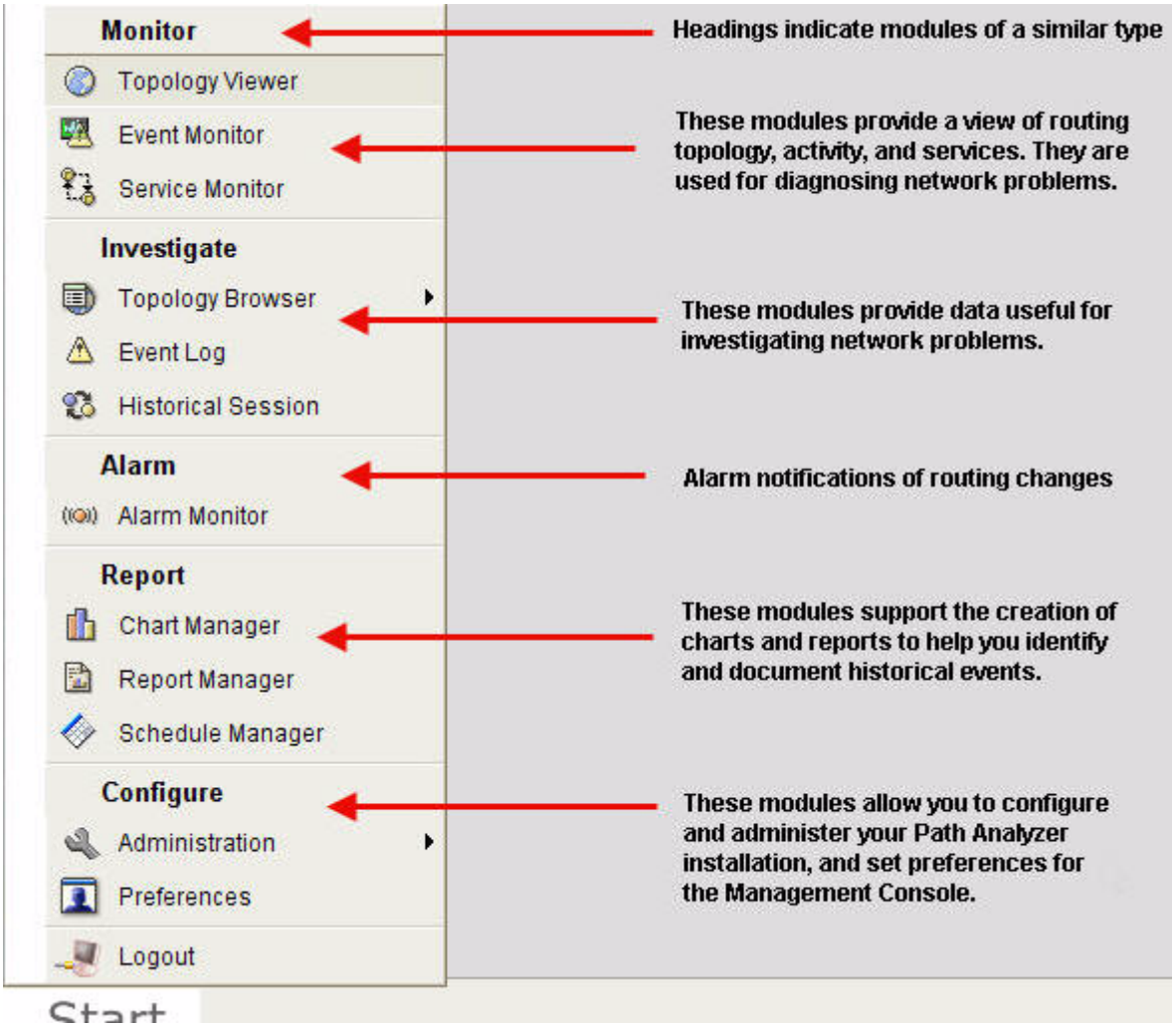
Features of the Management Console

The lower-left corner of the Path Analyzer Management Console contains the taskbar. Clicking the Start button opens a list of applications or modules on the Management Console. Path Analyzer modules provide a range of functions that enable you to monitor network routing activity.

Path Analyzer Taskbar

All Path Analyzer modules or applications, including the Topology Viewer, are located in the taskbar in the lower left corner of the Management Console, as shown in Figure 1-5.

Figure 1-5 Path Analyzer Modules in Taskbar



Select a Module

To select a module:

Step 1 Click **Start** at the bottom left corner of the Management Console.

Step 2 Choose one of the following modules from its category:

Table 1-1 Module Selections of the Taskbar

Category	Module	Description
Monitor	—	Provides options for viewing and monitoring your network topology, activity, and business-critical services.
	Topology Viewer	A topological view of your network. See Monitoring Your Network's Topology on page 2-1.
	Event Monitor	Routing statistics for activity that occurs on your network.
	Service Monitor	Create and monitor services; provides visual representations of the elements in your network. See Monitoring Unicast and Multicast Services on page 3-1.
Investigate	—	Investigate the routing issues in your network and identify critical changes and the root cause of problems.
	Topology Browser	The Real-time Topology Browser supplements the topology shown in the Topology Viewer with information about every entity in your network. See Getting Detailed Information About Topology Viewer Elements, page 2-45 and Navigating in Topology Browser Dialog Boxes, page 2-48. In Investigative Mode, you can query and search for specific BGP or OSPF route advertisements or OSPF interfaces. See Querying for Network Elements (for OSPF Entities), page 2-82.
	Event Log	A continuously updated list of network events. See Monitoring Changes in Routing on page 4-1 for information.
	Historical Session	Configure a historical view of the changes that have occurred in your network, which allows you to replay your network's history. See Replaying Your Network's History on page 13-1.
Alarm	Alarm Monitor	A scrollable list of alarms. Allows you to set a wide variety of alarms on network entities and services. See Setting and Monitoring Alarms on page 8-1.

Table 1-1 Module Selections of the Taskbar (continued)

Category	Module	Description
Report	—	Format reporting data on network conditions.
	Chart Manager	Create bar charts, pie charts, and tables of formatted data to identify trends in OSPF and BGP routing, or to identify network entities most affected by routing changes See Generating Charts on page 10-1.
	Report Manager	Generate predefined reports that provide a high-level view of data from multiple charts. See Generating Reports on page 9-1.
	Schedule Manager	Schedule chart or report generation.

Table 1-1 Module Selections of the Taskbar (continued)

Category	Module	Description
Configure	—	Provides options that affect the configuration of your Path Analyzer system.
	Administration	Configure Listeners and Collectors (the virtual routers that passively collect routing information), monitor your Path Analyzer system, set up and administer user accounts, and set customized naming conventions for your enterprise network and the autonomous systems and routing domains that comprise it. For more information, see the *Cisco Service Path Analyzer System Administration Guide*.
	The Administration menu includes the following modules:	
	System	Provides options for: • Viewing Path Analyzer Server statistics. • Configuring your Path Analyzer Server and components. • Upgrading your system. • Setting performance features.
	Data Management	Provides options for exporting and purging your Path Analyzer database
	User	Provides options for configuring and managing user accounts
	Domain	Provides options for: • Naming your enterprise, autonomous systems, domains, and routers. • Adding and removing autonomous systems. • Configuring and managing static routes and next hop resolutions.
	Alarm Export	Provides options for exporting Path Analyzer alarm triggers to your network management system.
	Tagging	Import and export BGP tags from and to XML files. Mark tags for deletion and purge tags from the Path Analyzer database. See BGP Tagging on page 6-1.

Table 1-1 Module Selections of the Taskbar (continued)

Category	Module	Description
Preferences	—	Set preferences for Topology Viewer settings, router names, time formats and automatic start and completion settings. See Set Preferences, page 1-24.
Logout	—	This option is also available from the Path Analyzer menu bar, **File > Logout**. You can also exit Path Analyzer by selecting **File > Exit** in the menu bar.

A Real-time View of Your Network

By default, the Path Analyzer Management Console provides you with real-time views of your network in the Topology Viewer and other modules of the Path Analyzer taskbar.

For detailed information about network elements represented in the Topology Viewer and the visual color changes that indicate transformations in routing patterns, see Identifying Topology Viewer Elements, page 2-14.

Network Topology in the Topology Viewer

The Topology Viewer presents the real-time, hierarchical, Layer 3 routing topology that overlays your Layer 2 physical topology but remains hidden from your NMS. The Topology Viewer shows the structure of your network hierarchy, including the lowest-level components that guide data across your network. From the highest to lowest levels of your network, you can view the:

- Enterprise (comprising one or more autonomous systems).
- Lower-level routing domains that make up each autonomous system.
- Components of routing domains, including routers and subnets, and the links over which data passes between routers and networks.
- Router interfaces that forward packets over links to the next hop.

The Topology Browser also provides tables of data and statistics about the components in your network. Right-clicking a topology element, such as a router, reveals options for viewing information about its attributes, interfaces, and routes. Information available in the Topology Browser can assist you in determining the cause of changes in routing patterns on your network.

For information about the Graphical and Topology Browsers and querying for topology elements using Investigative Topology Browser, see Monitoring Your Network's Topology on page 2-1.

Figure 1-6 Topology Viewer

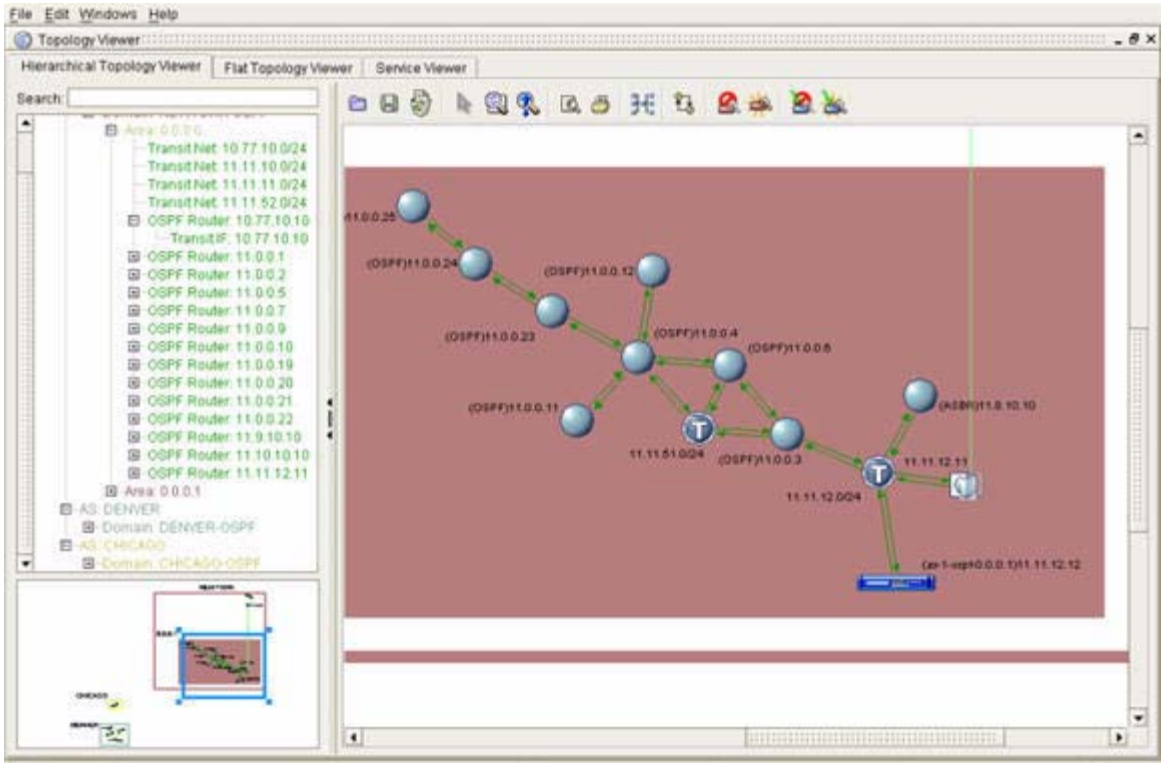


Figure 1-6 shows the Topology Viewer.

The Event Monitor provides a current view of network activity, compared to an average amount of activity. This allows you to identify periods of unexpected, unusual, or frequent routing changes in your network. Starting Event Monitor in the morning after running Path Analyzer overnight enables you to locate spikes in activity that occurred during the night. Running Event Monitor at intervals allows you to track periods of infrequent, unexpected activity over time.

Event Monitor presents normalized, raw realtime data related to your network, or the T-score of network activity as a measure of variance from the norm.You can also display data with exponential smoothing, placing greater emphasis on present or past activity.

For detailed information about using the Event Monitor to view network activity, see Monitoring Network Activity on page 5-1.

Figure 1-7 Network Activity Graph in the Event Monitor

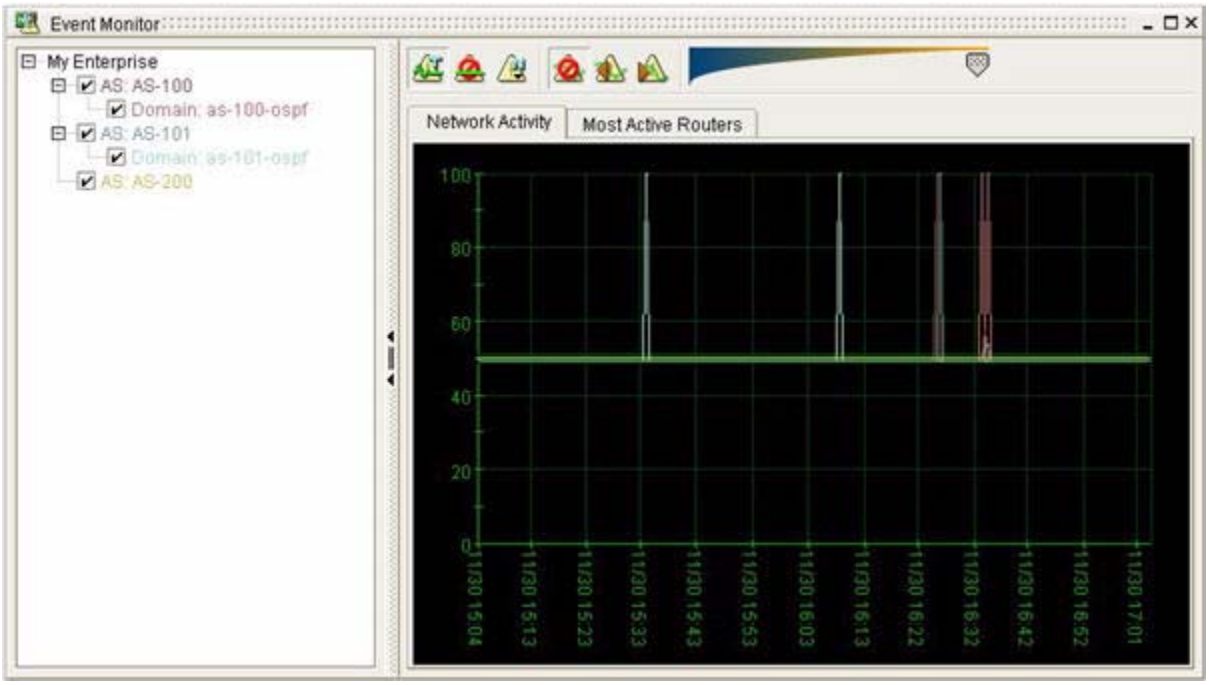


Figure 1-7 shows the Network Activity Graph in the Event Monitor.

Monitor Service Paths

Services are complete data flows related to applications and resources on your network. You can see a complete path as the data traverses the servers and departments that provide it to the people, places, and processes that use it.

From Service Monitor, you can:

- Create and track the progress of a service and its related paths as it traverses multiple OSPF and BGP routing domains in your network.
- Determine its availability and conformity to the baseline you set for it.
- Identify the root cause of issues that affect the ability of a service to traverse the network.

Figure 1-8 Graphical Service Path

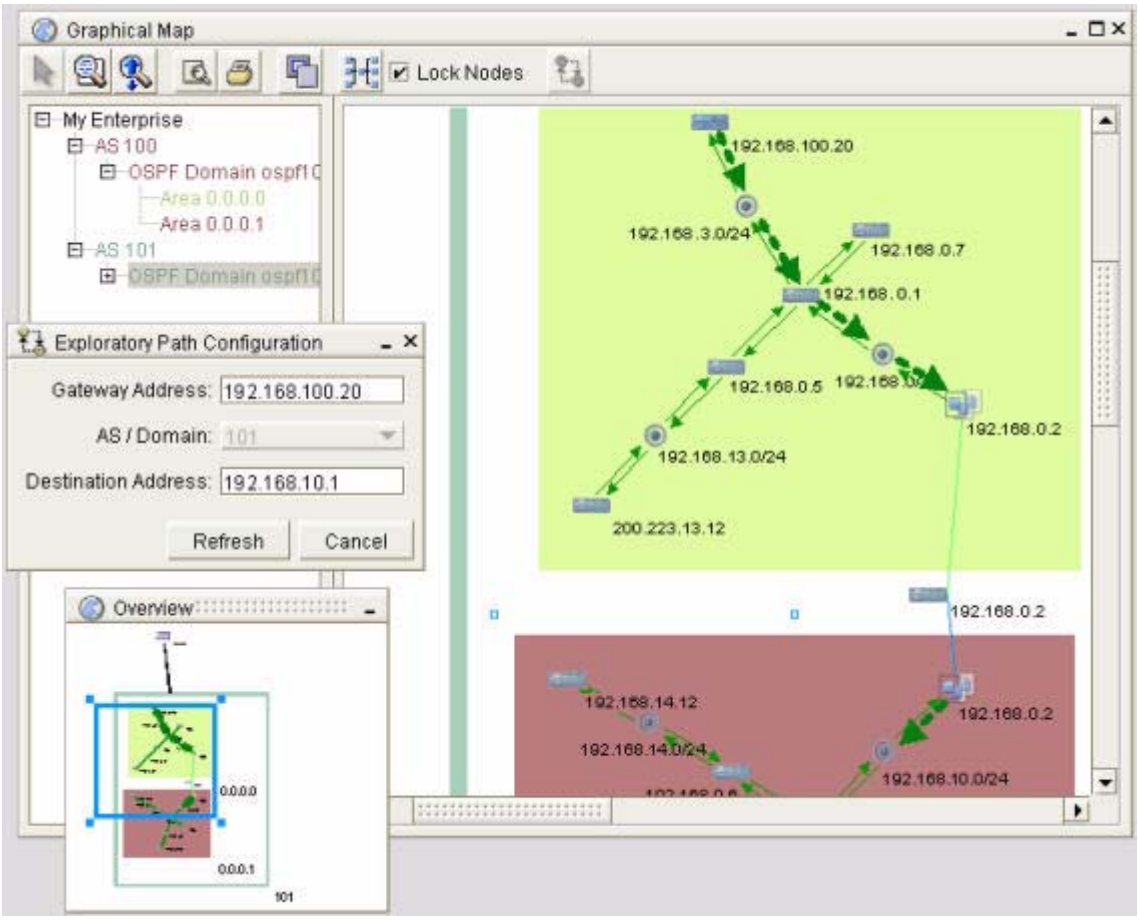


Figure 1-8 shows a Graphical Service Path in the Topology Viewer.

An awareness of the Layer 3 topology that overlies the physical view of the network, allows you to monitor and set alarms on the data flows and readily identify the root cause of routing faults.

For information about creating and monitoring services in your network, see Monitoring Unicast and Multicast Services on page 3-1.

Monitor Routing Changes in OSPF or BGP Event Logs

Path Analyzer Event Logs provide detailed lists of changes in routing patterns. Collectively, these routing changes are referred to as *events*. A familiarity with routing events help you determine the root cause of routing issues in your network.

After viewing the dates and times of network activity in Event Monitor, you can view the Event Logs for information about the specific, real-time or historical changes that have occurred in your network.

BGP and OSPF Event Logs

From the highest level of your network hierarchy, you can view the entire set of events that occur across your enterprise. Selecting an autonomous system in the Event Log lets you view all BGP events related to that system, derived from update messages obtained from the BGP speaker, which forms an adjacency with a Path Analyzer Listener.

Similarly, you can select an OSPF routing domain and view its related events, which are derived from the Link State Advertisements (LSAs) of routers from the OSPF domain, which form an adjacency with a Listener.

For information about viewing, filtering, and querying for OSPF and BGP routing events, see Monitoring Changes in Routing on page 4-1.

Events can indicate routing issues, such as misconfigurations, or spurious routes initiated by changes in the cost of a router interface. Network management systems, which identify physical network issues, cannot detect these routing changes.

Changes in routing occur quickly, often within milliseconds. The latency inherent in network management systems, which rely on polling and traps, can cause them to overlook routing changes. Without Path Analyzer, obtaining this information requires laborious research, using the results of `traceroute` and other commands.

Figure 1-9 Event Log Showing OSPF Events

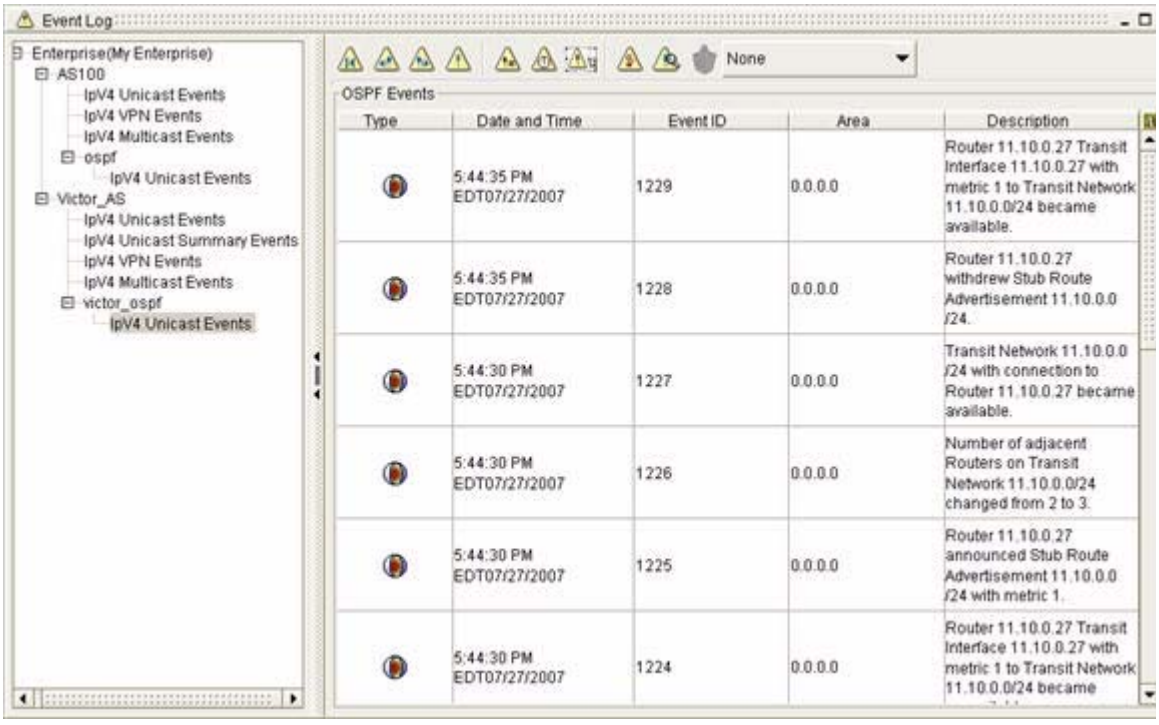


Figure 1-9 shows the OSPF Event Log.

Query for Specific Events

Running the OSPF or BGP Event Monitor in Investigative Mode allows you to query for specific events to determine the root cause of issues or trace the reasons for changes on your network. You can view, filter, and query the full set of enterprise events, or events that belong to a selected autonomous system or routing domain. For information about querying for OSPF events, see Monitoring Changes in Routing on page 4-1.

Set and Monitor Alarms and their Triggers

In network management systems (NMS's), alarms are automated notifications of a change or a selected series of changes that occurs in your network. Path Analyzer provides Alarm Monitor, which enables you to set alarms that trigger notifications when routing changes occur over Open Shortest Path First (OSPF) protocol or Border Gateway Protocol (BGP).

From the Alarm Monitor, you can set, view, and acknowledge OSPF, BGP, and Service alarms. You can also view and browse through alarm triggers, the changes in routing patterns that activate alarms. For detailed information, see Setting and Monitoring Alarms on page 8-1. For information about alarm triggers, see Changes that Trigger Alarms, page 8-1, and Working in the Trigger Log, page 8-68 for information about using the Alarm Log.

Create Reports and Charts

Path Analyzer reports encompass a collection of charts that describe network trends and top-performing network entities over a designated time period. You can generate and print reports to inform colleagues about trends in the status of your network, appliances that require upgrades, and scalability and performance requirements.

For information about creating reports, see Generating Reports on page 9-1.

For information about creating charts, see Generating Charts on page 10-1.

Replay and View Historical Events

The term *historical* means that you can view network conditions as they existed at a previous time. During a Historical Session, you can set the start and end dates of the time period you are interested in, which resets Management Console conditions. For information about replaying historical events, see Replaying Your Network's History on page 13-1.

Navigating in the Path Analyzer Management Console

Figure 1-10 shows the topology of a network in a Topology Viewer that has been resized to take up the full view of the Management Console.

In Figure 1-10, the green arrows indicate the segments of a monitored exploratory path, a flow of data that passes between two endpoints and traverses multiple OSPF routing domains.

Path Analyzer updates the Topology Viewer on a millisecond-to-millisecond basis with information it derives from the routers on your network. You can use the Flat Topology Viewer or Hierarchical Topology Viewer tabs within the Topology Viewer to observe the state of physical routers and subnets, entire routing domains, and changes to the logical paths of data across the network.

Figure 1-10 Exploratory Path in Topology Viewer

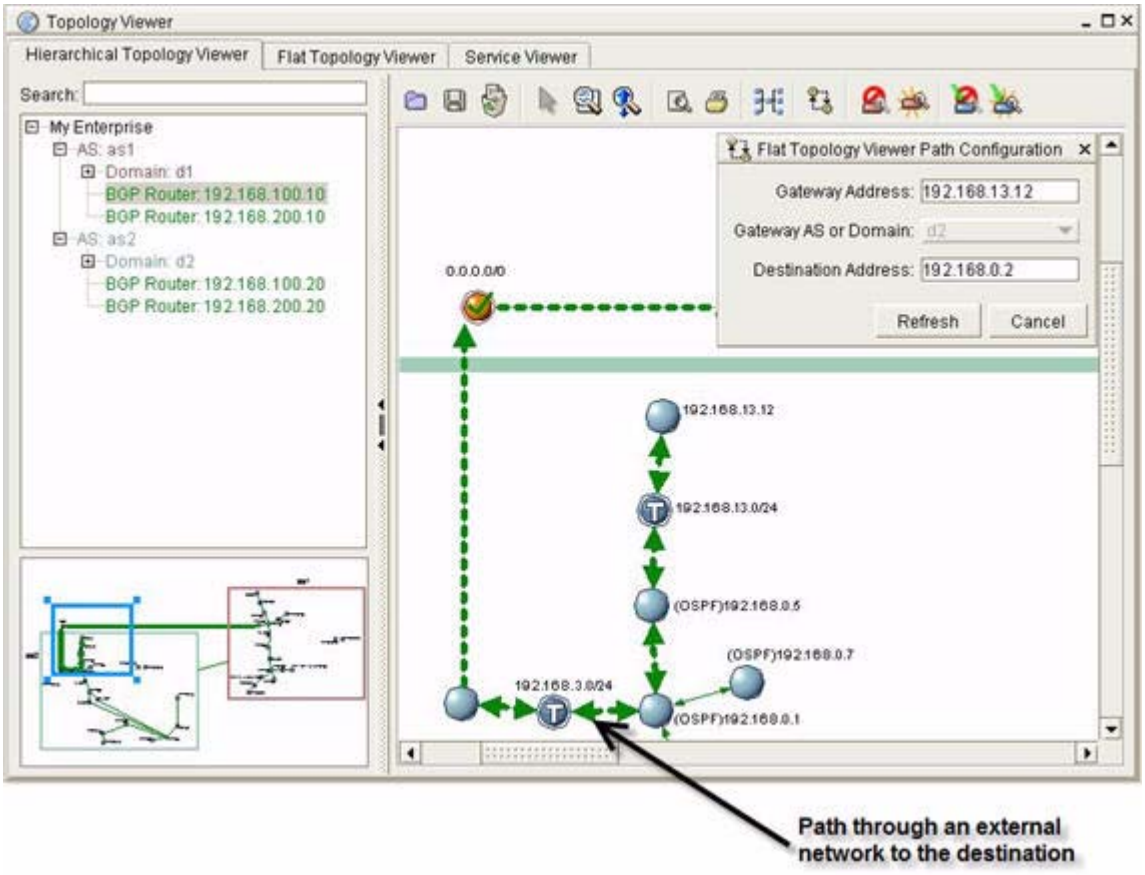


Figure 1-10 shows an exploratory path in the Topology Viewer.

Move and Resize Windows and Dialog Boxes

Each Path Analyzer module opens into a window that shows the content of the module, such as the Topology Viewer or the Events List. If you click an item within a window, such as a button in an Event Log window, additional dialog boxes open. All windows, and many dialog boxes within Path Analyzer modules, can be moved and resized, except those in Chart Manager and Administration.

Chart Manager and Administration windows were designed to take up a minimal amount of console space, allowing access to your topology, network events, service paths, and alarms while you create charts and complete system administration tasks.

The taskbar of the Management Console provides features to Manage Windows and Sessions.

Move a Window or Dialog Box

To move a window or a dialog box:

Step 1 Click the title bar of the window or dialog box.

Step 2 Drag the window or dialog box to the desired location on the Management Console.

Resize a Window or Dialog Box

To resize a window or dialog box:

Step 1 Position your mouse pointer over a corner or an edge of the window or dialog box. The mouse pointer changes to a bi-directional arrow.

Step 2 Click a corner or an edge of the window or dialog box.

Step 3 Drag the corner or edge of the dialog box outward until the window or dialog box increases to the desired size.

or

Drag the corner or edge of the dialog box inward until the window or dialog box decreases to the desired size.

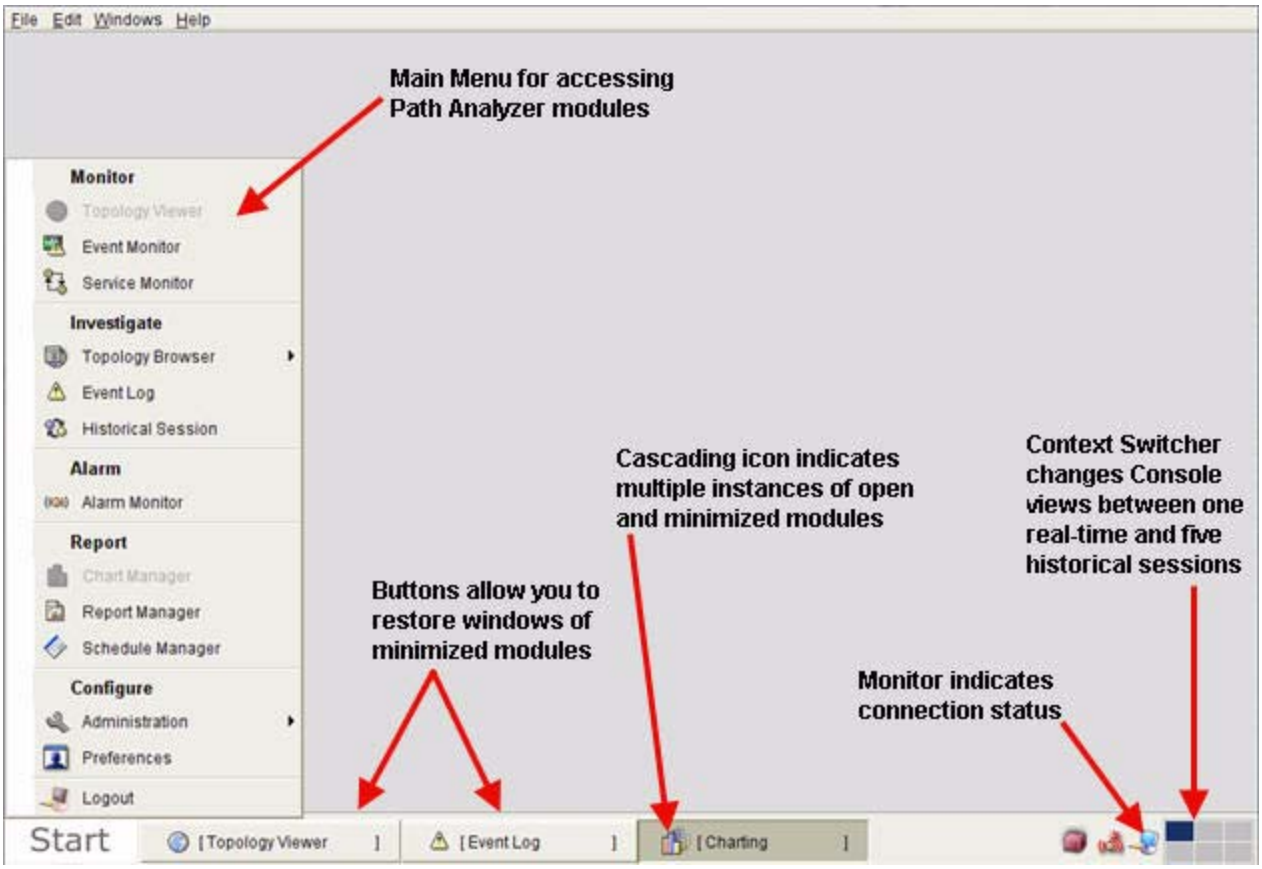
Manage Windows and Sessions

From the Path Analyzer Management Console, you can run one real-time session and up to five historical sessions simultaneously. In each historical session, you can open modules, such as the Topology Viewer, Service Monitor, and Event Log, to view the state of your network topology, paths, and events as they occurred during the specified time period.

To simplify the management of windows and sessions, the Path Analyzer taskbar allows you to minimize and stack the windows of open sessions and switch between the real-time and historical sessions.

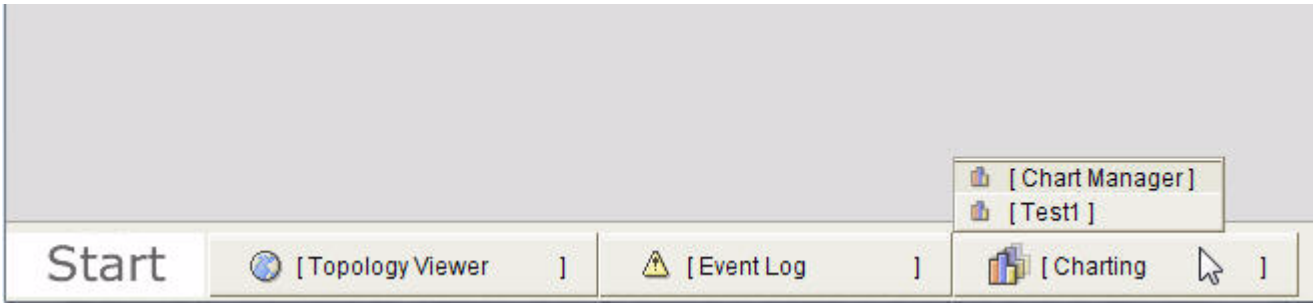
Figure 1-11 shows features of the taskbar that control views of information in the Management Console.

Figure 1-11 Taskbar Features



Clicking the button that represents a minimized module causes a submenu to be displayed, such as the submenu of the Charting module, shown in Figure 1-12.

Figure 1-12 Submenu of Topology Viewer Button in Taskbar



Selecting an option from the submenu causes the corresponding window to be opened and moved in front of other open windows, if it was previously minimized, or causes the window to be minimized if it was previously open.

In Figure 1-12, both the Event Log window and the Topology Viewer window are minimized. Clicking the Event Log option from the submenu causes the Event Log window to display in front of other open windows in the Management Console. Clicking the Charting module option allows you to select which chart window you want to display, the Chart Manager or the Test1 chart.

Minimize Open Windows

To minimize open windows:

Step 1 Click the Minimize button, if it is present in the title bar of the window.

Step 2 Or, perform one of the following two options:

- Click the button of the module you want to minimize in the taskbar.
- Select the name of the window from the submenu. See Figure 1-12 for an example of a module button and its submenus.

Restore a Minimized Window

To restore a minimized window:

Step 1 Click the button in the taskbar of the module associated with the window you want to restore.

Step 2 Select the name of the window from the submenu. The selected module window opens and becomes the active window in the Management Console.

Change between Real-time and Historical Sessions

From the taskbar, click one of the following:

- First cell of the Context Switcher to restore the real-time session
- An active cell of the Context Switcher to view a selected historical session:

Figure 1-13 Context Switcher with Real-time and Two Historical Sessions

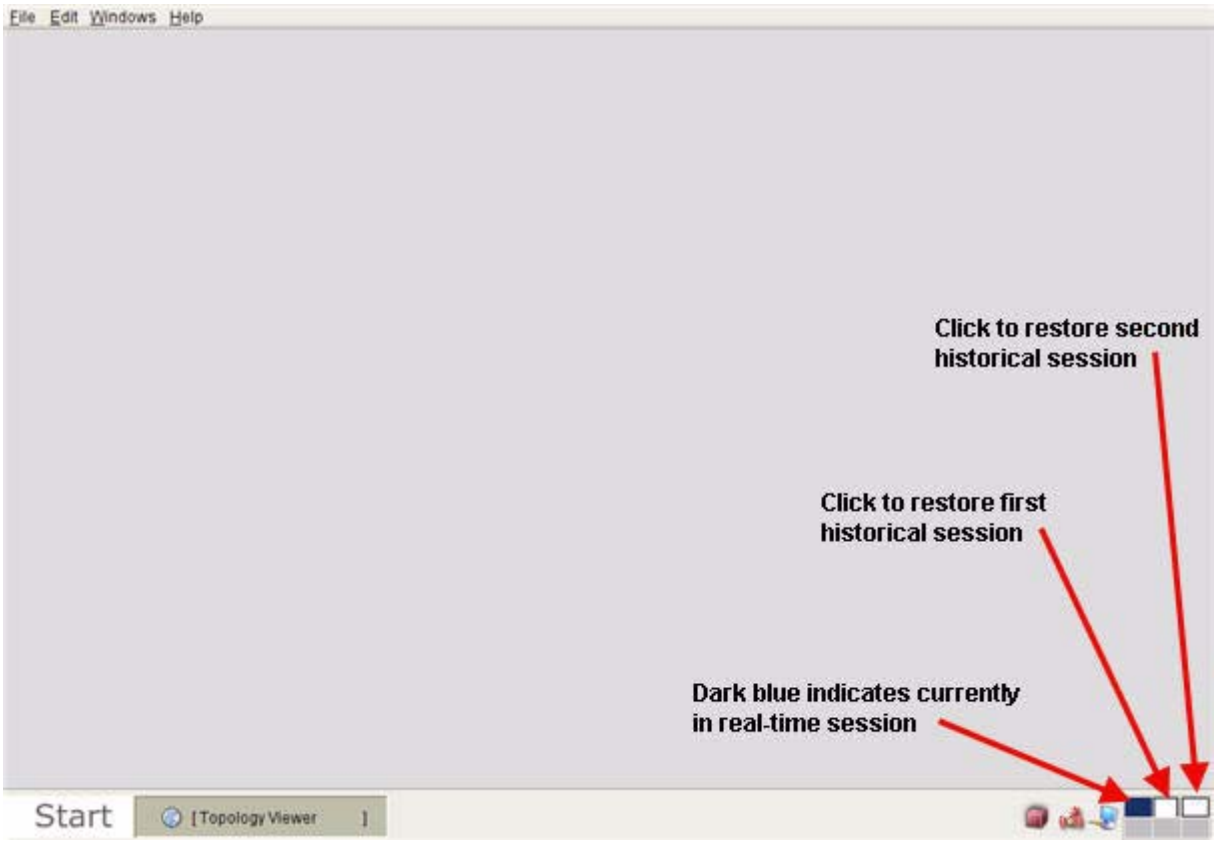


Figure 1-13 shows the Context Switcher with one real-time and two historical sessions.

Select a Module Window

The Windows menu allows you to select a specific module window when many modules are open on your Management Console at the same time.

Select a Real-time Module Window

In the Path Analyzer menu bar:

- Click **Windows > Real-time > Desktop** to run the selected real-time view of the Management Console.

or

- Click **Windows > Real-time > <module>** where <module> is replaced by the name of the Path Analyzer module. The selected module window appears in front of all other open windows.

Select a Historical View of a Module

- Click **Windows > History**

to run the selected historical view of the Management Console.

or

- Click **Windows > History > <module>**

where **<module>** is replaced by the name of the Path Analyzer Management Console module. The selected module window appears in front of all other open windows.

Log out of Path Analyzer

To log out of Path Analyzer:

Step 1 Select **File > Logout** from the Path Analyzer menu bar. The Logout box appears, prompting for confirmation.

Step 2 Click **Yes** to log out of the Path Analyzer Management Console.

or

Click **No** to remain logged into the Management Console.

Exit Path Analyzer

From the Path Analyzer menu bar, select **File > Exit**. The Management Console window closes.

Move or Copy Information

Copying information from fields in windows or dialog boxes allows you to paste information into a text file or fields in other windows and dialog boxes.

Copy, then Paste

To copy, then paste:

Step 1 Select information from a field in a window or dialog box.

Step 2 Select **Edit > Copy** from the Path Analyzer menu bar, or use the keyboard command Ctrl+C. Selected information is duplicated in a memory buffer and continues to be displayed in the field.

Step 3 Place your cursor a field in the same or another window or dialog box.

or

Open and place your cursor in a text editor.

Step 4 Type Ctrl+V on your keyboard.

Selected information is transferred into the field or text editor you selected.

If you paste information into a text file, you can save the text file and store the information to view it again.

Save Tabulated Data

You can save selected rows or an entire set of tabulated data presented in a Topology Browser or other dialog box of a Path Analyzer module to a Comma Separated Value (*.csv) file.

By default, the file is saved in the location of your Path Analyzer executable (*.exe) file, which you selected when you installed the Management Console. You can also select another directory in which to store the file.

To save tabulated data in a current Path Analyzer dialog box presenting tabulated data:

Step 1 Select the rows of data you want to save, or select the entire table.

Step 2 Select one of the following options from the Path Analyzer menu bar:

- **Edit > Export to CSV > Select Rows**

Selected rows are saved in a *.csv file located in the directory where you store the Path Analyzer executable file.

- **Edit > Export to CSV > Entire Table**

The entire selected table is saved in a *.csv file located in the directory where you store the Path Analyzer executable file.

- **Edit > Export to CSV > Change Output File**

Opens the Choose File dialog box, in which you can select a location in which to save the *.csv file. Selected rows or the entire table are saved in the specified location.

Set Preferences

Path Analyzer user preferences allow you to control the display of network elements and information in the Management Console. You can:

- Select Topology Viewer Settings, page 1-25—Select options that affect how the location, type, and size of topology elements are displayed.
- Select Preferences for Router Names, page 1-29—Show full or truncated router names, Router IDs, and generic router names of the routers displayed in the Topology Viewer, event descriptions, alarms, and other parts of the Management Console.
- Set the Formatting of Dates and Times, page 1-32—Formatting of time stamps displayed in modules of the Management Console.
- Set Automatic Completion of Fields, page 1-33—Set Path Analyzer to automatically complete words and entries you type into fields or turn off auto-completion.
- Set Modules to Start Automatically, page 1-34—Select Path Analyzer modules to start automatically after you log into the Management Console.

Figure 1-14 Topology Viewer Settings in Preferences Screen

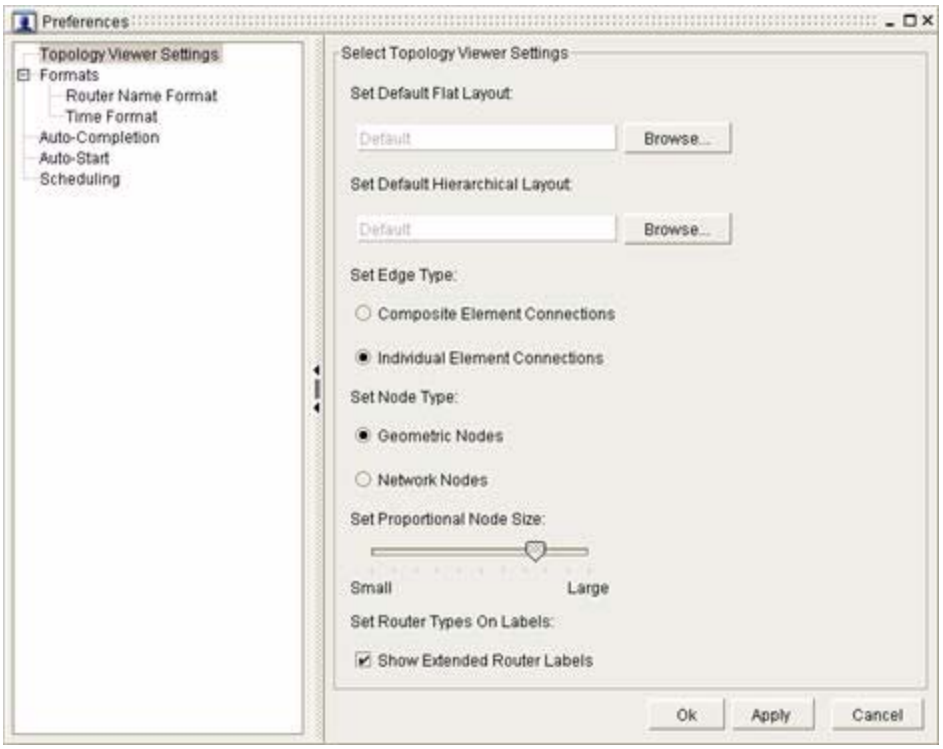


Figure 1-14 shows the Topology Viewer settings in Preferences.

Select Topology Viewer Settings

See Save a Topological Layout, page 2-42 for information about positioning elements in the Flat Topology Viewer and saving the configuration for later use. See Remove a Topological Layout, page 2-42 for information about positioning elements in the Hierarchical Topology Viewer. Use the following procedures to restore the saved configuration in the Flat or Hierarchical Topology Viewers.

Set the Default Flat Layout

To set the default flat layout:

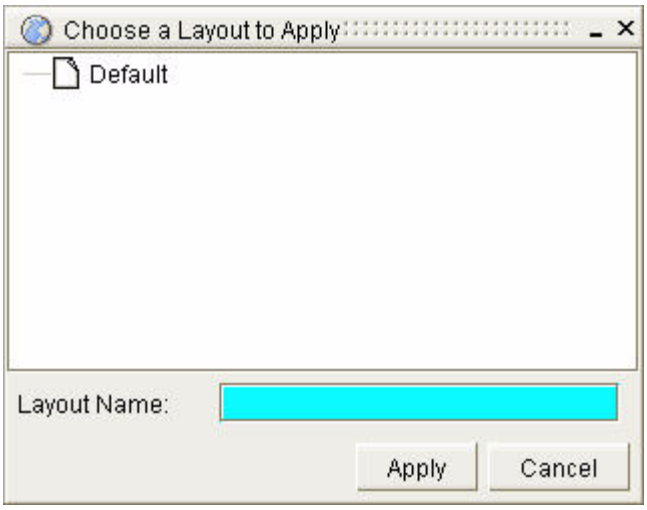
Step 1 Select **Start** > **Preferences** from the Path Analyzer taskbar.

The Preference dialog box appears, showing options for Topology Viewer Settings.

Step 2 Click **Browse** in the Set Default Flat Configuration field.

The Choose a Layout to Apply dialog box appears (see Figure 1-15).

Figure 1-15 Choose a Layout to Apply in Preferences Screen



Step 3 Select the configuration to apply.

or

In the Layout Name field, type the name of the configuration to apply.

Step 4 Click **Apply**.

Step 5 Open the Topology Viewer if you have not already done so, move it into the foreground of the Management Console, and select the Flat Topology Viewer to view the flat layout.

Step 6 Select additional settings, including:

- Set the Default Hierarchical Layout, page 1-26.
- Set the Edge Type, page 1-27.
- Set the Node Type, page 1-28.
- Set the Proportional Node Size, page 1-28.
- Set Router Types on Labels, page 1-29.

or

Click **OK** to submit your selection without making additional changes.

Set the Default Hierarchical Layout

To set the default Hierarchical layout:

Step 1 Select **Start** > **Preferences** from the Path Analyzer taskbar.

The Preferences dialog box appears, showing options for Topology Viewer Settings.

Step 2 Click **Browse** in the Set Default Hierarchical Configuration field.

The Choose a Layout to Apply dialog box appears.

Step 3 Select the configuration to apply.

or

In the Layout Name field, type the name of the configuration to apply.

Step 4 Click **Apply**.

Step 5 Move the Topology Viewer into the foreground of the Management Console and select the Hierarchical Topology Viewer to view the hierarchical layout.

Step 6 Select additional settings, including:

- Set the Default Flat Layout, page 1-25.
- Set the Edge Type, page 1-27.
- Set the Node Type, page 1-28.
- Set the Proportional Node Size, page 1-28.
- Set Router Types on Labels, page 1-29.

or

Click **OK** to submit your selection without making additional changes.

Set the Edge Type

To set the Edge Type:

Step 1 Use the procedures Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Step 2 Select **Start** > **Preferences** from the Path Analyzer taskbar.

The Preferences dialog box appears, showing options for Topology Viewer Settings.

Step 3 Select how to display point-to-point and transit-to-router links:

Select one of the following options and view the change in the Map:

- **Composite Element Connections—**Each point-to-point, transit-to- router, or transit interface link is represented by a double terminated arrow.
- **Individual Element Connections**—Each point-to-point, transit-to- router, or transit interface link is represented by a single terminated arrow pointing in the direction of the data. When data passes in both directions between two routers or a router and a network, two parallel arrows are displayed indicating both directions.

For information about the types of links displayed in the Topology Viewer, see Interfaces and Links, page 2-30.

Step 4 Click **Apply** to select additional settings, including:

Set the Default Flat Layout, page 1-25.

Set the Default Hierarchical Layout, page 1-26.

Set the Edge Type, page 1-27.

Set the Node Type, page 1-28.

Set the Proportional Node Size, page 1-28.

Set Router Types on Labels, page 1-29.

or

Click **OK** to submit your selection without making additional changes.

Set the Node Type

To set the Node Type:

Step 1 Use the procedures Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Step 2 Select **Start > Preferences** from the Path Analyzer taskbar.

The Preferences dialog box appears, showing options for Topology Viewer Settings.

Step 3 Select the radio button in the Set Node Type field for either:

- **Geometric Nodes**, or
- **Network Nodes**.

For example icons of how geometric vs. network nodes are displayed within the Topology Viewer, see Table 2-4.

Step 4 Click **Apply** to select additional settings, including:

- Set the Default Flat Layout, page 1-25.
- Set the Default Hierarchical Layout, page 1-26.
- Set the Edge Type, page 1-27.
- Set the Proportional Node Size, page 1-28.
- Set Router Types on Labels, page 1-29.

or

Click **OK** to submit your selection without making additional changes.

Set the Proportional Node Size

To set the Proportional Node Size:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Step 2 Select **Start > Preferences** from the Path Analyzer taskbar.

The Preferences dialog box appears, showing options for Topology Viewer Settings.

Step 3 Adjust the setting in the Set Proportional Node Size field:

- Drag the slider toward the Small setting to reduce the size of icons displayed in the Topology Viewer after you restart it.
- Drag the slider toward the Large setting to increase the size of icons displayed in the Topology Viewer after you restart it.

Step 4 Click **Apply** to select additional settings, including:

- Set the Default Flat Layout, page 1-25.
- Set the Default Hierarchical Layout, page 1-26.
- Set the Edge Type, page 1-27.
- Set the Proportional Node Size, page 1-28.
- Set Router Types on Labels, page 1-29.

or

Click **OK** to submit your selection without making additional changes.

Set Router Types on Labels

Set the router type on labels:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Step 2 Select **Start** > **Preferences** from the Path Analyzer taskbar.

The Preferences dialog box appears, showing options for Topology Viewer Settings.

Step 3 Click the **Show Extended Router Labels** check box In the Set Router Types on Labels field. A check mark is displayed in the check box when this option is selected, indicating that the type of router is appended to label of the router.

Step 4 Click **Apply** to select additional settings, including:

- Set the Default Flat Layout, page 1-25.
- Set the Default Hierarchical Layout, page 1-26.
- Set the Edge Type, page 1-27.
- Set the Node Type, page 1-28.
- Set the Proportional Node Size, page 1-28.

or

Click **OK** to submit your selection without making additional changes.

Select Preferences for Router Names

Set the Label Size

To set the label size:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Step 2 Select **Start** > **Preferences** from the Path Analyzer taskbar.

The Preferences dialog box appears, showing options for Topology Viewer Settings.

Step 3 Adjust the setting in the Label Size field:

- Drag the slider toward the Small setting to reduce the size of labels that are displayed with router and network icons in the Topology Viewer.
- Drag the slider toward the Large setting to increase the size of labels that are displayed with router and network icons in the Topology Viewer.

Step 4 Click **Apply** if you want to select additional settings.

or

Click **OK** to submit your selection without making additional changes. Restarting the Topology Viewer causes labels to be displayed with the size you selected.

Set Router Name Formats

To set router name formats:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Step 2 Select **Start > Preferences** from the Path Analyzer taskbar.

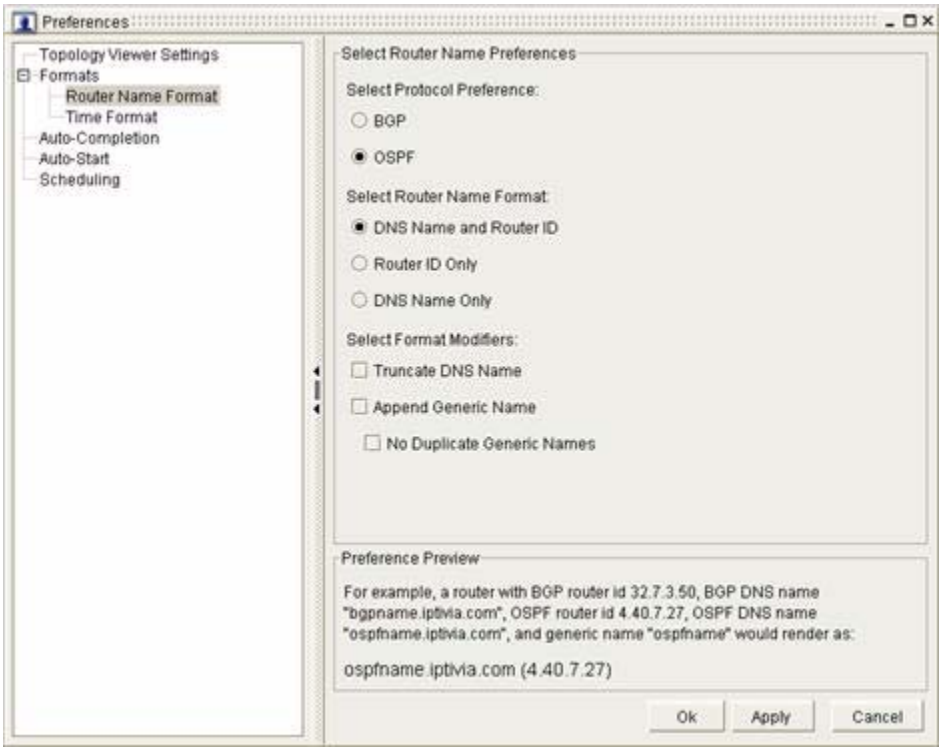
The Preferences dialog box appears, showing options for Topology Viewer Settings (see Figure 1-16).

Step 3 Select **Formats > Router Name Format** from the hierarchy of options. The Select Router Name Preferences fields are displayed in the active view of the Preferences dialog box.

Step 4 Select one of the following options in the Select Protocol Preference field:

- **BGP**—Sets formatting for all BGP routers.
- **OSPF**—Sets formatting for all OSPF routers.

Figure 1-16 Router Name Format Fields in Preferences Screen



Note For each of your selections, the Preference Preview field shows an example of how router names are displayed in the Topology Viewer.

Step 5 Select one of the following options in the Select Router Name Format field:

- **DNS Name and Router ID**
- **Router ID Only**
- **DNS Name Only**

Step 6 In the Select Format Modifiers field, select one or both of the following options:

- **Truncate DNS Name**—Removes the file extension from the DNS name of routers.
- **Append Generic Name**—Adds a hyphen and the generic router name.
- **No Duplicate Generic Name**—Resolves duplicate router names when the DNS name or Router ID are the same as the generic name.

For example, if you select DNS Name Only for a router with a DNS name `ASBR90.cisco.com`, then you select Truncate DNS Name, the name is shortened to `ASBR90`.

If the DNS Name is the same as the generic router name, when you select Append Generic Name, the name is displayed as: `ASBR90 - ASBR90`.

Selecting No Duplicate Generic Name shortens the name to `ASBR90`, resolving the duplicated name.

Step 7 Click **OK**.

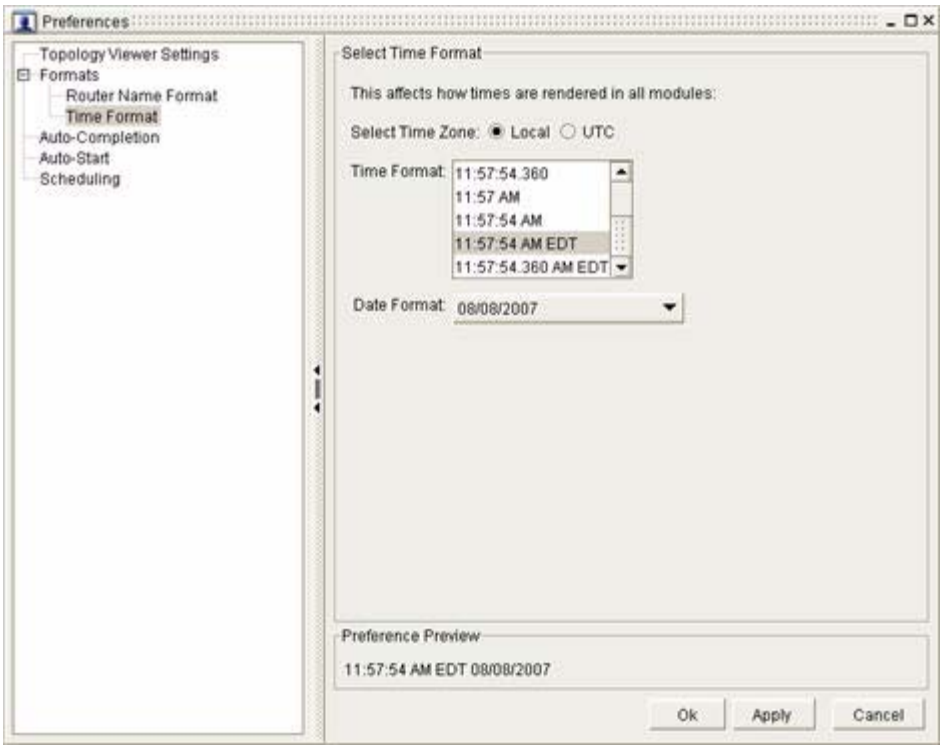
Your selections are displayed for all routers in the modules of the Path Analyzer Management Console.

Set the Formatting of Dates and Times

To set the formatting of dates and times in Path Analyzer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Figure 1-17 Date and Time Format Fields in Preferences Screen



Step 2 Select **Start** > **Preferences** from the Path Analyzer taskbar.

The Preferences dialog box appears, showing options for Topology Viewer Settings.

Step 3 Select **Time Format** (see Figure 1-17).

Step 4 Select a radio button for either **Local** or **UTC i**n the Select Time Zone field.

Step 5 From the Time Format menu, select a format for time values displayed in Path Analyzer modules.

Step 6 From the Date Format menu, select a format for date values displayed in Path Analyzer modules.

The Preference Preview field shows how your selection will look in the Path Analyzer Management Console.

Step 7 Click **OK**. The Preferences dialog box closes. Path Analyzer modules present time stamps according to your selection.

Set Automatic Completion of Fields

To set the automatic completion of fields:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Step 2 Select **Start** > **Preferences** from the Path Analyzer taskbar.

The Preference dialog box appears, showing options for Topology Viewer Settings.

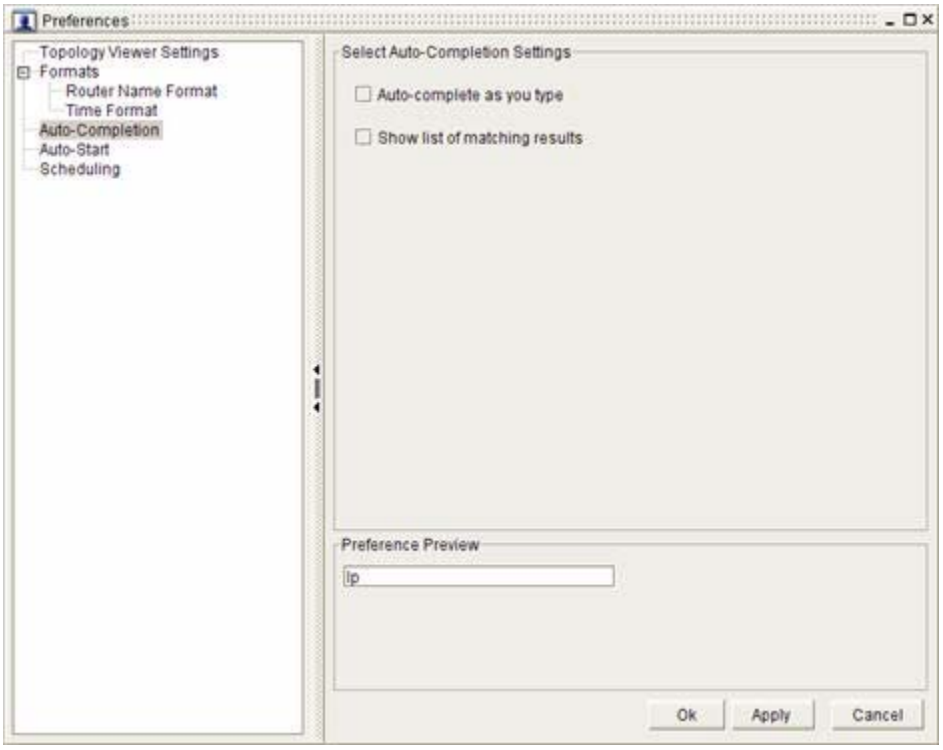
Step 3 Select **Auto-Completion** from the hierarchy of options.

The Select Router Name Preference fields are displayed in the active view of the Preference dialog box (see Figure 1-18).

- Select **Auto-complete as you type** to set the fields in Path Analyzer dialog boxes and windows to automatically complete your entries as you type them.
- Select **Show list of matching results** to display for fields that provide search capabilities, such as in Query dialog boxes.

A check mark is displayed in the check box when this option is selected.

Figure 1-18 Auto-Completion Fields in Preferences Screen



Step 4 Click **Apply** if you want to select additional settings.

or

Click **OK** to submit your selection without making additional changes.

Set Modules to Start Automatically

To set modules to open automatically when you start Path Analyzer:

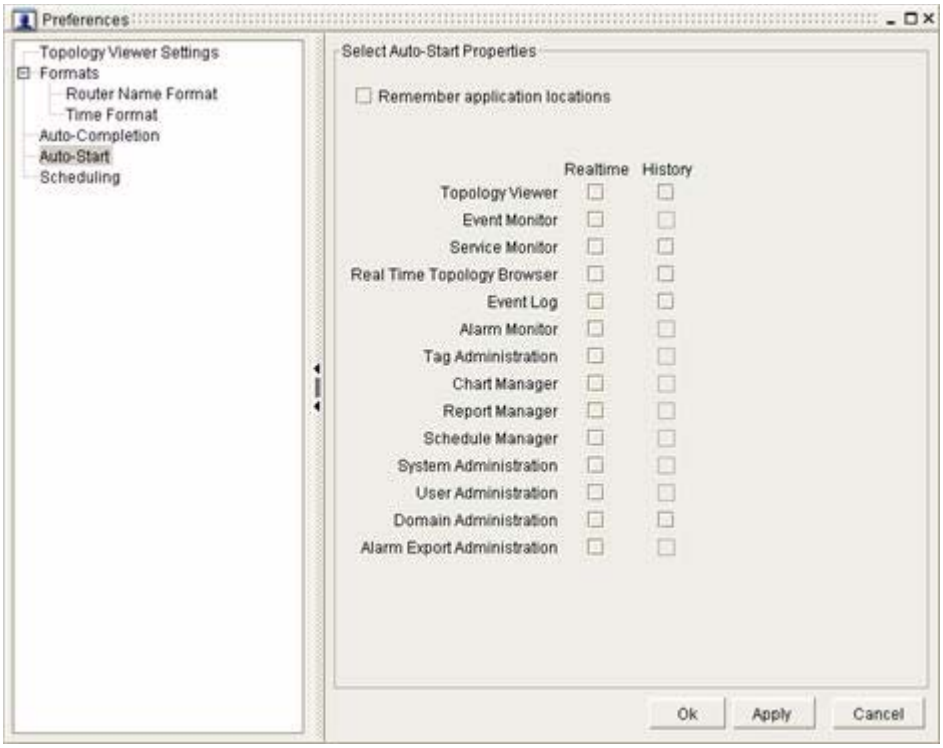
Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Step 2 Select **Start** > **Preferences** from the Path Analyzer taskbar.

The Preference dialog box appears, showing options for Topology Viewer Settings.

Step 3 Select **Auto-Start** from the hierarchy of options (see Figure 1-19).

Figure 1-19 Auto-Start Fields in Preferences Screen



Step 4 Select **Remember application locations** to make Path Analyzer track the location and placement of modules as you use them within the Management Console.

A check mark is displayed in the check box when this option is selected.

Step 5 From the Realtime column, select the modules you want Path Analyzer to track and record for placement during a real-time session of the Management Console.

This option causes the Path Analyzer modules you used previously to be displayed when you restart the Real-time Management Console.

Step 6 From the History column, select the modules you want Path Analyzer to track and record for placement during a real-time session of the Management Console.

This option causes the Path Analyzer modules you used previously to be displayed when you rerun a historical session in the Management Console.

Step 7 Click **Apply** if you want to select additional settings.

or

Click **OK** to submit your selection without making additional changes.

Set the Amount of Time to Keep Charts, Reports, and Schedules

To set the amount of time to keep charts, reports, and schedules in Path Analyzer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4 to view your preferences in the Flat or Hierarchal Map.

Step 2 Select **Start** > **Preferences** from the Path Analyzer taskbar.

The Preference dialog box appears, showing options for Topology Viewer Settings.

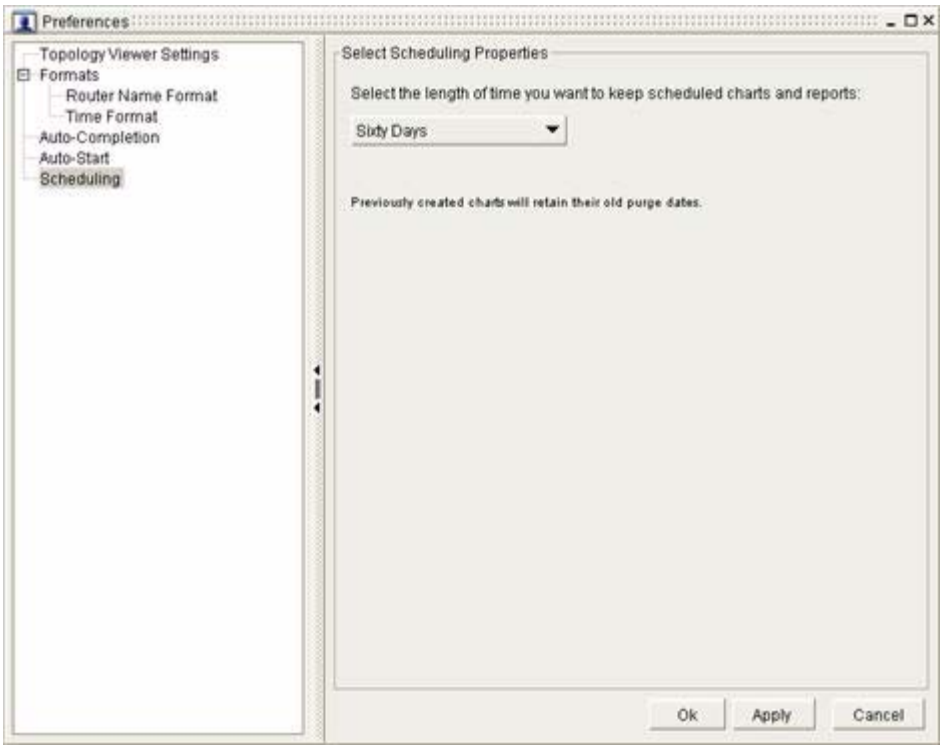
Step 3 Select **Scheduling** from the hierarchy of options (see Figure 1-20).

Step 4 Click the down arrow in the options list, and select one of the following:

- **One Day**
- **One Week**
- **Thirty Days**
- **Sixty Days**
- **One Hundred Eighty Days**
- **One Year**
- **Forever**

Charts, reports, and schedules are removed from the Path Analyzer system after the selected period of time has elapsed.

Figure 1-20 Scheduling in Preferences Screen



Step 5 Click **Apply** if you want to select additional settings.

or

Click **OK** to submit your selection without making additional changes.

Using Help

Path Analyzer's technical documentation is available to help you before and after you log into the Path Analyzer Management Console.

You can access technical documentation from the Help screen or the PDF documents that you received from your sales representative. To receive the most up-to-date technical documentations, please contact your sales or customer service representative.

View an Online Manual

Step 1 From the Path Analyzer Management Console, click **Help**.

Step 2 Select one of the following options:

- **User Guide**
- **System Administrator Guide**
- **Alarm Reference**

Find Version and Copyright Information

From the Path Analyzer Management Console, click **Help > About Path Analyzer**.

The version number and copyright date of your Path Analyzer Management Console is displayed in the About dialog box.

CHAPTER 2

Monitoring Your Network's Topology

Viewing Your Network Topology in Detail

Your network is a complex hierarchy of systems, subsystems, and components. At the highest level, your network consists of one or more autonomous systems, which include collections of routers.

Structure of Your Network in Cisco Service Path Analyzer

Each autonomous system is generally divided into domains for easier administration. Router messages are exchanged within each domain over a shared interior gateway protocol (IGP), such as:

- Open Shortest Path First (OSPF)
- Interior Border Gateway Protocol (iBGP)
- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System - Intermediate System (IS-IS) Protocol

Note The current release of Cisco Service Path Analyzer (hereafter referred to as Path Analyzer) supports a one-to-one correspondence between autonomous systems and routing domains. In the visual display of your network topology in Path Analyzer, an autonomous system contains one routing domain, which is divided into many smaller OSPF domains, called areas.

Exchanges of Routers Between Autonomous Systems

Specialized routers called Autonomous System Boundary Routers (ASBRs) have interfaces in multiple autonomous systems and exchange routing data between them. ASBRs communicate over shared external gateway protocols, such as external Border Gateway Protocol (eBGP).

Path Analyzer Listeners collect routing data from iBGP, OSPF, and eBGP routers. The Path Analyzer Server processes collected data from Listeners and generates the dynamic, real-time topology of your network in the Topology Viewer and Topology Monitor of the Path Analyzer Management Console.

Topology Viewer Shows Your Network's Topology

The Topology Viewer presents three views of your network in the following tabs:

- **Flat Topology Viewer**—Provides the flat, graphical view of the entire topology, without visual demarcations between OSPF areas. The Flat Topology Viewer also provides tabular displays of detailed information about the areas, routers, interfaces, networks, route advertisements, and routes that comprise your network.

  From the topological view of your network, you can easily locate and identify the cause of routing problems, view router details and interfaces, and track the flow of data.

- **Hierarchical Topology Viewer**—Provides an individual view of each autonomous system and OSPF area contained within an autonomous system. From the Hierarchical Topology Viewer, you can expand an autonomous system and expand an area to view the routers and networks contained in the domain. Further expanding the view at each level of your network lets you view a selected network segment and drill down through selected entities.

  For detailed information about the Topology Viewer and depiction of network elements, see Viewing Your Network Topology, page 2-6 and Identifying Topology Viewer Elements, page 2-14.

- **Service Viewer**—Allows you to select and view a service that was configured in your Path Analyzer system from the Service Monitor. The Service Viewer provides a view of the individual service paths that comprise the service and shows the status of routers, links, and networks on each service path. For information about creating and monitoring services in Path Analyzer, see Monitoring Unicast and Multicast Services on page 3-1.

  The Service Monitor lets you view the flow of data between selected endpoints. From the Service Viewer, you can discover if the data flow conforms to or deviates from the baseline you set when you configured the routers.

Routing Issues at a Glance

Small configuration changes on a router can significantly impact the way data is routed across your network. Because the Topology Viewer presents a clear picture of the way data traverses your network, you can quickly identify when routing patterns have changed. See Viewing Your Network Topology, page 2-6.

You can also complement the topological view with tabulated data to find information about an entity displayed in the topology. For example, the high-level view from the Topology Viewer shows where data flow is re-routed or interrupted. By pivoting from the router in the topological view to the router attributes shown in the Topology Browser, you can identify the change made to an interface metric that caused the data flow to be re-routed.

Topology Browser dialog boxes allow you to delve into specific details of a router, router interface, or advertisement, while maintaining a high-level view of your network. For information, see Getting Detailed Information About Topology Viewer Elements, page 2-45.

Note Topology Browser dialog boxes provide information about OSPF routers, interfaces, and routes, and are updated dynamically to display the most recent set of data values for each viewer element you select.

Topology Browser dialog boxes that provide information about BGP routers, interfaces, and routes require a manual update to view the latest data. See Refresh Values in a Topology Browser Dialog Box, page 2-95.

Open Investigative Event Log to Query for Related Events

Right-clicking a router, Transit network, or link provides options to open the Investigative OSPF or BGP Event Log and query for events. By looking at a path, you can identify segments that have become unavailable. Unavailable routers, subnets, and links on the path are displayed in red.

Path Analyzer helps you track and identify the root cause of routing issues by indicating unavailable routes and presenting the relevant Event Logs. For information about pivoting to Event Log from a selected router or Transit network, see Pivoting to the Event Log, page 2-64.

Real-time and Historical Views

You can view the topological map of your network in either of the following modes:

- **Real-time—**Starts the current and dynamic display of your network topology, enabling you to review current network conditions and identify problem areas.
- **Historical**—Returns your network to a previous state, enabling you to review past network topology and conditions. For information about starting the Topology Viewer while running a past sequence of events, see Replaying Your Network's History on page 13-1.

Query for Details of Network Elements

The Investigative Topology Browser wizard enables you to query for details about specific OSPF or BGP routers, interfaces, or route advertisements. Using this fast, enterprise-wide query, you can obtain information about a selected router, interface, or route advertisement. See Start the Investigative Topology Browser Wizard, page 2-5.

You can also find information about more than one interface or route advertisement by issuing detailed queries across multiple areas.

For information, see Querying for Network Elements (for OSPF Entities), page 2-82.

Topology Tasks

- Starting the Topology Viewer, page 2-4
- Viewing Your Network Topology, page 2-6
- Viewing Changes of Status, page 2-13
- Identifying Topology Viewer Elements, page 2-14
- Navigating in the Topology Viewer, page 2-32
- Viewing Services in the Service Viewer, page 2-45
- Getting Detailed Information About Topology Viewer Elements, page 2-45
- Navigating in Topology Browser Dialog Boxes, page 2-48
- Viewing Metrics and Attributes, page 2-54
- Pivoting to the Event Log, page 2-64
- Using the Topology Filter Wizard for BGP Entities, page 2-65
- Making Routing Information Base (RIB) Comparisons for BGP Routes, page 2-81

- Querying for Network Elements (for OSPF Entities), page 2-82
- Previewing and Printing a Topology, page 2-95

Starting the Topology Viewer

The Topology Viewer displays a graphical representation of your enterprise networks. Within the Topology Viewer, you can:

- Start the Flat Topology Viewer, page 2-4
- Start the Hierarchical Topology Viewer, page 2-4
- Start the Topology Browser, page 2-5

Start the Flat Topology Viewer

To start the Flat Topology Viewer:

Step 1 Click **Start > Topology Viewer** in the Path Anaylzer taskbar.

The Topology Viewer opens in the Path Anaylzer Management Console, showing the current view of the network topology.

Step 2 Select the **Flat Topology Viewer** tab.

The Flat Topology Viewer appears, showing icons that represent the autonomous systems that form your network.

Step 3 Right-click an autonomous system and click **Expand**.

The complete topology of the autonomous system is displayed.

Start the Hierarchical Topology Viewer

To start the Hierarchical Topology Viewer:

Step 1 Click **Start > Topology Viewer** in the Path Anaylzer taskbar.

The Topology Viewer opens in the Path Anaylzer Management Console, showing the current view of the network topology.

Step 2 Select the **Hierarchical Topology Viewer** tab.

The Hierarchical Topology Viewer appears, showing the autonomous systems that form your network.

Step 3 Right-click an autonomous system and click **Expand**. See Expand an Autonomous System, page 2-37.

OSPF areas are displayed within the autonomous system. Area Border Routers (ABRs) are displayed between areas.

Step 4 Right-click and expand an area. (An area is marked with a capital A). See Expand an Area, page 2-38.

The routers, subnets, and links within the area are displayed.

Start the Service Viewer

To start the Service Viewer:

Step 1 Click **Start > Topology Viewer** from the Path Anaylzer taskbar.

The Topology Viewer, page 2-96 opens in the Path Anaylzer Management Console, showing the current view of the network topology.

Step 2 Select the **Service Viewer** tab.

The Service Viewer appears.

Start the Topology Browser

To start the Topology Browser, click **Start > Topology Browser > Real-time**.

The BGP Router List Dialog Box, page 2-108 opens in the Path Analyzer Management Console. From the Enterprise Overview dialog box, you can click links (in blue) to open related Topology Browser dialog boxes.

To return to the Enterprise Overview dialog box at any time, click the **Go To Enterprise Overview** icon  in the toolbar of any Topology Browser dialog box.

Related Topics

- Getting Detailed Information About Topology Viewer Elements, page 2-45
- Navigating in Topology Browser Dialog Boxes, page 2-48
- Viewing Metrics and Attributes, page 2-54

Start the Investigative Topology Browser Wizard

To start the Investigative Topology Browser wizard, click **Start > Topology Browser > Investigative**.

The Investigative Topology Browser wizard opens in the Path Anaylzer Management Console.

Related Topics

Using the Topology Filter Wizard for BGP Entities, page 2-65

Querying for Network Elements (for OSPF Entities), page 2-82

Note From the Preferences window (**Start > Preferences**), you can set viewing options in the Flat, Hierarchical, and Service Viewers of the Topology Viewer. For information, see Select Topology Viewer Settings, page 1-25.

Viewing Your Network Topology

The Topology Viewer provides a visual representation of your overall network topology and network status. From the top of the hierarchy, the Topology Viewer provides you with a view of the autonomous systems that comprise your network.

In the Topology Viewer, your network topology is presented in three views:

- **Flat Topology Viewer** of your entire topology. You can open the Flat Topology Viewer to view the availability of routers, interfaces, subnets, and links in your network. See View the Flat Topology Viewer, page 2-6.
- **Hierarchical Topology Viewer** of the components that form your network, including autonomous systems, lower-level areas, and components, routers, Transit networks, and links. In the Hierarchical Topology Viewer, you expand an element to view the lower-level elements it contains and collect information about state and availability. See View the Hierarchical Topology Viewer, page 2-7.
- **Service Viewer** of the service paths that comprise a critical service path configured in Service Monitor. See View the Hierarchical Topology Viewer, page 2-7.

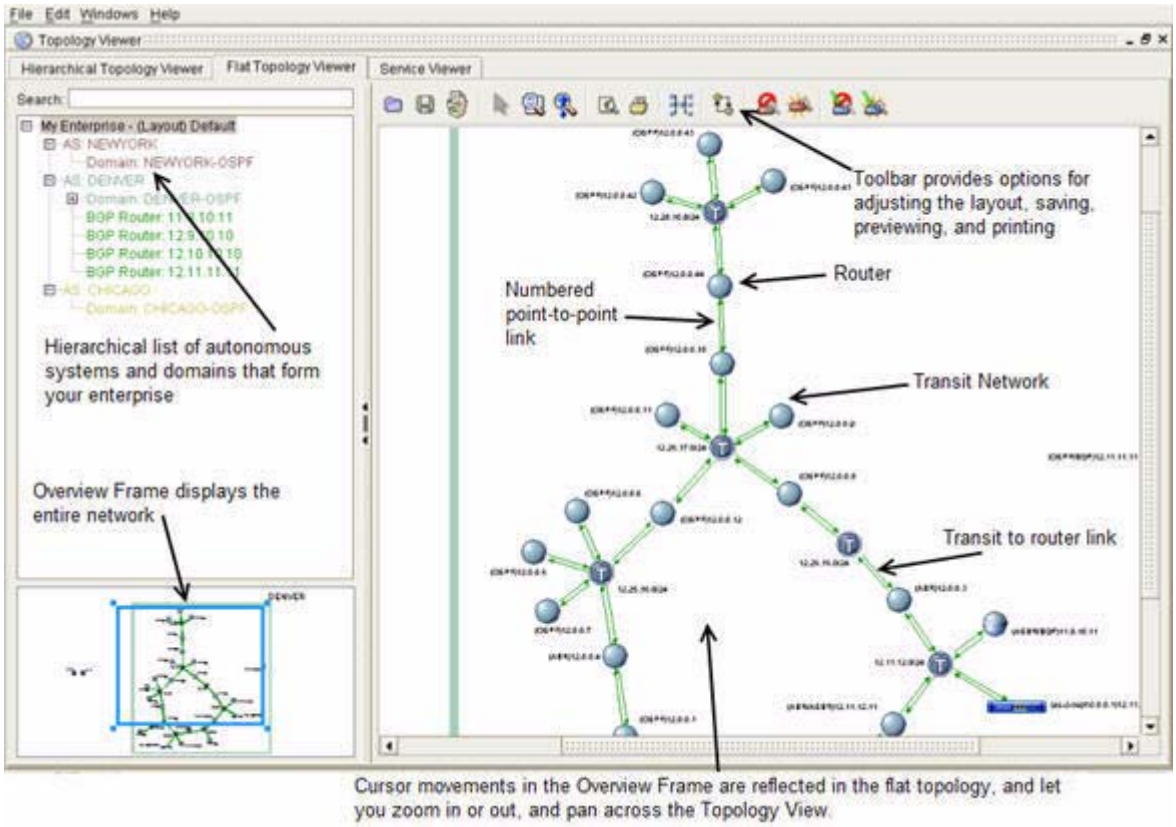
View the Flat Topology Viewer

If you want to view all areas in your network topology without viewing entities between areas, you can right-click and expand an autonomous system in the Flat Topology Viewer. The Flat Topology Viewer shows all routers within an autonomous system without showing demarcations between areas.

The Flat Topology Viewer positions topology elements according to a hub-and-spoke layout, allowing you to view your network as an entity comprised of interconnected OSPF areas. Elements in the hierarchical list correspond directly to the icons that represent each element in the visual view. Selecting an element from the hierarchical list pinpoints and brings the corresponding icon to the forefront in the visual view.

Right-clicking an autonomous system, OSPF area, or router provides options for viewing its attributes Figure 2-1 shows the layout of an expanded area in the Flat Topology Viewer.

Figure 2-1 Flat Topology Viewer



The Flat Topology Viewer enables you to obtain a quick, integrated view of your network topology without showing OSPF areas. This allows you to view the complete, uninterrupted path of data as it traverses your network.

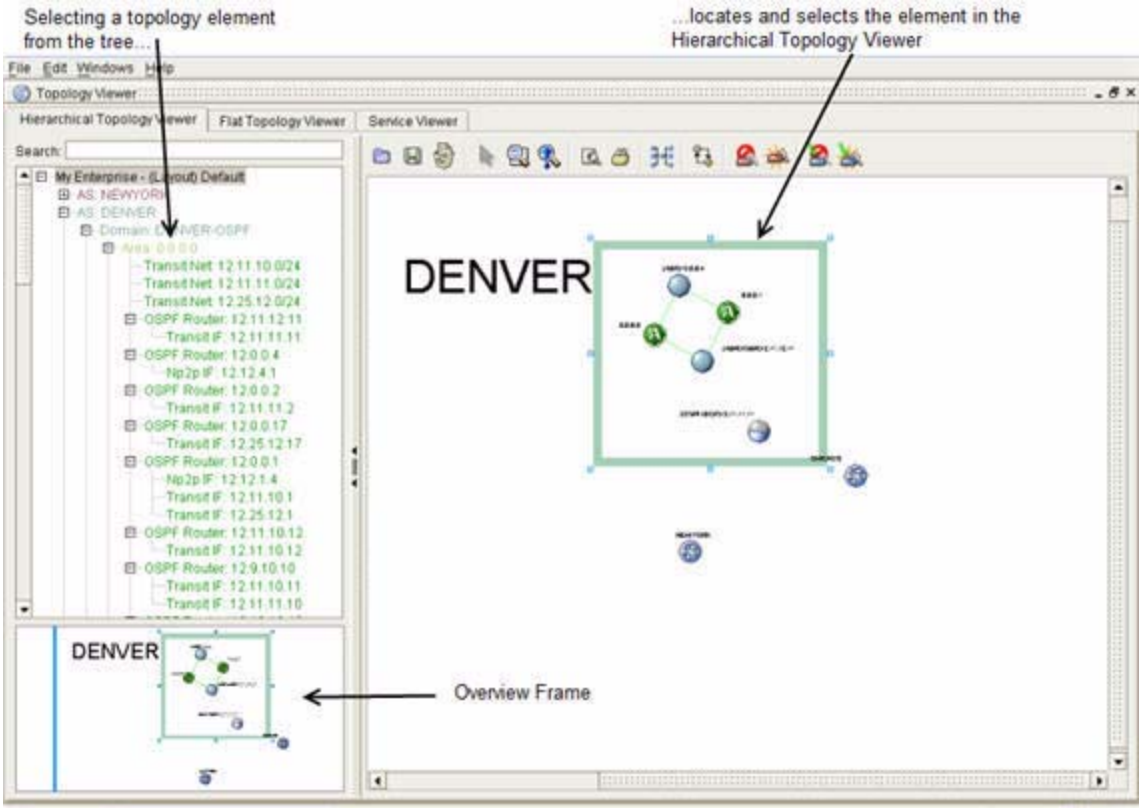
View the Hierarchical Topology Viewer

The Hierarchical Topology Viewer shows a similar layout as the Flat Topology Viewer, displaying a hierarchical list of autonomous systems and OSPF areas, a toolbar of options, the Overview Frame, and a view of the network topology.

The Hierarchical View of the topology requires you to select and expand an autonomous system to view the areas it contains. Figure 2-2 shows a view of an expanded autonomous system that contains two areas connected by an ASBR.

By expanding an autonomous system in the Hierarchical Topology Viewer, you can view the areas it contains. Right-clicking an area provides options to expand it and view the routers it contains.

Figure 2-2 Hierarchical Topology Viewer



Elements of your network topology, including autonomous systems, areas, routers, and Transit networks, are represented by a default set of icons that you can change in **Start > Preferences**. For information about the display of all elements of the network topology, see Table 2-1.

Arrows represent links—data that passes between two routers or between a router and a Transit network. The Topology Viewer shows a representation of the following types of links:

- Numbered Point-to-Point (NP2P)
- Unnumbered Point-to-Point (UP2P)
- Transit Interface (passes from the router to the Transit network)
- Transit-to-Router Interface (passes from the Transit network to the router)

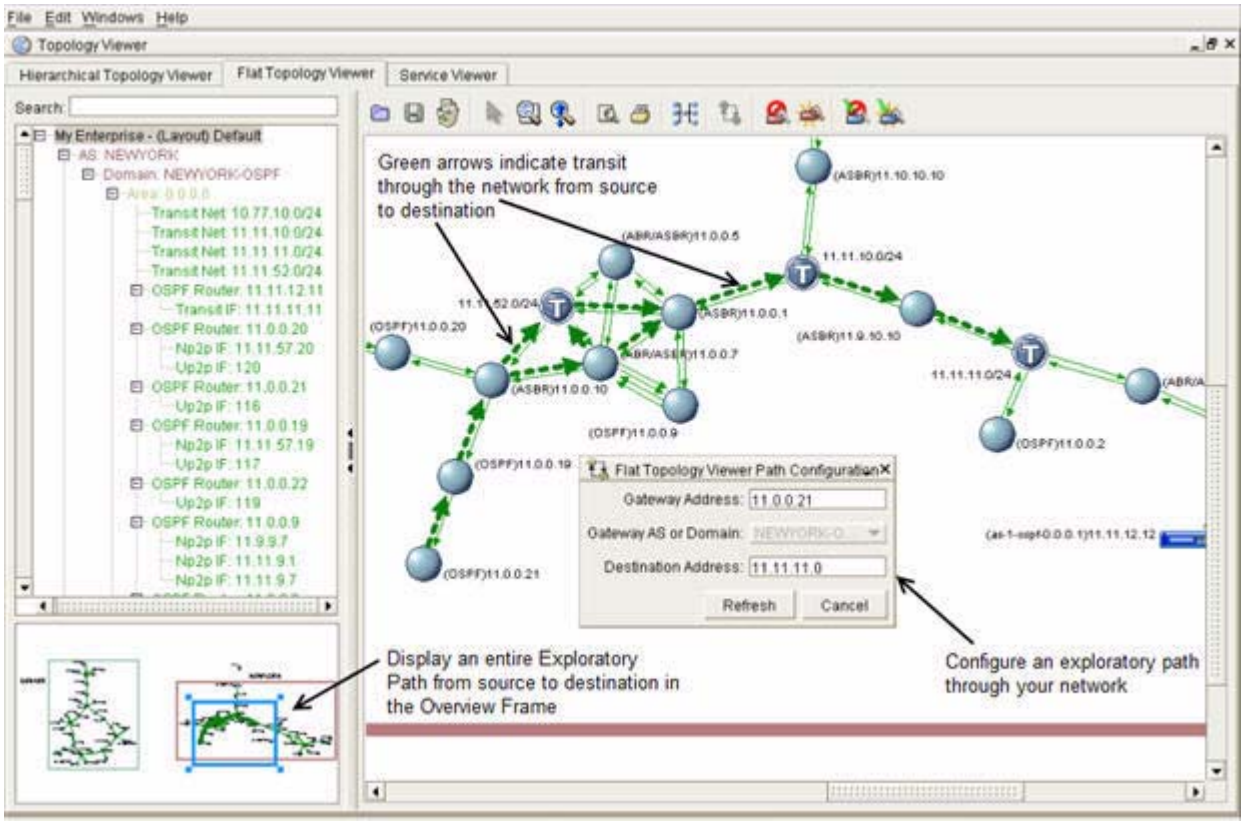
For information about links presented in the Topology Viewer, see Interfaces and Links, page 2-30. For information about changing the appearance of links displayed in the Topology Viewer, see Set the Edge Type, page 1-27.

View Exploratory Paths

Path Analyzer monitors data as it traverses your network from the first gateway that receives data to the router one hop from the destination, within an autonomous system. Using the Exploratory Paths feature of the Flat and Hierarchical Topology Viewers, you can view the traversal of a selected path across an autonomous system.

You can view an exploratory path graphically, represented as a heavy, dotted green line between a selected gateway and destination. Figure 2-3 shows an exploratory path that traverses through an autonomous system.

Figure 2-3 Exploratory Path in Topology Viewer



View an Exploratory Path

To view an exploratory path in the Topology Viewer:

Step 1 Use the procedure to Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Locate the originating gateway and final destination of the path, then click the **Configure Exploratory Path** icon.

The Exploratory Path Configuration dialog box appears.

Step 3 Enter the Router ID or name of the router that originates the path in the Gateway Address field.

Step 4 In the Gateway AS or Domain field:

- Ensure the correctness of the identifier of the OSPF area or BGP routing domain in which the gateway router is located. This value is selected automatically.

or

- Select the identifier of the OSPF area or BGP routing domain in which the gateway router is located.

Step 5 Enter the IP address of the path's destination in the Destination Address field.

Step 6 Click **Refresh**.

In the Topology Viewer, the exploratory path is displayed as a heavy, dotted, green line that connects routers and traverses domains.

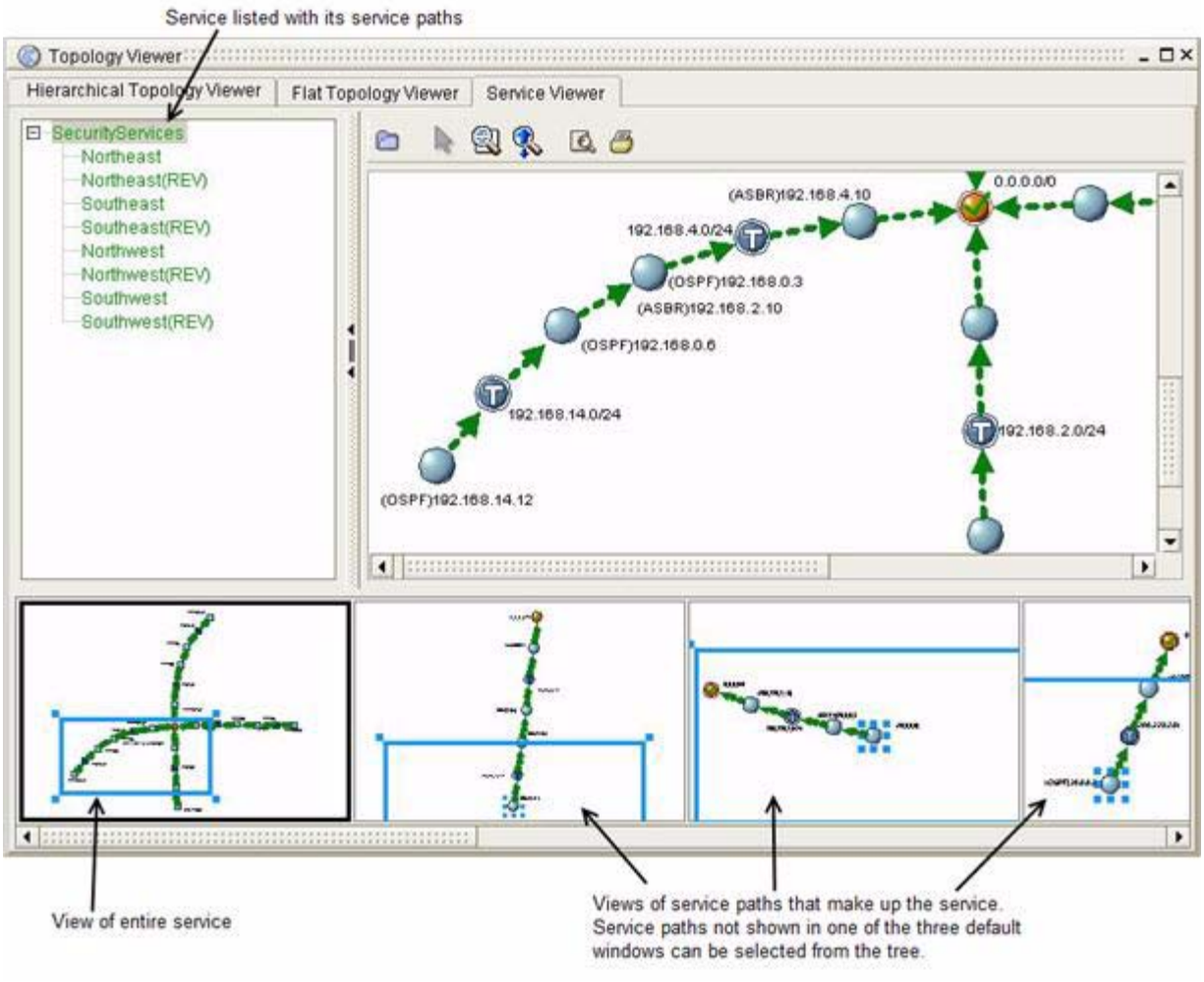
View the Service Viewer

In Path Analyzer, services represent the consumers of your data and applications. Consumers include people or departments, geographical locations, or nodes, including servers and routers, that rely on your network to obtain or receive the data, applications, or specialized services you provide (such as medical records, interactive billing and reimbursement forms, Internet-based music, and gaming applications).

After you configure a service and its related paths in Service Monitor (see Monitoring Unicast and Multicast Services on page 3-1), you can select the service from the hierarchical tree and view it in the Service Viewer.

Figure 2-4 shows the correlation between the hierarchical tree and the visual map of the service and its service paths.

Figure 2-4 Service Viewer



How Path Anaylzer Generates the Network Topology

Table 2-1 shows the process Path Analyzer uses to generate the topology and routing changes, called events, that occur between the multiple autonomous systems (AS's) of your network:

Table 2-1 How Path Anaylzer Generates the Multi-AS Topology

Protocol: BGP		
Component	**Task**	**Result**
Listener	**What:** Forms an adjacency with a BGP speaker... **Where:**...at the edge of an autonomous system.	Listener obtains all routing information exchanged between autonomous systems.
Listener	**What:** Sends BGP routing messages received from the adjacent BGP speaker... **Where:**...to the Path Analyzer Server.	Path Analyzer Server generates routing changes as events, and constructs the view of your network's topology across autonomous systems.
Path Analyzer Server	**What:** Persists all generated events for recorded real-time and historical event and topological data... **Where:**...in the Path Analyzer database.	Data is made available to modules of the Path Analyzer Management Console.
Management Console	**What:** Presents accurate, graphical view of routing topology that is superimposed on your network's physical topology... **Where:**...in the modules of the Path Analyzer Management Console.	Topology Viewer shows current, dynamic topology. The Historical Topology Viewer allows you to replay and watch historical, topological changes. Information about each type of topology element, such as the attributes of a topology element, or the external route advertisements associated with a router, are provided in the Topology Browser.

Table 2-2 shows the process Path Analyzer uses to generate the topology and routing changes, called *events*, that occur within an autonomous system of your network: These changes also occur within and between OSPF areas.

Table 2-2 How Path Anaylzer Generates the Multi-Area Topology

Protocol: OSPF		
Component	**Task**	**Result**
Listener	**What:** Forms an adjacency with an OSPF router... **Where:**...in the backbone of your network or in another high-volume area.	The Listener obtains all routing information exchanged within and between OSPF areas.
Listener	**What:** Sends OSPF routing messages, called Link State Advertisements (LSAs), received from the adjacent OSPF router... **Where:**...to the Path Analyzer Server.	Path Analyzer Server generates routing changes as events and constructs the view of your network's topology within and across OSPF areas.
Path Analyzer Server	**What:** Persists all generated events for recorded real-time and historical event and topological data... **Where:**... in the Path Analyzer database.	Data is made available to modules of the Path Analyzer Management Console.
Management Console	**What:** Presents an accurate, graphical view of routing topology that is superimposed on your network's physical topology. **Where:**...in the modules of the Path Analyzer Management Console.	Topology Viewer shows current, dynamic topology. Historical Topology Viewer allows you to replay and watch historical, topological changes as they recur. Information about each type of topology element, such as the attributes of a topology element, or the external route advertisements associated with a router, are provided in the Topology Browser.

Viewing Changes of Status

Network elements change status as conditions change. For example, if a router becomes unavailable and interrupts routing in your network, the Topology Viewer immediately depicts the change. The router and affected links are displayed in red to indicate the change.

Note To reduce the display of routers in the Topology Viewer, you can hide all unavailable routers or edge routers. See Hide and Show Routers and Topology Elements, page 2-43 for information.

Table 2-3 shows the following status changes displayed in the Topology Viewer and other modules of the Path Anaylzer Management Console.

Table 2-3 Status Changes Displayed in Topology Viewer

Status	Description
Available	Indicates that a router or interface is functioning properly without interrupting routing. Path Analyzer assigns an *Available* status to a topology element if the most recent LSA associated with the topology element indicates that the topology element is available on the network.
Unavailable	Indicates that the topology element is unavailable due to a misconfiguration, software issue, connectivity issue, or hardware problem, and that the issue has interrupted normal and expected routing functions. Path Analyzer assigns an *Unavailable* status to a router and its associated links if it becomes unavailable or disconnected from the network.

Identifying Topology Viewer Elements

Topology Viewer provides detailed information about the following elements of your network topology:

- Autonomous Systems, page 2-19
- Areas, page 2-20
- Routers, page 2-21
- OSFP Routes and Advertisements, page 2-25
- Networks and Subnets, page 2-29
- Interfaces and Links, page 2-30

Table 2-4 shows how each of these elements can be represented in the topology, depending on your preferences you select under the menu **Start > Preferences**. See Set Preferences, page 1-24.

The Topology Viewer uses two sets of icons:

- Geometric Node Icons—Rounded icons
- Network Node Icons—Rectangular icons

The sections following Table 2-1 provide detailed information about each element type and how to select and view information about an element in the topology.

Table 2-4 Topology Icons

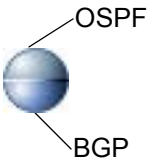
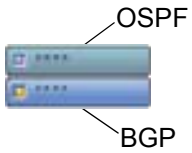
Topology Element	Geometric Node Icons	Network Node Icons
Autonomous System		
Area (green)		
Router—Path Analyzer supports BGP and OSPF routers and provides icons that indicate the router's type and status.		
BGP speaker, Available/Up (blue)		
BGP speaker, Unknown (gray)		
OSPF router Available/Up (blue)		
OSPF router Unavailable/Down (red)		
OSPF router Unknown (gray)		
Combined router: OSPF router with status Available/Up and BGP speaker with status Available/Up (blue/blue)		
Combined router: OSPF router with status Available/Up and BGP speaker with status Unknown (blue/gray)		

Table 2-4 Topology Icons (continued)

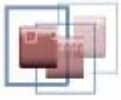
Topology Element	Geometric Node Icons	Network Node Icons
Combined router: OSPF router with status Unavailable/Down and BGP speaker with status Available/Up (red/gray)		
Combined router: OSPF router with status Unavailable/Down and BGP speaker with status Unknown (red/gray)		
Combined router: OSPF router with status Unknown and BGP speaker with status Available/Up (gray/blue)		
Combined router: OSPF router with state Unknown and BGP speaker with state Unknown (gray/gray)		
Area Border Routers (ABR) are representations of a router's interfaces in a border area. ABRs have three states—Available/Up, Unavailable/Down, and Unknown—and are represented by the following icons.		
ABR, Available/Up (blue)		
ABR, Available/Up (red)		

Table 2-4 Topology Icons (continued)

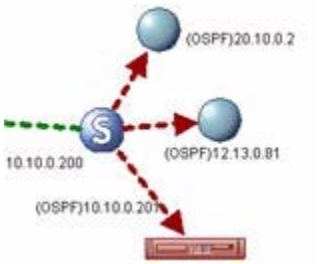
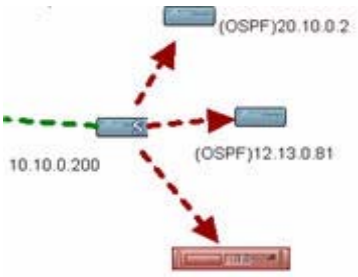
Topology Element	Geometric Node Icons	Network Node Icons
ABR, Unknown (gray)		
Multicast sources and routers have two states, Available/Up and Unavailable/Down, represented by the following icons.		
Source, Available/Up (blue)		
Source, Unavailable/Down (Icon = blue) (Link = red)		
Leaf router, Available/Up (blue)		
Leaf router, Unavailable/Down (red)		
Transit networks have three states—Available/Up, Unavailable/Down, and Unknown—and are represented by the following icons:		
Transit network, Available/Up (blue)		
Transit network, Unavailable/Down (red)		

Table 2-4 Topology Icons (continued)

Topology Element	Geometric Node Icons	Network Node Icons
Transit network, Unknown (gray)		
Stub Networks have three states—Available/Up, Unavailable/Down, and Unknown—and are represented by the following icons:		
Stub network, Available/Up (blue)		
Stub network, Unavailable/Down (red)		
Stub network, Unknown (gray)		
Routes—The following icons are used to represent Type 3 and Type 4 Summary Routes.		
Type 3 Summary Route, Available/Up (red/blue)		
Type 4 Summary Route, Available/Up (red/blue)		
External Routes have three states—Available/Up, Unavailable/Down, and Unknown, and are represented by the following icons.		
External Route, Available/Up (yellow+green check)		
External Route, Unavailable/Down (red+black x)		

Table 2-4 Topology Icons (continued)

Topology Element	Geometric Node Icons	Network Node Icons
External Route, Unknown (gray)		
Path Anaylzer Listeners have three states, Available/Up, Unavailable/Down, and Backup Listener. They are represented by the following icons.		
Available/Up (blue)		
Unavailable/Down (red)		
Backup Listener (yellow)		

Autonomous Systems

At the highest level of the network hierarchy, the Topology Viewer shows an enterprise-wide view of all autonomous systems. Each autonomous system is represented by the icons in Figure 2-5, listed with the name your Path Analyzer administrator provided during the initial configuration of your system.

Figure 2-5 Autonomous System Icons

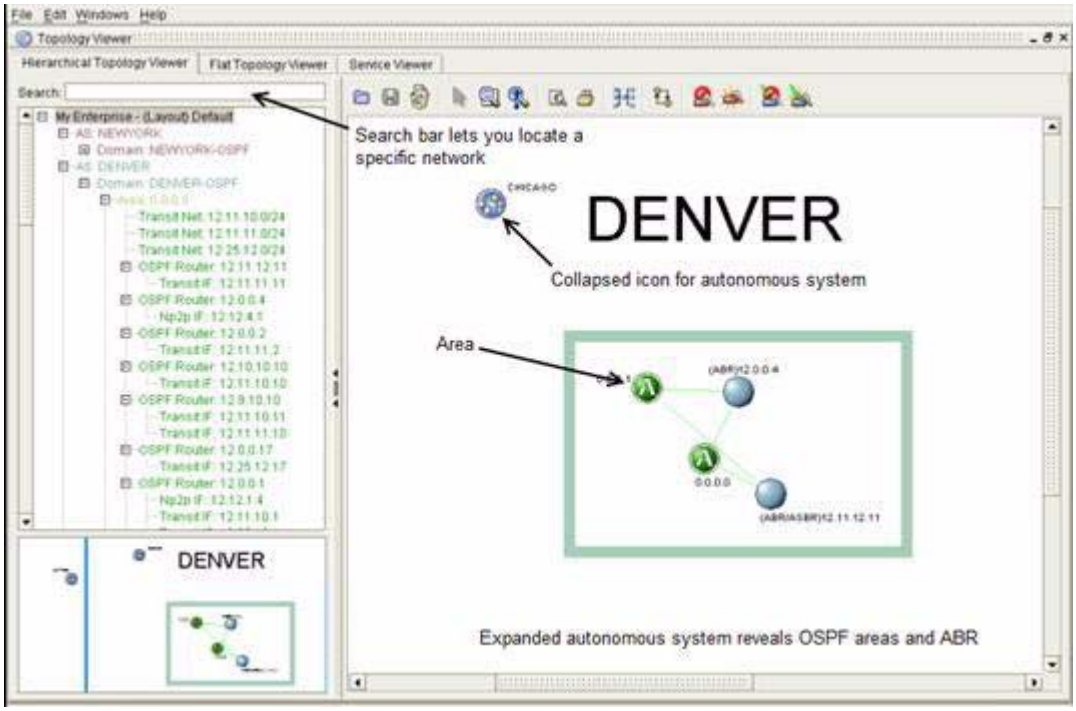
Autonomous Systems in the Topology Viewer

Figure 2-6 shows an autonomous system displayed as icons in the Topology Viewer. While autonomous systems are displayed as icons, their contents are hidden, and they are considered to be collapsed or closed.

Expanding an autonomous system reveals its subsystems, the OSPF areas in which routers forward data and exchange routing updates over a shared IGP, such as OSPF, iBGP, or IS-IS. The Topology Viewer presents information about routing that occurs over OSPF and iBGP.

Figure 2-6 also shows a view of the areas contained in the autonomous system. Right-clicking the collapsed icon of an autonomous system causes a menu to display, showing options to expand the autonomous system or an overview of its features in tabular form.

Figure 2-6 Expanded Autonomous System in Hierarchical Viewer



Related Tasks

- View Details of the Enterprise Network, page 2-54
- View All Autonomous Systems in the Enterprise Network, page 2-55
- View Details of an Autonomous System, page 2-55
- View Areas in a Domain, page 2-55
- View Details of an Area, page 2-56
- View All OSPF Routers in an AS, page 2-56
- View All OSPF Routes in an AS, page 2-60

Areas

Areas are logical clusters of routers that carry data to destination subnets over a shared routing protocol. These routers are grouped for easier administration. In the Topology Viewer, an area is represented by the icon in Figure 2-7.

Figure 2-7 Area Icons

Area Data and Metrics

Right-clicking an OSPF Area and selecting **Show Overview** opens a table that shows a total count of the routers, routes, and networks in the area. See View Details of an Area, page 2-56.

Related Tasks

- View Areas in a Domain, page 2-55
- View Details of an Area, page 2-56

Routers

In the Topology Viewer, depending on the Topology Viewer Settings you select from **Start > Preferences,** router icons are labeled to indicate the protocol the router uses and the type of router.

Routers that use only OSPF are labeled with OSPF on the router icon. Routers that use only BGP are labeled BGP. Specialized routers are labeled with the type of router.

Table 2-5 describes all routers presented in the Topology Viewer. For detailed information about icons used to represent routers in the Topology Viewer, see Table 2-4.

Table 2-5 Router Descriptions

Router Type	Description
Core or Internal Router	A router that serves one area; all of its interfaces are configured to support the transmission of information in the same OSPF area.
Backbone Router	Attaches to Area 0, the backbone, over one or more interfaces. Backbone routers that use OSPF are represented by the same icon as core routers.
Area Border Router (ABR)	Attaches to multiple OSPF areas.
Autonomous System Boundary Router (ASBR)	Attaches to and announces connectivity to another autonomous system.
Combined ABR/ASBR	Functions as an ABR and an ASBR.
BGP Router	Forwards packets over BGP only. **Note:** The concept of an Unavailable BGP router does not exist in Path Anaylzer.
BGP/OSPF Router	Forwards packets over OSPF and BGP interfaces.
BGP router and OSPF ABR on the same device	Forwards packets over OSPF and BGP interfaces and functions as an ABR, forwarding packets to more than one OSPF area.
BGP router and OSPF ASBR on the same device	Forwards packets over OSPF and BGP interfaces, and functions as an ASBR. Announces to OSPF routers in the same autonomous system its ability to form an adjacency with a BGP speaker.
BGP router and combined OSPF ABR/ASBR on the same device	Forwards packets over OSPF and BGP interfaces and functions as an ABR and ASBR.

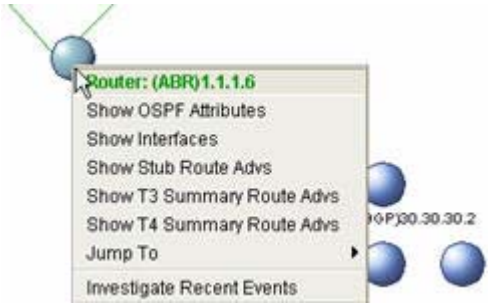
Related Tasks

- View All OSPF Routers in an AS, page 2-56
- View OSPF Interfaces for All Routers in an AS, page 2-57
- View Attributes of an OSPF Router, page 2-58
- View the Interfaces of a Specific OSPF Router, page 2-60
- View Route Advertisements Announced by a Specific Router, page 2-61

Router Attributes

Right-clicking a router and clicking **Show Attributes** allows you to view the attributes of a router, the number of interfaces, routes, and route advertisements. What is displayed depends on the type of router and your network configuration. Figure 2-8 shows OSPF attributes for an ABR router.

Figure 2-8 Show OSPF Attributes for an ABR Router

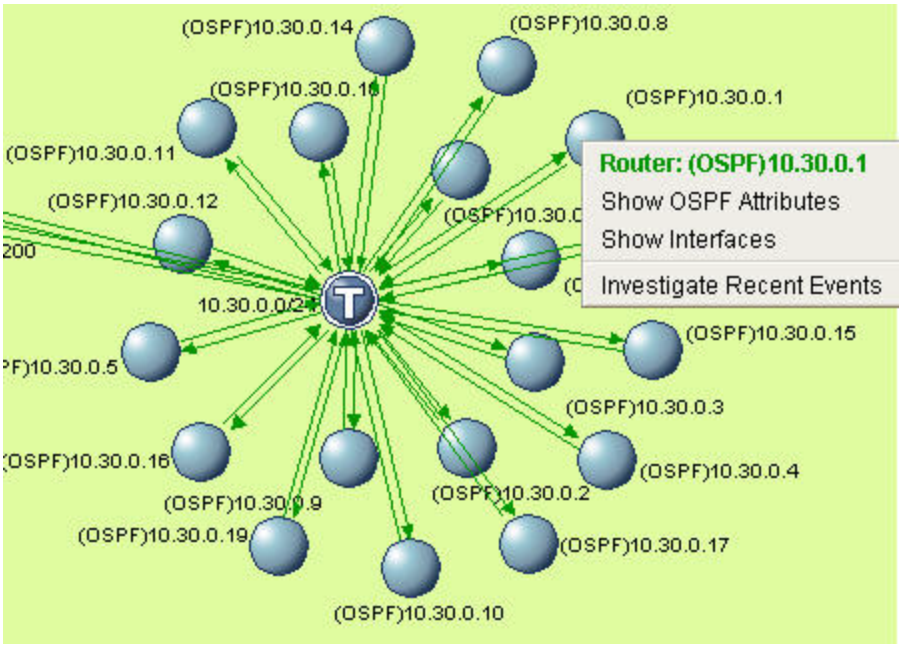


Router Interfaces

Right-clicking a router and selecting **Show Interfaces** allows you to view details about router interfaces, including the type of interface, status of an interface, IP address of a numbered router interface or Management Information Base (MIB) identifier for an unnumbered router interface. See View the Interfaces of a Specific OSPF Router, page 2-60 for the steps to take to view router interfaces.

Figure 2-9 shows interfaces for an ABR router.

Figure 2-9 Show Interface for a Router

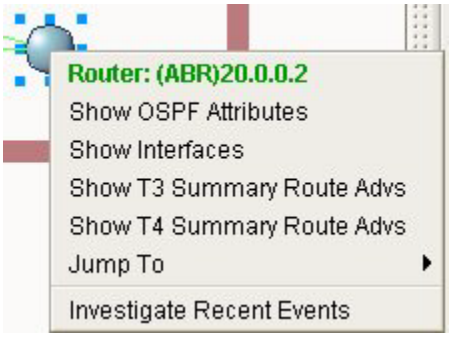


OSPF Route Advertisements

Right-clicking routers, such as ABRs and ASBRs, allows you to select additional options. For example, right-clicking an ABR provides options for viewing the Type 3 or 4 Summary advertisements of the router.

See View Route Advertisements Announced by a Specific Router, page 2-61 for instructions on viewing the routes associated with a router. Figure 2-10 shows router selections for an ABR.

Figure 2-10 Options of an ABR



All Routers

See View All OSPF Routers in an AS, page 2-56 for instructions on viewing a detailed list of all routers in your autonomous system or area of your network.

Show or Hide Routers

In the Flat and Hierarchical Topology Viewers, you can select options to show or hide unavailable or edge routers. See Hide and Show Routers and Topology Elements, page 2-43.

Hiding Unavailable Routers

If you take multiple routers off line simultaneously and do not want to view them while they are unavailable, it is convenient to hide them. When the routers become available, they are displayed as available routers in the Topology Viewer. If the routers become unavailable again, they are displayed as unavailable until you choose to hide them. The Hide option is a one-time, manual selection. You can hide routers any time they become unavailable.

Hiding Edge Routers

Edge routers connect to Transit networks. Hiding edge routers helps to limit your view of specific networks and remove clusters of routers that you do not want to see.

Routers and Area Nodes

In the Flat and Hierarchical Topology Viewers, every ABR is associated with at least one area node, a logical entity that represents the router as it exists in the area. The area node representation indicates that the ABR has a presence in an area and that one or more of its interfaces are bound to the area.

For information about the states of area nodes in the Topology Viewer, see Table 2-4.

Figure 2-11 shows Area Node ions.

Figure 2-11 Area Node Icons

The correlation between area nodes and router interfaces is not one to one. For example, a router that has three interfaces in Area 0 and three interfaces in Area 1 has only two area nodes: one in Area 0 and another in Area 1.

For information about the associated ABR for a given area node, see Jump to an ABR, page 2-41. For information about locating the interfaces of an ABR that reside in a specific area, see Jump to an Area from an Area Node, page 2-40.

Area Node Attributes

Right-clicking an area node and clicking **Show Attributes** allows you to view attributes of the area node, such as:

- ABR or combined ABR/ASBR to which the area node belongs
- Area in which the area node resides
- Number of router interfaces that the area node represents
- Status of the ABR or combined ABR/ASBR as it pertains to the area.
- Types and numbers of routes (Stub, External, T3 Summary, etc.)

See View OSPF Attributes of an Area Node, page 2-62 for detailed information.

OSFP Routes and Advertisements

The term *route* refers to the IP address and subnet mask of a possible destination to which a router can forward a packet. The destination of a route may be located in the same area as the advertising router, a different area, or in an external autonomous system. To view the icons that represent routes in the Topology Viewer, see Table 2-4.

Every router maintains a routing table that lists possible route advertisements for a destination. The routing table contains information about the cost of links to a destination, enabling the router to calculate the cost of a path and to select the correct interface over which to send a packet toward the destination.

In the Flat and Hierarchical Topology Viewers, you can view a tabular display of the route advertisements that belong to an available router. If the router becomes unavailable, menu selections related to its advertisements may also become unavailable.

Selections vary, depending on the type of router. For example, an ABR or combined ABR/ASBR can have Type 3 and Type 4 Summary Route Advertisements. Because an ASBR can announce routes to destinations in other autonomous systems, right-clicking an ASBR can provide selections for external routes advertisements announced in OSPF Type 5 Link State Advertisements (LSAs).

For example, Figure 2-12 shows the menu options of an ABR that has Type 3 and Type 4 Summary Route Advertisements.

Figure 2-12 Selections to Show Type 3 and 4 Summary Route Advertisements of an ABR

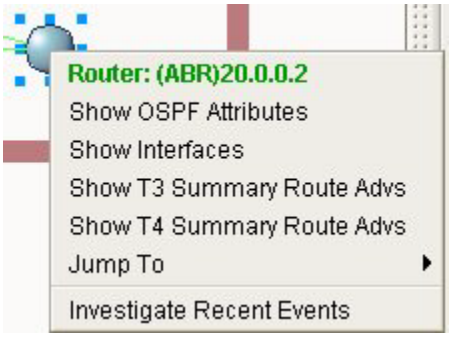


Figure 2-13 shows menu options of an ASBR that has External and Stub Route Advertisements.

Figure 2-13 Selection to Show External Route Advertisements of an ASBR

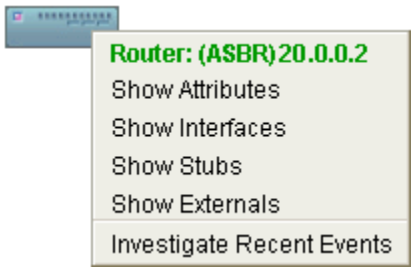


Table 2-6 Route Advertisements Displayed in the Topology Viewer

Advertise-ment type	Description	How to find Route Attributes
Type 3 Summary Route Advertisement	Represents a Type 3 Summary Route Advertisement. ABRs and combined ABR/ASBRs advertise Type 3 Summary routes to routers in the same area to inform them about routes in other areas of the same autonomous system.	Right-clicking an ABR or a combined ABR/ASBR causes the **Show T3 Summary Route Advs** option to be displayed. Selecting this option opens the T3 Summary Route Advertisements for OSPF Router Dialog Box, page 2-131.
Type 4 Summary Route Advertisement	Represents a Type 4 Summary Route Advertisement. ABRs and combined ABR/ASBRs advertise Type 4 Summary routes to all routers in the same area to inform about the cost of reaching an ASBR in another area.	Right-clicking an ABR or a combined ABR/ASBR causes the **Show T4 Summary Route Advs** option to be displayed. Selecting this option opens the T4 Summary Route Advertisements for OSPF Router Dialog Box, page 2-132.
External Route Advertisement	Represents a route to a network external to the autonomous system. To advertise external routes, ASBRs send Type 5 LSAs to all routers within the autonomous system, Type 5 LSAs are summaries of external routes.	Right-clicking an ASBR or a combined ABR/ASBR causes the **Show External Routes** option to be displayed. Selecting this option opens the External Route Advertisements for OSPF Router Dialog Box, page 2-133.
Stub Route Advertisement	Represents a route to a Stub network.	Right-clicking a router that has a connection to a host in a Stub network causes the **Show Stub Routes** option to be displayed. Selecting this option opens the Stub Route Advertisements for OSPF Router Dialog Box, page 2-135.

Viewing Routes from Uninstrumented Areas

In instrumented areas of your network, a router forms an adjacency with a Path Analyzer Listener, Path Analyzer Server, and Management Console. Uninstrumented areas are not installed with Path Analyzer. Figure 2-14 shows Type 3 Summary route icons.

Figure 2-14 Type 3 Summary Route Icons

ABRs announce Type 3 Summary Routes to routers in the same area to inform about destinations in other areas.

In the T3 Summary Route Advertisements for OSPF Router Dialog Box, page 2-131 of an ABR in your instrumented area, you can view Type 3 Summary Route advertisements received from ABRs in uninstrumented areas. You cannot view additional information about the uninstrumented areas.

ABRs in instrumented areas of your network likewise announce Type 3 Summary Route Advertisements to routers in uninstrumented areas. However, you cannot view the route advertisements in the uninstrumented area.

See View Route Advertisements Announced by a Specific Router, page 2-61 for information about viewing Type 3 Summary Route Advertisements.

Type 4 Summary Route Advertisements

ABRs announce Type 4 Summary routes to routers in the same area to advertise how to reach an ASBR Figure 2-15 shows Type 4 Summary route icons.

Figure 2-15 Type 4 Summary Route Icons

In the T4 Summary Route Advertisements for OSPF Router Dialog Box, page 2-132 of an ABR in your instrumented area, you can view Type 4 Summary Route advertisements received from ABRs in uninstrumented areas.

ABRs in instrumented areas of your network likewise announce Type 4 Summary Route Advertisements to routers in uninstrumented areas. However, you cannot view the route advertisements in the uninstrumented area.

See View Route Advertisements Announced by a Specific Router, page 2-61 for information about viewing Type 4 Summary Route Advertisements.

All Routes

See View All OSPF Routes in an AS, page 2-60 for the steps to take to view a detailed list of all possible route advertisements in your network topology.

Related Tasks

- View All OSPF Routes in an AS, page 2-60
- View Route Advertisements Announced by a Specific Router, page 2-61
- Query for an OSPF Route Advertisement, page 2-90

BGP Routes, Prefixes, and Prefix Families

You can right-click a BGP router and select any of the following menu choices to view detailed information about the routes associated with the router:

- **Show Bgp IpV4 Routes**—Opens the IPV4 Routes for a Router Dialog Box, page 2-142.
- **Show Bgp IpV4 Multicast Routes**—Opens the IPV4 Multicast Routes for a Router Dialog Box, page 2-144
- **Show Bgp Vpn Routes**—VPN Route List Dialog Box, page 2-145.

BGP prefixes (e.g., 10.4.29.1/24) are divided into three families: IPV4, IPV4 Multicast, and VPN.

For example, Figure 2-16 shows the menu options of a BGP router. Note that the menus displayed will depend on the routes associated with the individual router you have selected.

Figure 2-16 Menu Options of a BGP Router

BGP Filtering

The following BGP tables can be queried using the BGP Topology Filter wizard:

- Router Table
- IPV4 Prefix List
- IPV4 Multicast Prefix List
- IPV4 VPN Prefix List
- IPV4 Route List
- VPN Route List
- VRFs

See Using the Topology Filter Wizard for BGP Entities, page 2-65 and BGP Query Types and Constraints, page 2-66.

Related Tasks

- View All BGP Routers in an AS, page 2-57.
- View Attributes of a BGP Router, page 2-58.
- View All IPV4 Prefixes Within an AS for a BGP Router, page 2-58.
- View All IPV4 Multicast Prefixes Within an AS for a BGP Router, page 2-59.
- View All VPN Prefixes Within an AS for a BGP Router, page 2-59.
- View All IPV4 Routes Within an AS for a BGP Router, page 2-59.

- View All IPV4 Multicast Routes Within an AS for a BGP Router, page 2-59.
- View All VPN Routes Within an AS for a BGP Router, page 2-60.

Networks and Subnets

The Topology Viewer shows Transit networks graphically, as icons, and provides tabular information about Stub routes. To view the icons that represent the states of the Transit and Stub networks in Topology Viewer, see Table 2-4.

Transit Networks

In the Topology Viewer, Transit networks are represented by circular icons that contain a T (for Transit) in the center. Transit networks interconnect a set of routers, allowing data to pass through the network on the way to the destination host.

Figure 2-17 Transit Network Icons

Every OSPF Transit network has one *designated router* (DR) that:

- establishes adjacencies with all routers on the network
- broadcasts network link state advertisements to all routers on the network
- helps synchronize all routers on the network

Every Transit network also has a *backup designated router* (BDR) that takes over the DR's responsibilities if the DR becomes unavailable.

In the Topology Viewer, Transit networks are displayed as blue icons to represent an available or connected status and as red icons to represent an unavailable or disconnected status. Figure 2-17 shows Transit network icons used in the Topology Viewer. For information about the color of a topology element and its status, see Viewing Changes of Status, page 2-13.

Stub Networks

Stub networks allow data flow only for systems that are directly connected to the Stub network. Stub networks do not allow data transport through the network to destinations outside the Transit network. Routes to Stub networks are referred to as *Stub routes*, and are represented by icons in Figure 2-18.

Figure 2-18 Stub Network Icons

Information about a router's Stub route advertisements is provided in the Stub Route Advertisements for OSPF Router Dialog Box on page 2-135.

See View Route Advertisements Announced by a Specific Router, page 2-61 for information about how to view all route advertisements, including stub route advertisements for a selected router.

See Stub Route Advertisements for OSPF Router Dialog Box, page 2-135 for information about the fields and values provided for a stub route advertisement.

Network Attributes

Right-clicking a network and clicking **Show Attributes** enables you to view attributes of the network, such as the unique ID of the interface of the designated router.

Related Tasks

- View Attributes of a Transit Interface, page 2-62.
- View Attributes of a Transit-to-Router Link, page 2-63.
- View Attributes of a Numbered Point-to-Point (NP2P) Interface, page 2-63.
- View Attributes of an Unnumbered Point-to-Point (UP2P) Interface, page 2-63.

Interfaces and Links

In the Topology Viewer, arrows represent router-to-subnet, router-to-router, or subnet-to-router links. Links are visual representations of the next hop a packet takes over a router interface toward the destination. The direction of the arrows indicates how information flows between the end points of the link, for example, from a router to a Transit network.

Status of Links in the Topology Viewer

The color and appearance of a link can indicate the state of the link or user actions completed on the link. For example, a green link indicates that both end-points of the link are available and functioning properly.

Table 2-7 describes how colors are used to differentiate the status of links in the Topology Viewer.

Table 2-7 Status of Links in the Topology Viewer

Link Color	Description
Green	Individual or composite link is available.
Red	Individual link is unavailable. Composite link is unavailable in one direction.
Yellow	Composite link made up of multiple point-to-point links consists of available and unavailable individual links.
Heavy, Green, Dotted	A service path, displayed graphically in Service Monitor, is available and conforms to the set baseline. A heavy, green dotted line indicates availability and confirms that data flows across the set baseline. See Viewing Unicast Services Graphically, page 3-19.
Heavy, Red, Dotted	All or part of the configured baseline of a service or service path is unavailable.

Table 2-7 Status of Links in the Topology Viewer (continued)

Link Color	Description
Heavy, Yellow, Dotted	Due to the unavailability of the configured segment or entire baseline, the service or service path is transmitted over another segment. The re-routed transmission is displayed as a heavy, yellow dotted line. The affected service and related service paths are considered to be available but non-conforming to the set baseline. See Viewing Multicast Services Graphically, page 3-53 for information about the display of services and service paths in the Topology Viewer.
Heavy, Blue, Dotted	When a configured segment or entire baseline becomes unavailable and packets are forwarded over another path, the original, intended baseline is displayed as a heavy, blue dotted line.
Cyan	Links in a graphical service path are selected in response to a mouse click.

Link Attributes

The Topology Browser provides tabular information about attributes of a link.

For information about viewing the attributes of a link, see:

- View Attributes of a Transit Interface, page 2-62
- View Attributes of a Transit-to-Router Link, page 2-63
- View Attributes of a Numbered Point-to-Point (NP2P) Interface, page 2-63
- View Attributes of an Unnumbered Point-to-Point (UP2P) Interface, page 2-63

Table 2-8 Link Types and Link Attribute Dialog Boxes

Link Type	Description	Find Link Attributes in Topology Browser
Transit interface link	Link from a router to a Transit network.	Attributes for Transit Interface Dialog Box on page 2-124
Transit-to-Router link	Link from a Transit network to a router.	Attributes for Transit to Router Link Dialog Box on page 2-122
Numbered Point-to-Point Interface (NP2P)	Direct link between two routers. Router interfaces are identified by assigned, unique IP addresses.	Attributes for Numbered Point-to-Point Interface Dialog Box on page 2-122
Unnumbered Point-to-Point Interface (UP2P)	Direct link between two routers. Router interfaces are identified by unique Management Interface Base (MIB) index numbers.	Attributes for Unnumbered Point-to-Point Interface Dialog Box on page 2-123

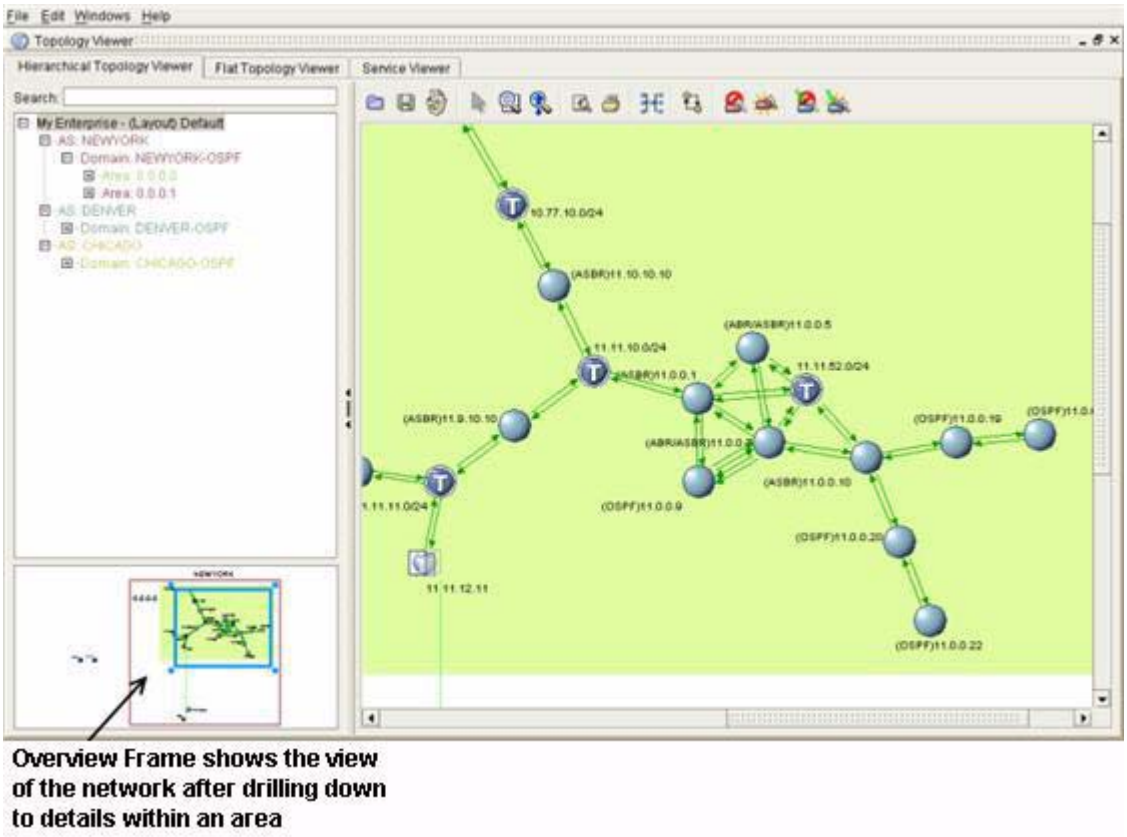
Related Tasks

- View Attributes of a Transit Interface, page 2-62
- View Attributes of a Transit-to-Router Link, page 2-63
- View Attributes of a Numbered Point-to-Point (NP2P) Interface, page 2-63
- View Attributes of an Unnumbered Point-to-Point (UP2P) Interface, page 2-63
- Issue a Fast Query, page 2-83
- Query for an OSPF Interface, page 2-84

Navigating in the Topology Viewer

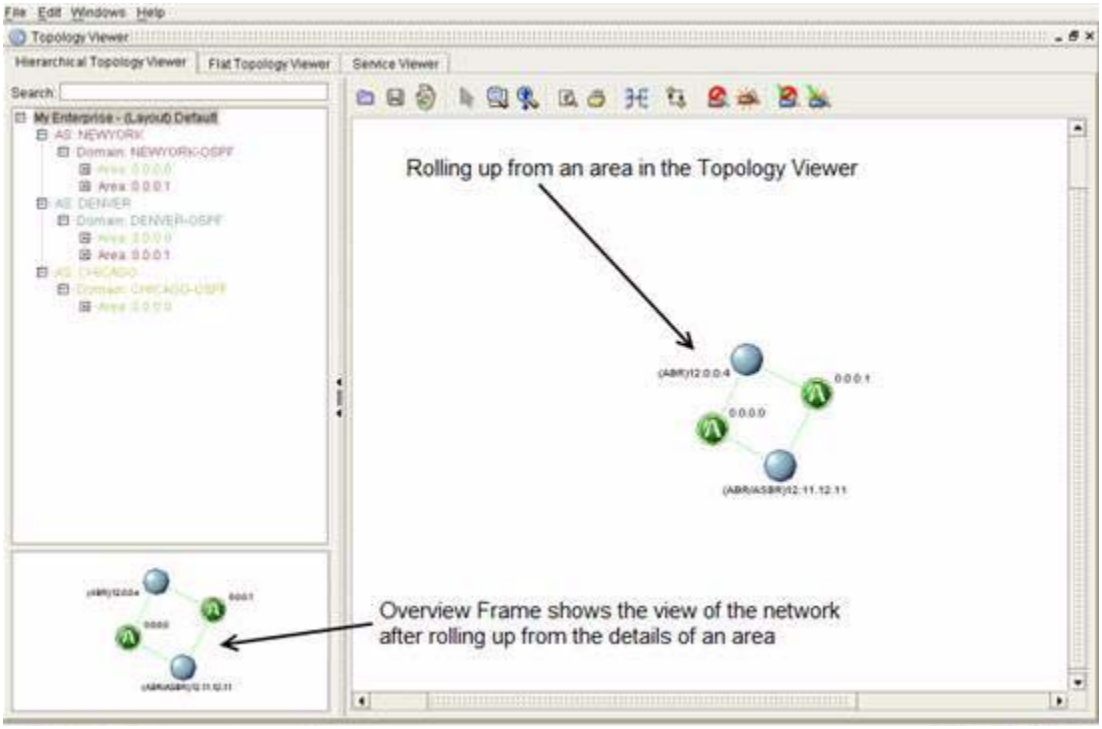
In the Topology Viewer, you can look at the contents of autonomous systems and areas by expanding or collapsing them. You can **Drill Down** to fill the Topology Viewer and Overview Frame with the selected autonomous system or area, as shown in Figure 2-19.

Figure 2-19 Drilled-Down View of a Network in Overview Frame and Topology Viewer



You can **Roll Up** to view an edge of the selected autonomous system or area, then drag the navigation box in the Overview Frame to view other parts of your network, as shown in Figure 2-20.

Figure 2-20 Rolled-Up View of a Network in Overview Frame and Topology Viewer



See Limit and Expand Your View of the Topology, page 2-38.

Navigate Using the Overview Frame

The Overview Frame contains a miniature overview of your multi-area network, resized to fit the dimensions of the frame.

Within the Overview Frame, you can move the navigation box to pan across the Topology Viewer to see different areas of your topology. You can also zoom in and out from the Overview Frame to change your view. For detailed information, see the following sections:

- Pan Across the Topology Viewer, page 2-34
- Zoom in Using the Overview Frame, page 2-35
- Resize the Topology Viewer, page 2-37

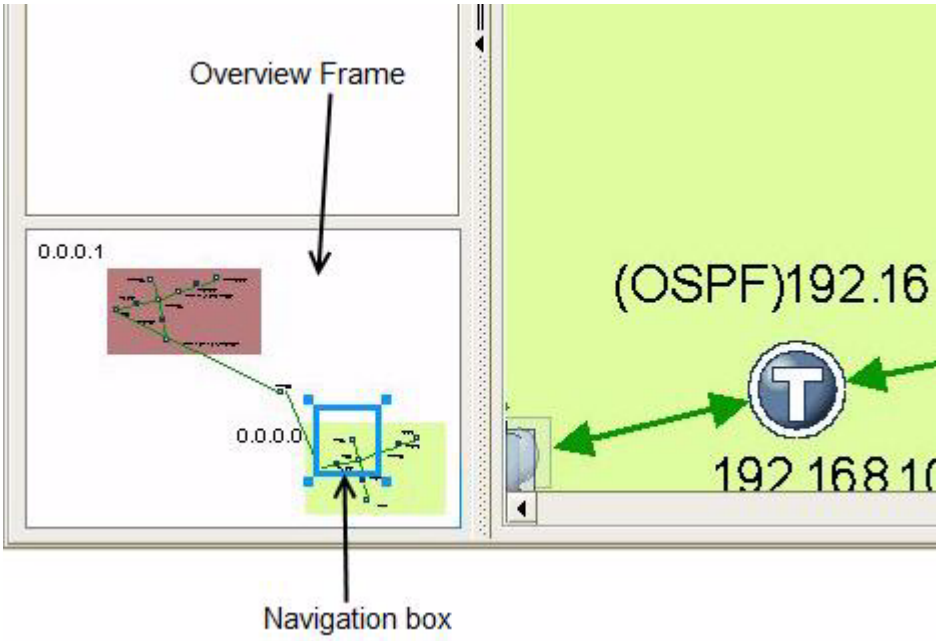
Pan Across the Topology Viewer

To pan across the Topology Viewer to view different areas of your topology:

Step 1 Click inside the navigation box in the Overview Frame.

The mouse pointer changes from an arrow shape to a hand. See Navigating in the Topology Viewer, page 2-32.

Figure 2-21 Overview Frame



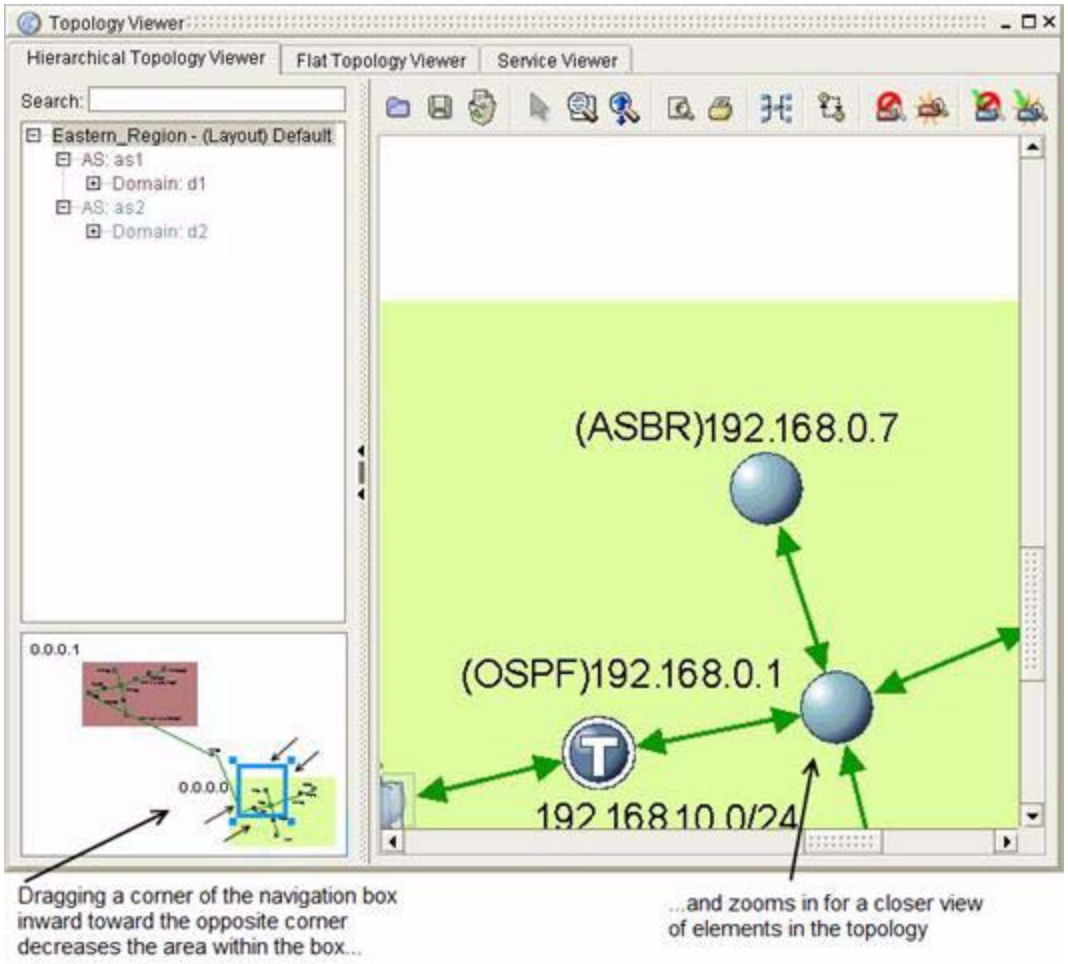
Step 2 Drag the navigation box to the desired portion of the Topology Viewer depicted in the Overview Frame (see Figure 2-21).

Step 3 Release the mouse button.

Zoom in Using the Overview Frame

Drag a corner of the navigation box inward toward the opposite corner to zoom in for a closer view of topology elements, as shown in Figure 2-22.

Figure 2-22 Zooming In with the Overview Frame

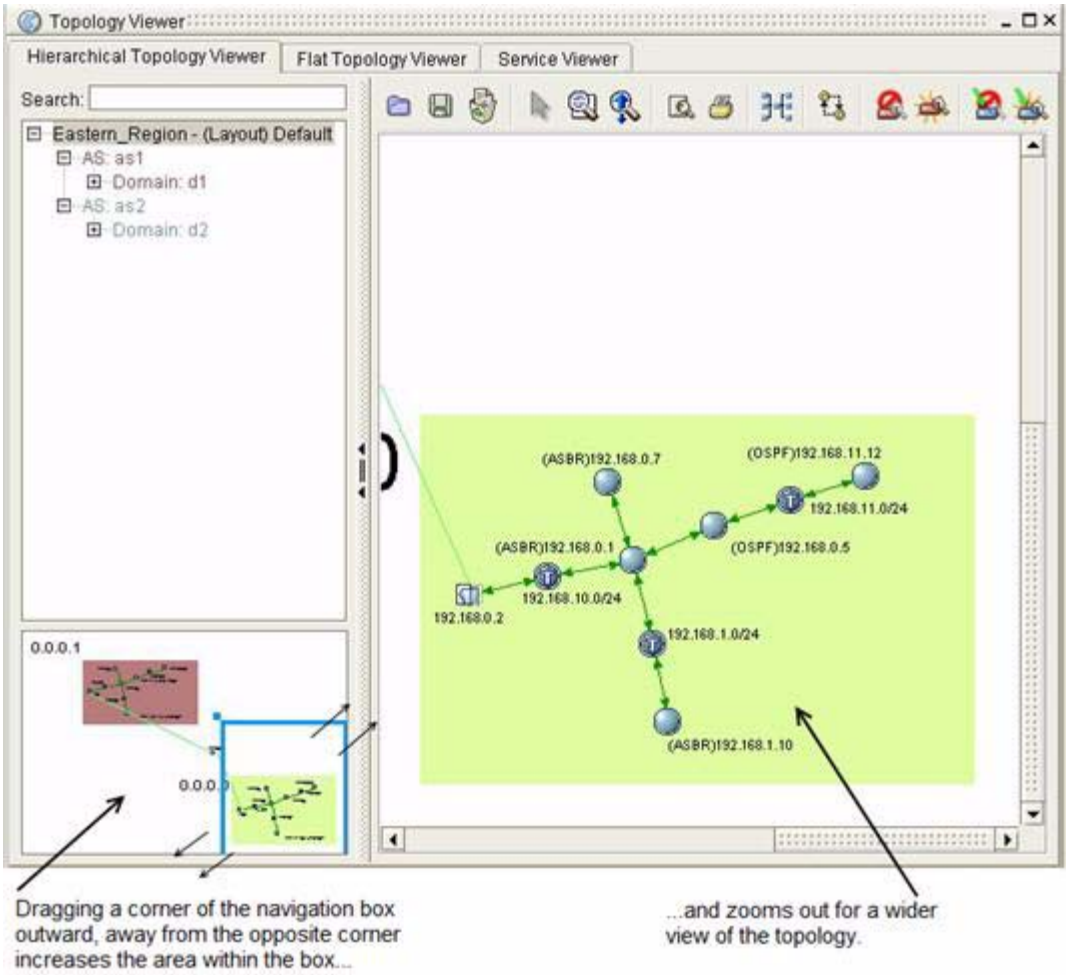


You can also zoom in or out from the Topology Viewer using controls in the toolbar. For information, see Navigating in the Topology Viewer, page 2-32 and Topology Viewer Toolbar, page 2-97.

Zoom Out Using the Overview Frame

Drag a corner of the navigation box outward, away from the opposite corner, to zoom out for a wider view of the topology, as shown in Figure 2-23.

Figure 2-23 Zooming Out with the Overview Frame



Zoom from the Toolbar

- To zoom in on a specific area of the Topology Viewer, click the **Zoom to Area** icon. Select the portion of the Topology Viewer to view more closely.

- To zoom in on a topology element, click the **Drag to Zoom** icon.

  Drag the zoom cursor in a downward motion by moving your mouse toward you, until you achieve the desired perspective.

- To zoom out from the Topology Viewer, click the **Drag to Zoom** icon. Drag the zoom cursor in an upward motion by moving your mouse away from you, until you achieve the desired viewing perspective. See Topology Viewer Toolbar, page 2-97.

Resize the Topology Viewer

To resize the Topology Viewer:

Step 1 Position your mouse over a corner or an edge of the Topology Viewer. The mouse pointer changes to a bi-directional arrow.

Step 2 Click a corner or an edge of the Topology Viewer.

Step 3 Drag the corner or edge of the Topology Viewer outward until the map increases to the desired size.

or

Drag the corner or edge of the Topology Viewer inward until the map decreases to the desired size.

Move Topology Viewer Elements

By changing the position of topology elements, including routers and networks, you can create a view of your network as you envision it.

Click the topology element you want to move, then drag it to its new location. You can also click and drag the label of a topology element.

Expand and Collapse Topology Elements

Expand an autonomous system or area to view its contents.

Expand an Autonomous System

To expand an autonomous system and view its contents:

Step 1 Right-click the autonomous system you want to expand.

Step 2 Select **Expand**. The contents of the autonomous system are displayed.

Collapse an Autonomous System

From the flat or hierarchical display of an expanded autonomous system, right-click and select **Collapse**. The icon of the autonomous system is displayed.

Expand an Area

This option is available if you previously expanded an autonomous system in the hierarchical view of the Topology Viewer.

To expand an area:

Step 1 Right-click the area you want to expand.

Step 2 Select **Expand**. The contents of the area are displayed.

Collapse an Area

Right-click inside the expanded area and select **Collapse**. The icon of the area is displayed.

Limit and Expand Your View of the Topology

After expanding an autonomous system or area, you can limit your viewing area of the network by:

- Double-clicking within the autonomous system or area

  or
- Right-clicking and selecting **Drill Down**.

Selecting the **Drill Down** option within an expanded autonomous system or area causes the selected autonomous system or area to take up the entire Overview Frame and Topology Viewer windows, providing you with a closer, narrower view of components that make up an area.

Drill Down

To drill down in an expanded autonomous system:

Step 1 Right-click within the autonomous system.

Step 2 Select **Drill Down**.

The Overview Frame and current window of the Topology Viewer show the selected autonomous system, providing a limited view of the network.

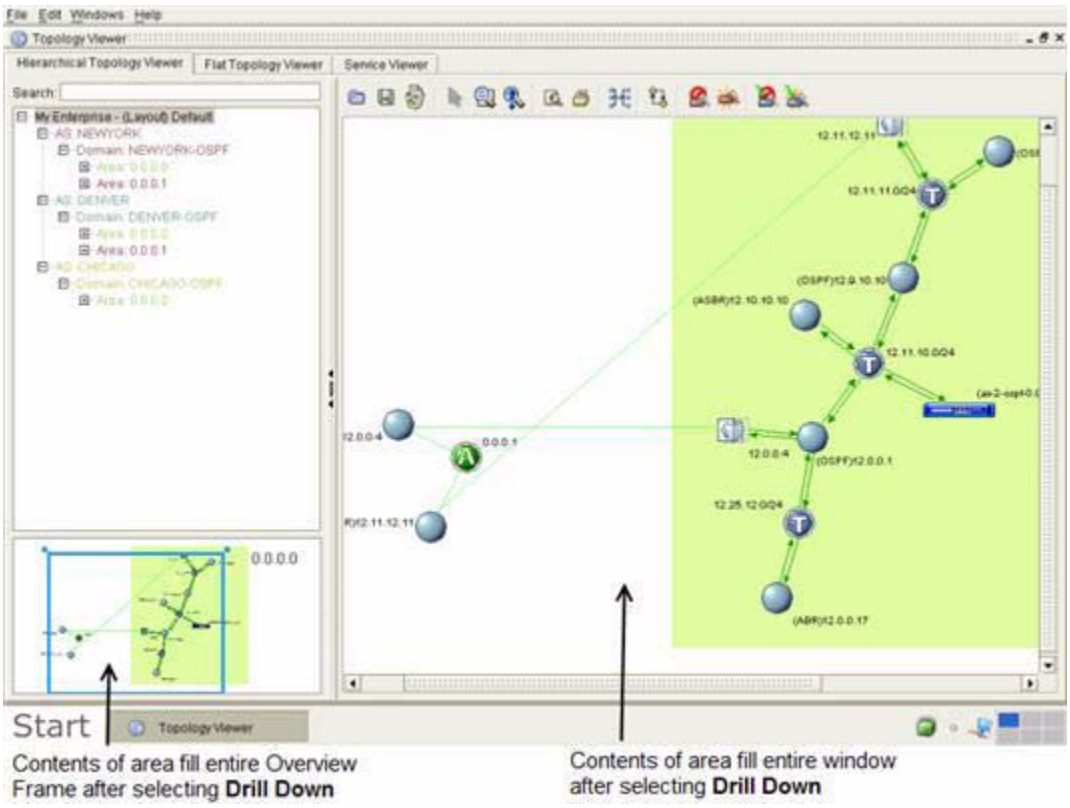
To drill down in an expanded area:

Step 1 Right-click within the area.

Step 2 Select **Drill Down**.

The Overview Frame and current window of the Topology Viewer show the selected area, providing a limited view of the network (see Figure 2-24).

Figure 2-24 Area View After Drilling Down



Roll Up

By selecting the **Roll Up** option within an expanded autonomous system or area, you can adjust the viewing area to include the entire network topology.

To roll up in an expanded autonomous system:

Step 1 Right-click within the autonomous system.

Step 2 Select **Roll Up**.

The Topology Viewer includes the entire network topology. You can use the scroll bars or Overview Frame to navigate out of the current autonomous system and view other portions of your network.

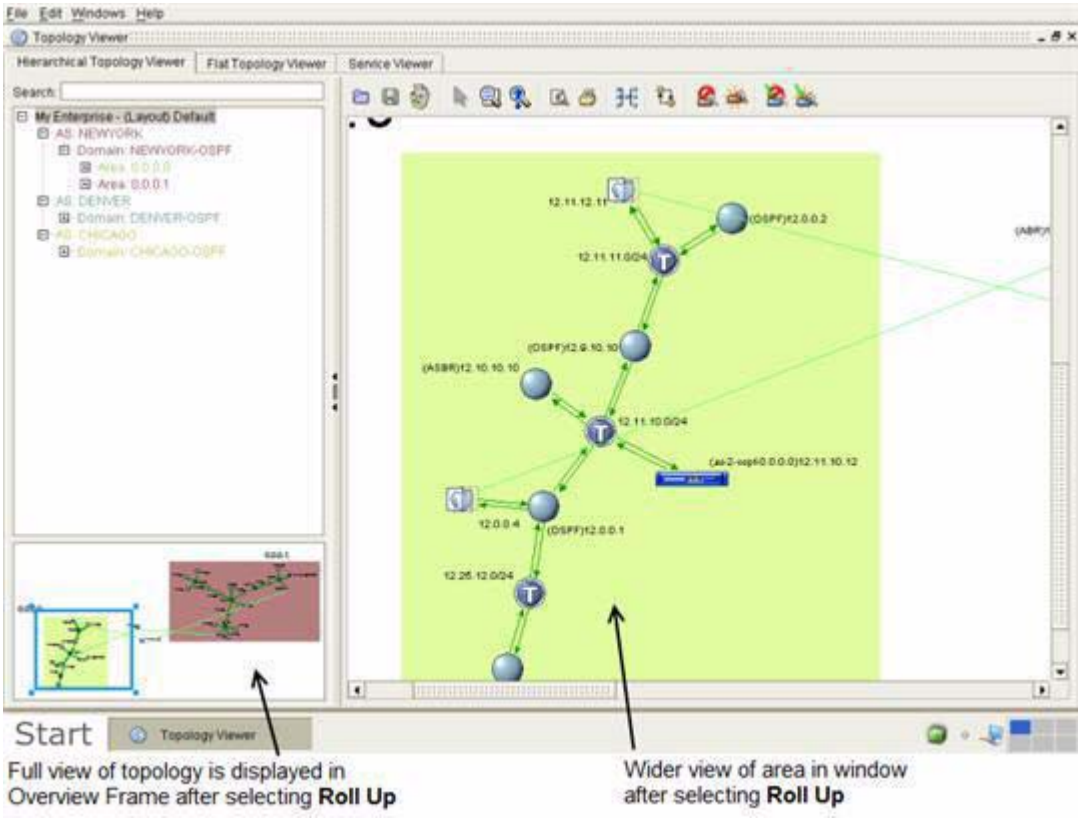
To roll up in an expanded area:

Step 1 Right-click within the area.

Step 2 Select **Roll Up**.

The Topology Viewer view includes the entire network topology (see Figure 2-25). You can use the scroll bars or Overview Frame to navigate out of the current area and view other portions of your network.

Figure 2-25 Area View After Rolling Up



Change Location from an Area Node

In the Topology Viewer, you can jump from an area node (via an ABR that has interfaces in another area) to another area, or a router in another area.

Jump to an Area from an Area Node

To jump to an area from an area node:

Step 1 In the hierarchical Topology Viewer, right-click the area node of an ABR that has interfaces in another area.

Step 2 Click **Jump To** > **Area <IP_Address>**, where <*IP_Address*> is the area identifier in the format of an IP address.

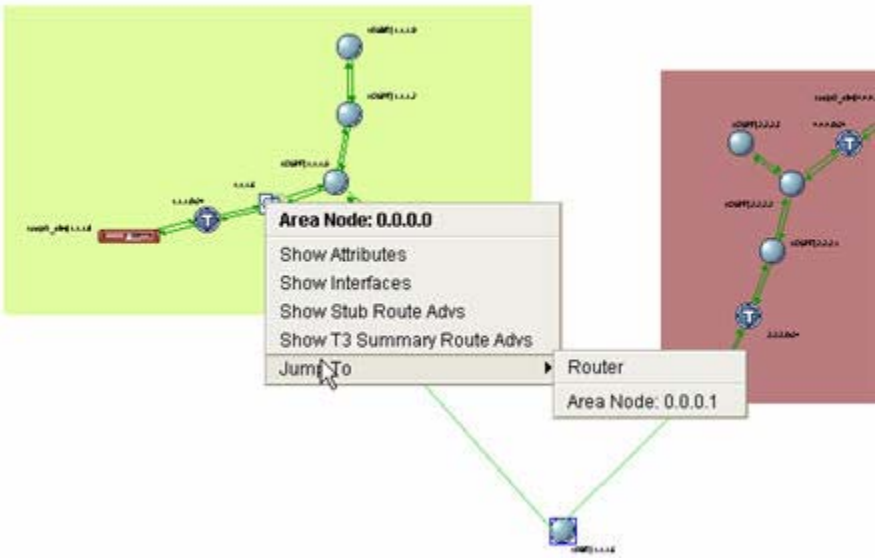
Jump to an ABR

To jump from an area node to a router:

Step 1 In the hierarchical Topology Viewer, right-click the area node of an ABR that has interfaces in another area.

Step 2 Click **Jump To** > **Router** (see Figure 2-26).

Figure 2-26 Jump-To Menu for ABR



The ABR associated with the area node is displayed in the Topology Viewer.

Change the Layout of the Topology Viewer

The Topology Viewer has a set structure that affects how components, such as routers and networks, are arranged in an expanded autonomous system or area. You can drag and drop topology elements to change their placement in the Topology Viewer. Refreshing the display causes topology elements to return to their original locations according to the structure of the Topology Viewer.

Refresh the Layout

To refresh the layout of the Topology Viewer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Click the **Refresh Layout** icon  in the Topology Viewer Toolbar, page 2-97.

You are prompted to confirm your choice.

Step 3 Click **Yes**.

The layout presented in the current Topology Viewer is updated using the default settings that arrange the layout of topology elements.

Save a Topological Layout

After positioning topology elements, you can save the layout and re-use it later.

Save the Layout

To save a layout of the Topology Viewer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Move topology elements, such as routers and Transit networks, to locations where you want to view them.

Step 3 Click the **Save Current Layout** icon  in the Topology Viewer Toolbar, page 2-97.

The Choose a Layout to Save Dialog Box, page 2-102 appears.

Step 4 Enter a name for the new configuration in the Layout Name field.

Step 5 Click **Save**.

For information about showing a saved layout, see Set the Default Flat Layout, page 1-25.

Remove a Topological Layout

You can remove a topological layout from the Flat or Hierarchical Topology Viewers when you do not want to use the layout.

Remove a Layout

To remove a topological layout from the Topology Viewer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Click the **Remove Layout** icon  in the Topology Viewer Toolbar, page 2-97.

The Choose a Layout to Remove Dialog Box, page 2-103 appears.

Step 3 Select the layout to remove from the list of layouts.

or

Step 1 Enter the name of the layout to remove in the Layout Name field.

Step 2 Click **Remove**. The name of the layout is removed from the Choose a Layout to Remove dialog box and the Topology Viewer. The name of the previous layout appears at the top of the hierarchical tree in the Topology Viewer until you Apply a New Layout or exit and restart the Path Anaylzer Management Console.

Apply a Topological Layout

To apply a saved layout to the Topology Viewer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Click the **Apply Layout** icon  in the Topology Viewer Toolbar, page 2-97.

The Choose a Layout to Apply Dialog Box, page 2-102 appears.

Step 3 Select the layout to apply from the list of layouts.

or

Enter the name of the layout to apply in the Layout Name field.

Step 4 Click **Apply**.

The new layout is applied. Its name appears at the top of the hierarchical tree in the Flat Topology Viewer.

Hide and Show Routers and Topology Elements

Hiding routers is useful when you wish to view a specific set of routers. You can hide unavailable routers and edge routers.

When to Hide Unavailable Routers

You can identify a the point of failure for a routing error. You can hide unavailable routers or networks to limit your view to the affected router or network.

Hide Unavailable Elements

To hide unavailable routers or networks in the Topology Viewer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Click the **Hide Unavailable Elements** icon  in the Topology Viewer Toolbar, page 2-97.

Unavailable routers, networks, and links that were displayed previously are hidden from view.

Show Unavailable Elements

To show unavailable routers or networks in the Topology Viewer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Click the **Show Unavailable Elements** icon  in the Topology Viewer Toolbar, page 2-97.

Unavailable routers, networks, and links that were hidden previously are displayed in the maps of the Topology Viewer.

Note These changes do not propagate across all maps of the Topology Viewer. If you select to hide unavailable elements in the Flat Topology Viewer, click Hide Unavailable Elements in the Hierarchical Topology Viewer to make the change take effect in both maps.

When to Hide Edge Routers

Edge routers receive data from and forward data to a network, often over a single link. You can hide edge routers to decrease the number of routers displayed so that you can focus on the core routers in your network.

Hide Edge Routers

To hide edge routers in the Topology Viewer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Select **Hide Edge Routers**  from the Topology Viewer Toolbar, page 2-97.

Edge routers are hidden for all networks displayed in the current map.

Show Edge Routers

To show edge routers in the Topology Viewer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Select **Show Edge Routers**  from the Topology Viewer Toolbar, page 2-97.

Edge routers that were hidden previously are displayed in the current map.

Note These changes do not propagate across all maps of the Topology Viewer. If you choose to hide unavailable elements in the Flat Topology Viewer, click Hide Unavailable Elements in the Hierarchical Topology Viewer to make the change take effect in both maps.

Viewing Services in the Service Viewer

The Service Viewer shows details of a service you previously created in Service Monitor. Selecting a service or service path from the hierarchy in the left side of the Service Viewer presents a view of the service in the right side of the window.

See Figure 2-3 for a view of a service and its service paths displayed in the Service Viewer.

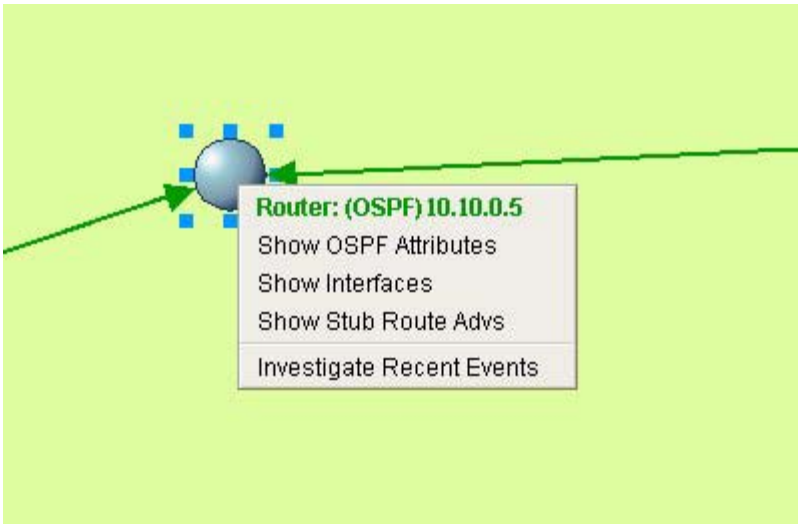
Getting Detailed Information About Topology Viewer Elements

Topology Viewer provides the Topology Browser dialog boxes, which allow you to delve deeper for information about a topology element while maintaining a high-level view of your network.

When you right-click a router, network, or link presented in the Topology Viewer, you receive a menu of options. Options vary depending on the type of network element. For example, the options of an OSPF router, which may have multiple interfaces and links to transit or Transit networks, differ from options for an ABR, which announces Type 3 and Type 4 Summary Routes within an area.

Figure 2-27 shows the list of options that can be displayed when you right-click an OSPF router.

Figure 2-27 Options Displayed After Right-Clicking an OSPF Router



Selecting an option from the list opens a Topology Browser dialog box that contains related data. In Figure 2-27 Clicking the **Show OSPF Attributes** command of an OSPF router opens the Attributes for OSPF Router dialog box of the selected ABR, shown in Figure 2-28.

Figure 2-28 Attributes for OSPF Router Dialog Box

Attributes for OSPF Router 169.185.96.74 in Domain 33464-Area0

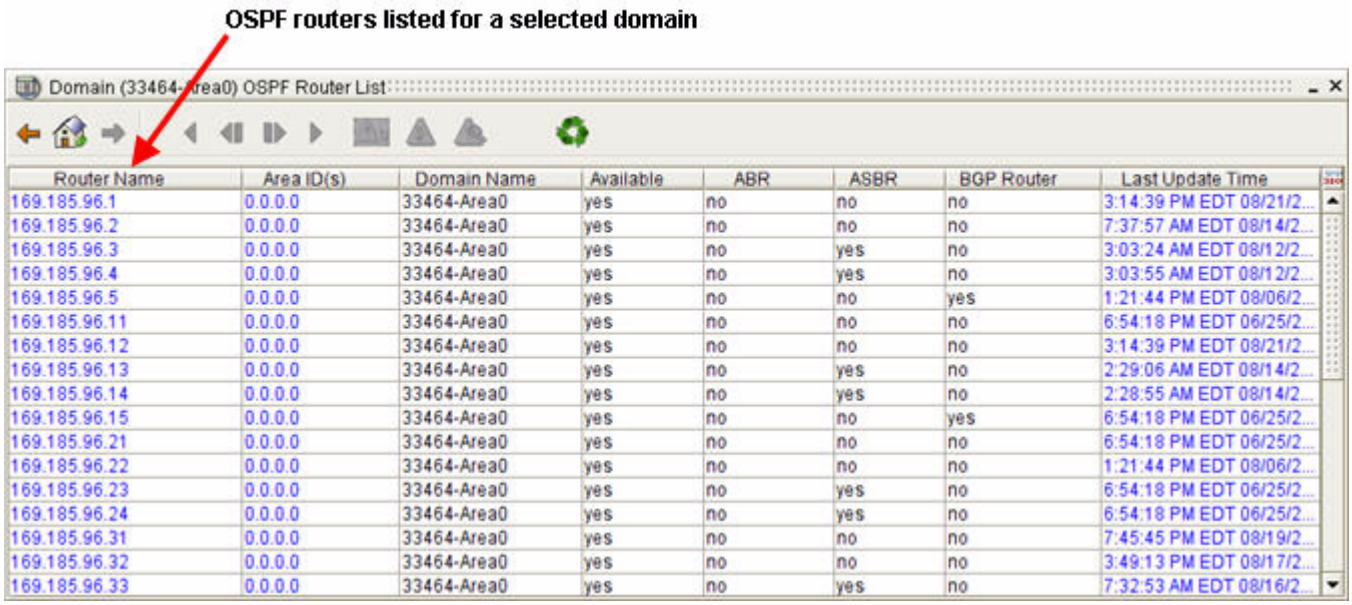
Attribute	Value
OSPF Router ID	169.185.96.74
DNS Name	N/A
User Defined Name	169.185.96.74
Area ID(s)	0.0.0.0
Domain Name	33464-Area0
Available	yes
ABR	no
ASBR	yes
AS Name	N/A
BGP Router ID	N/A
NP2P Interface Count	3
UP2P Interface Count	0
Transit Interface Count	0
Stub Route Advertisement Count	29
External Route Advertisement Count	2
T3 Summary Route Advertisement Count	0
T4 Summary Route Advertisement Count	0
Static Route Count	0
Last Update Time	12:39:56 AM EDT 07/28/2007

Link to Additional Information

Within all Topology Browser dialog boxes, values related to data in other Topology Browser dialog boxes are displayed as blue links. Clicking a link causes the corresponding dialog box to open and display related information about the item you selected.

For example, clicking the router link, 10.10.0.1, listed in the Router Name field of the Domain OSPF Router List dialog box in Figure 2-29, opens the Attributes for OSPF Router Dialog Box, page 2-119.

Figure 2-29 OSPF Router List Dialog Box

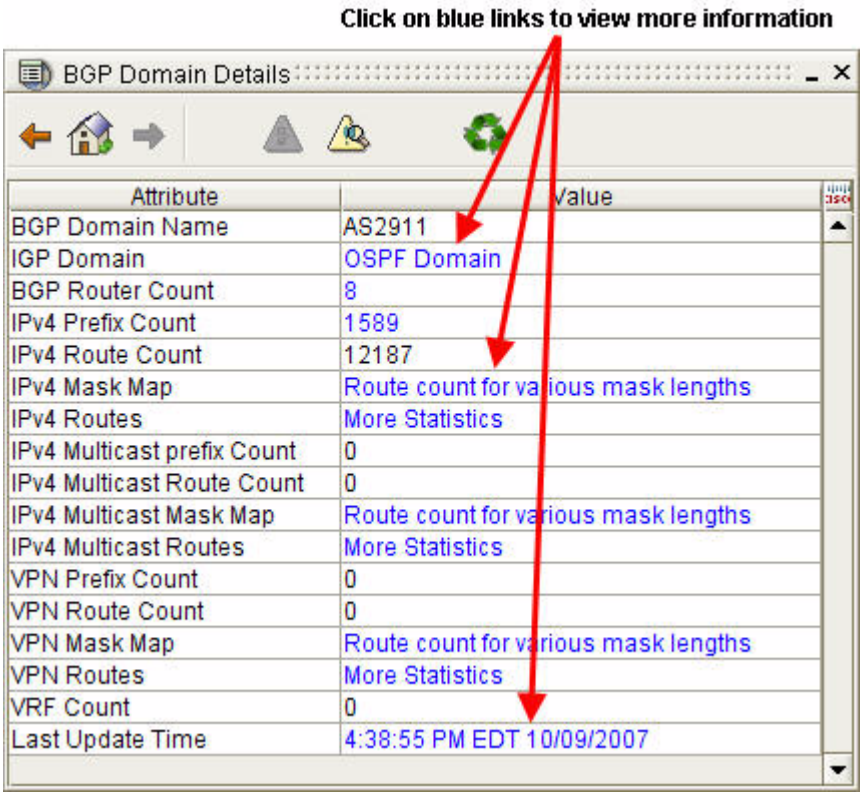


For detailed information about the components of the Topology Browser dialog boxes, see Topology Browser Dialog Boxes, page 2-99.

Navigating in Topology Browser Dialog Boxes

Topology Browser dialog boxes allow you to view information in up to ten dialog boxes simultaneously, an example of which is shown in Figure 2-30.

Figure 2-30 Attributes for OSPF Router Dialog Box



Clicking a blue link in a Topology Browser dialog box causes the related dialog box to be displayed in place of the previous one. The Browse Backward button becomes active, enabling you to browse backward or forward through the series of open dialog boxes.

Browse Backward

From the Topology Browser toolbar, click the **Browse Backward** icon.

The previous dialog box in the series appears. For additional information, see Getting Detailed Information About Topology Viewer Elements, page 2-45.

Browse Forward

From the Topology Browser toolbar, click the **Browse Forward** icon:

The next dialog box in the series appears. For additional information, see Getting Detailed Information About Topology Viewer Elements, page 2-45.

Note The Browse Forward icon is inactive until you click the Browse Backward icon. The active Browse Forward icon indicates that more than one dialog box is open, and you can browse forward through the series.

Get First, Previous, Last, and Next Entities

The **Get First Entities, Get Previous Entities, Get Last, Entities** and **Get Next Entities** icons are active when the number of items in a dialog box list exceeds the number of items you have specified using the icon for Select the Number of Rows to Display, page 2-50.

From the Topology Browser toolbar, click the **Get First Entities** icon:

The first "x" entities will be displayed (where x is the number of entities specified using the icon for Select the Number of Rows to Display, page 2-50).

For additional information, see Table 2-2.

From the Topology Browser toolbar, click the **Get Previous Entities** icon:

The previous "x" entities will be displayed (where x is the number of entities specified using the icon for Select the Number of Rows to Display, page 2-50).

For additional information, see Table 2-2.

From the Topology Browser toolbar, click the **Get Last Entities** icon:

The last "x" entities will be displayed (where x is the number of entities specified using the icon for Select the Number of Rows to Display, page 2-50).

For additional information, see Table 2-2.

From the Topology Browser toolbar, click the **Get Next Entities** icon:

The next "x" entities will be displayed (where x is the number of entities specified using the icon for Select the Number of Rows to Display, page 2-50).

For additional information, see Table 2-2.

Enterprise Overview

You get an overview of the enterprise by clicking on the **Go to Enterprise Overview** icon.

From the Topology Browser toolbar, click the **Go to Enterprise Overview** icon:

The following information is displayed:

- Enterprise ID
- Total BGP Domain Count
- Total BGP Router Count

Select the Number of Rows to Display

When a table appears in a Topology Browser Dialog box (See Figure 2-31 on page 2-52) you can select the number of rows to display in the table. This is helpful when there are a large number of table entries.

From the Topology Browser toolbar, click the **Select the Number of Rows to Display** icon.

The Select the limit Topology Browser Dialog box appears. Enter the number of rows to display (5-100) and click **OK**.

Specify the Filter for the Current Table

You can find specific data in a Topology Browser Dialog box table by using the filter icon.

From the Topology Browser toolbar, click the **Specify a Filter for the Current Table** icon.

You are then presented with a series of screens to complete. Use these screens to filter the table for the specific information you are seeking. The particular screens that appear will depend on the nature of the table you are viewing.

See Using the Topology Filter Wizard for BGP Entities, page 2-65.

Router Information Base (RIB) Comparison

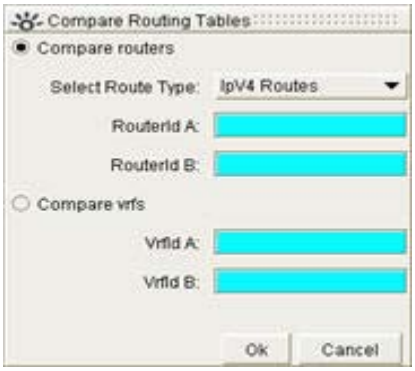
You can compare routing tables for the following kinds of routes:

- IPv4 routes
- IPv4 Multicast routes
- IPv4 VPN routes

within a specific domain, using the **RIB Comparison** icon in a Topology Browser Dialog box table.

From the Topology Browser toolbar, click the **RIB Comparison** icon.

The Compare Routing Tables Topology Browser Dialog box appears.



You can compare either Routers IDs or Virtual Routing and Forwarding (VRF) IDs. See Making Routing Information Base (RIB) Comparisons for BGP Routes, page 2-81.

Refresh Results

You can refresh the results in a Topology Browser Dialog box using the **Refresh Results** icon.

From the Topology Browser toolbar, click the **Refresh Results** icon.

Derive New Topology Query

The **Derive New Topology Query** icon is only available when you use the Investigative Topology Browser. It appears on any Topology Browser Query results box. You can use it to set up another query. See Querying for Network Elements (for OSPF Entities), page 2-82 to learn about the Investigative Topology Browser.

From the Topology Browser toolbar, click the **Derive New Topology Query** icon.

See Use a Query as a Template for a New Query, page 2-94.

Sort Data in a Column

The Topology Browser dialog boxes often provide long lists of information across several columns. You can sort the data values listed in the columns in increasing or decreasing order to find information more easily.

Clicking the first row of each Topology Browser dialog box sorts the content in the column and provides the Sort icon to indicate an increasing or decreasing sort (see Figure 2-31).

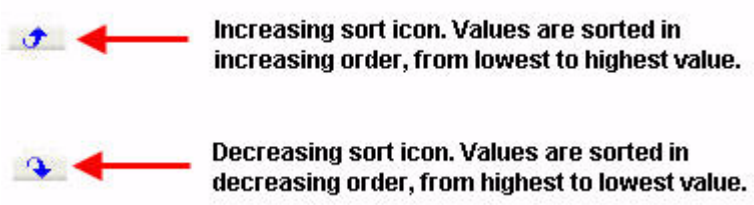
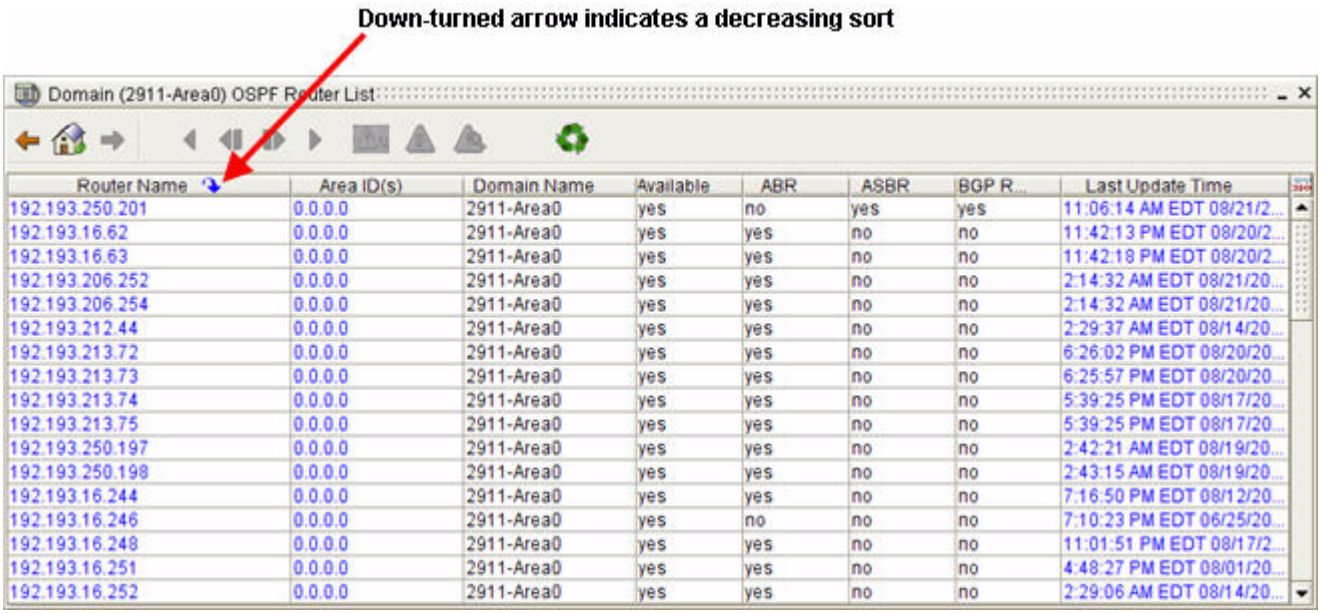


Figure 2-31 Router Names Arranged in Decreasing Value in Router List



Router Name	Area ID(s)	Domain Name	Available	ABR	ASBR	BGP R...	Last Update Time
192.193.250.201	0.0.0.0	2911-Area0	yes	no	yes	yes	11:06:14 AM EDT 08/21/2...
192.193.16.62	0.0.0.0	2911-Area0	yes	yes	no	no	11:42:13 PM EDT 08/20/2...
192.193.16.63	0.0.0.0	2911-Area0	yes	yes	no	no	11:42:18 PM EDT 08/20/2...
192.193.206.252	0.0.0.0	2911-Area0	yes	yes	no	no	2:14:32 AM EDT 08/21/20...
192.193.206.254	0.0.0.0	2911-Area0	yes	yes	no	no	2:14:32 AM EDT 08/21/20...
192.193.212.44	0.0.0.0	2911-Area0	yes	yes	no	no	2:29:37 AM EDT 08/14/20...
192.193.213.72	0.0.0.0	2911-Area0	yes	yes	no	no	6:26:02 PM EDT 08/20/20...
192.193.213.73	0.0.0.0	2911-Area0	yes	yes	no	no	6:25:57 PM EDT 08/20/20...
192.193.213.74	0.0.0.0	2911-Area0	yes	yes	no	no	5:39:25 PM EDT 08/17/20...
192.193.213.75	0.0.0.0	2911-Area0	yes	yes	no	no	5:39:25 PM EDT 08/17/20...
192.193.250.197	0.0.0.0	2911-Area0	yes	yes	no	no	2:42:21 AM EDT 08/19/20...
192.193.250.198	0.0.0.0	2911-Area0	yes	yes	no	no	2:43:15 AM EDT 08/19/20...
192.193.16.244	0.0.0.0	2911-Area0	yes	yes	no	no	7:16:50 PM EDT 08/12/20...
192.193.16.246	0.0.0.0	2911-Area0	yes	no	no	no	7:10:23 PM EDT 06/25/20...
192.193.16.248	0.0.0.0	2911-Area0	yes	yes	no	no	11:01:51 PM EDT 08/17/2...
192.193.16.251	0.0.0.0	2911-Area0	yes	yes	no	no	4:48:27 PM EDT 08/01/20...
192.193.16.252	0.0.0.0	2911-Area0	yes	yes	no	no	2:29:06 AM EDT 08/14/20...

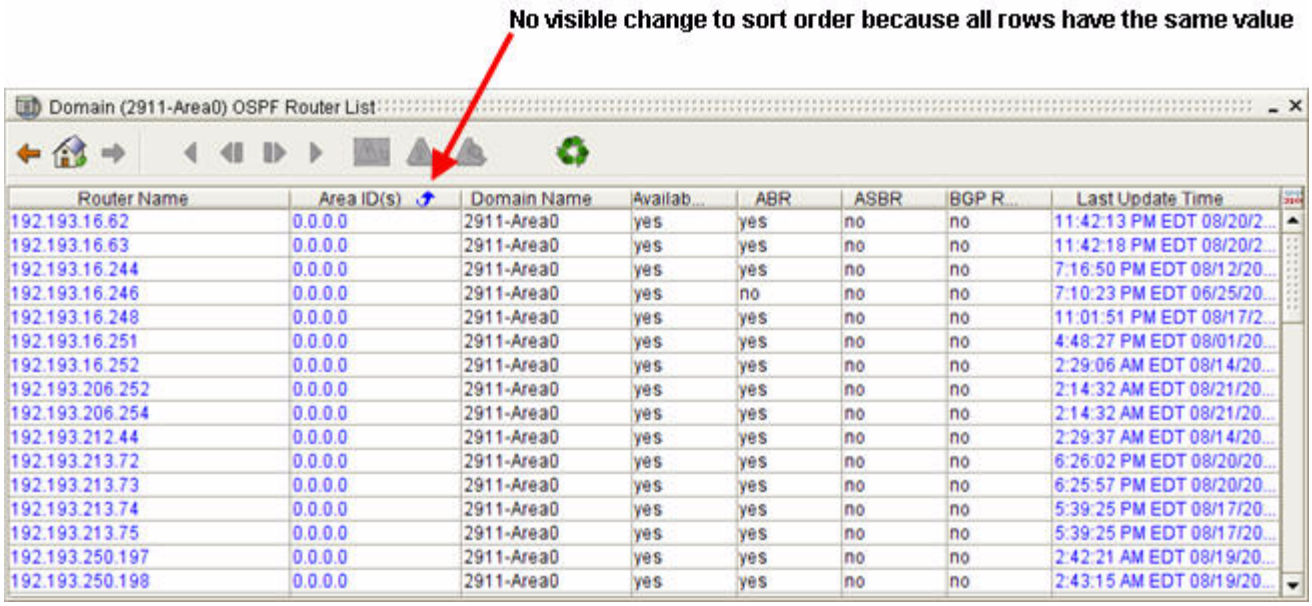
Sorting Other Columns

Clicking the heading of a column repositions the **Sort** icon to the top of the selected column and reorders the content listed in the column. Click the **Sort** icon again to rearrange the data values of the column in decreasing order.

Sorting in Columns that Show the Same Value in All Rows

Clicking the **Sort** icon in a column that contains the same values in all rows does not display a noticeable change in the sort order. For example, the **Domain Name** values remain the same in the Domain Name field whether rows are sorted by increasing or decreasing order because all routers belong to the same domain (see Figure 2-32).

Figure 2-32 Sorting Status Column Values in Router List

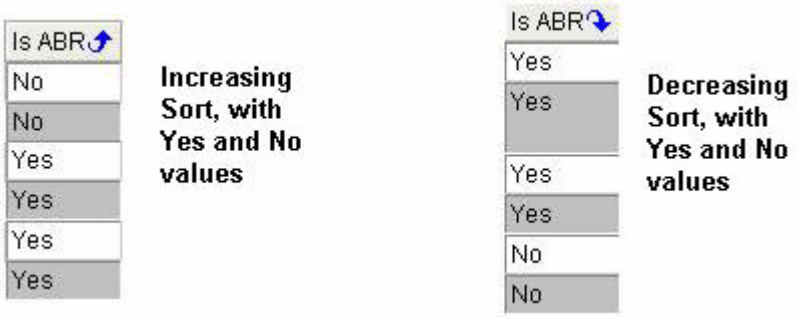


Router Name	Area ID(s)	Domain Name	Availab...	ABR	ASBR	BGP R...	Last Update Time
192.193.16.62	0.0.0.0	2911-Area0	yes	yes	no	no	11:42:13 PM EDT 08/20/2...
192.193.16.63	0.0.0.0	2911-Area0	yes	yes	no	no	11:42:18 PM EDT 08/20/2...
192.193.16.244	0.0.0.0	2911-Area0	yes	yes	no	no	7:16:50 PM EDT 08/12/20...
192.193.16.246	0.0.0.0	2911-Area0	yes	no	no	no	7:10:23 PM EDT 06/25/20...
192.193.16.248	0.0.0.0	2911-Area0	yes	yes	no	no	11:01:51 PM EDT 08/17/2...
192.193.16.251	0.0.0.0	2911-Area0	yes	yes	no	no	4:48:27 PM EDT 08/01/20...
192.193.16.252	0.0.0.0	2911-Area0	yes	yes	no	no	2:29:06 AM EDT 08/14/20...
192.193.206.252	0.0.0.0	2911-Area0	yes	yes	no	no	2:14:32 AM EDT 08/21/20...
192.193.206.254	0.0.0.0	2911-Area0	yes	yes	no	no	2:14:32 AM EDT 08/21/20...
192.193.212.44	0.0.0.0	2911-Area0	yes	yes	no	no	2:29:37 AM EDT 08/14/20...
192.193.213.72	0.0.0.0	2911-Area0	yes	yes	no	no	6:26:02 PM EDT 08/20/20...
192.193.213.73	0.0.0.0	2911-Area0	yes	yes	no	no	6:25:57 PM EDT 08/20/20...
192.193.213.74	0.0.0.0	2911-Area0	yes	yes	no	no	5:39:25 PM EDT 08/17/20...
192.193.213.75	0.0.0.0	2911-Area0	yes	yes	no	no	5:39:25 PM EDT 08/17/20...
192.193.250.197	0.0.0.0	2911-Area0	yes	yes	no	no	2:42:21 AM EDT 08/19/20...
192.193.250.198	0.0.0.0	2911-Area0	yes	yes	no	no	2:43:15 AM EDT 08/19/20...

Sorting in Columns that Show Different, but Non-Numeric Values

The **Sort** icon causes non-numeric values to be displayed in ascending or descending alphabetical order. For example, in a column with rows that display "Yes" or "No" values (such as the Is ABR and Is ASBR columns in Figure 2-33), an increasing sort organizes all rows with "No" values before rows with "Yes" values. A decreasing sort organizes all "Yes" values first.

Figure 2-33 Increasing and Decreasing Sorts for Columns with "Yes" and "No" Values



Sorting Dates and Times

For columns that list date and time values, such as the **Last Change Time** column in the Router List dialog box, an increasing sort organizes all rows from most recent date and time to least recent date and time. A decreasing sort organizes the rows from least recent date and time to most recent date and time.

Sort Rows by Increasing Value

In the Router Name column of the Topology Browser Domain OSPF Router List dialog box, click the Increasing **Sort** icon to list routers by IP address in increasing order:

See Sort Data in a Column, page 2-52.

Sort Rows by Decreasing Value

In the Router Name column of the Topology Browser Domain OSPF Router List dialog box, click the Decreasing **Sort** icon to list routers by IP address in decreasing order:

See Sort Data in a Column, page 2-52.

Move the Sort Arrow

To move the sort arrow:

Step 1 Click the heading of the column of data that you want to sort. The **Sort** icon moves to the heading and sorts the data in increasing order.

Step 2 Click the **Sort** icon again to rearrange the data in decreasing order.

See Sort Data in a Column, page 2-52.

Viewing Metrics and Attributes

You can view high-level attributes of your enterprise-wide network and its subsystems from the Path Anaylzer Management Console. The Topology Browser provides information about autonomous systems, routing domains, routers, Transit networks, interfaces, and route advertisements that carry data across your enterprise network.

View Details of the Enterprise Network

To view the details of an enterprise network:

Step 1 Use the procedure Start the Topology Browser, page 2-5.

The BGP Router List Dialog Box, page 2-108 appears, showing details about the enterprise network.

Step 2 Click the **Home** icon in any Topology Browser dialog box to return to the Enterprise Overview dialog box.

View All Autonomous Systems in the Enterprise Network

To view all autonomous systems in the enterprise network from the Topology Viewer, use the procedure in Start the Hierarchical Topology Viewer, page 2-4.

You will see the icons representing each autonomous system.

To view all autonomous systems in the enterprise network from the Topology Browser:

Step 1 Use the procedure in Start the Topology Browser, page 2-5.

Step 2 Click on the Total BGP Domain Count value in the Enterprise Overview Dialog Box, page 2-103.

The Autonomous System List Dialog Box, page 2-104 opens, showing the total number of autonomous systems in the enterprise network.

View Details of an Autonomous System

To view the details of an autonomous system from the Topology Viewer:

Step 1 Use the procedure in Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Right-click an autonomous system and select **Show Overview**.

The BGP Domain Details Dialog Box, page 2-106 appears, showing details about the AS domain you selected, including the BGP Domain name, IGP Domain, BGP router count, IPV4, VPN, and VRF information.

To view the details of an autonomous system from the Topology Browser:

Step 1 Use the procedure in Start the Topology Browser, page 2-5. The Enterprise Overview Dialog Box, page 2-103 appears.

Step 2 Click the value in the Total BGP Domain Count field. The Autonomous System List Dialog Box, page 2-104 appears.

Step 3 Click the value in the BGP Domain field for the AS for which you want more information.

The BGP Domain Details Dialog Box, page 2-106 appears, showing details about the AS domain you selected, including the BGP Domain name, IGP Domain, BGP router count, IPV4, VPN, and VRF information.

View Areas in a Domain

To view areas ion a domain from the Topology Viewer:

Step 1 Use the procedures in Start the Flat Topology Viewer, page 2-4 or Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Right-click an autonomous system and select **Expand**. The autonomous system expands, revealing the areas it contains.

To view areas ion a domain from the Topology Browser:

Step 1 Use the procedure in Start the Topology Browser, page 2-5. The Enterprise Overview Dialog Box, page 2-103 appears.

Step 2 Click the value in the Total BGP Domain Count field. The Autonomous System List Dialog Box, page 2-104 appears.

Step 3 Click the value in the BGP Domain field of the AS for which you want area information. The BGP Domain Details Dialog Box, page 2-106 appears.

Step 4 Click the value in the IGP Domain field. The OSPF Domain Details Dialog Box, page 2-104 appears.

Step 5 The value in the IGP Domain field will indicate the number of areas within the domain. Click on the value to see the Area IDs.

View Details of an Area

To view details of an area from the Topology Viewer:

Step 1 Use the procedure in Start the Hierarchical Topology Viewer, page 2-4.

Step 2 Use the procedure in View Areas in a Domain, page 2-55.

Step 3 Right-click an area.

Step 4 Click **Show Overview** to display details about the area in the Area Overview Dialog Box, page 2-117.

The Area Overview dialog box shows the number of routers, routes, and interface types in the area.

View All OSPF Routers in an AS

To view all OSPF routers in an autonomous system:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears.

Step 2 Click the value in the IGP Router Count field.

The OSPF Domain Details Dialog Box, page 2-104 appears.

Step 3 Click Total OSPF Router Count.

The Domain OSPF Router List Dialog Box, page 2-113 opens, listing all OSPF routers in the AS.

View All BGP Routers in an AS

To view all BGP routers in an autonomous system:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears.

Step 2 Click the link in the BGP Router Count field.

The BGP Router List Dialog Box, page 2-108 opens, listing all BGP routers shown in the AS.

View All OSPF Routers in an Area

To view all OSPF routers in an area:

Step 1 Use the procedure in View Details of an Area, page 2-56.

The Area Overview Dialog Box, page 2-117 appears.

Step 2 Click the value in the Total Router Count field.

The Area OSPF Router List Dialog Box, page 2-109 appears, showing values for all routers in the area.

View OSPF Interfaces for All Routers in an AS

To view all OSPF interfaces for all routers in an autonomous system:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears.

Step 2 Click the IGP Domain value.

The OSPF Domain Details Dialog Box, page 2-104 opens.

Step 3 Click the value in the Total OSPF Interface Count field.

The Domain OSPF Interface List Dialog Box, page 2-115 appears, showing all OSPF interfaces in the autonomous system.

View OSPF Interfaces for All Routers in an Area

To view all OSPF interfaces for all routers in an area:

Step 1 Use the procedure in View Details of an Area, page 2-56.

The Area Overview Dialog Box, page 2-117 appears.

Step 2 Click the Total Interface Count value. The Area OSPF Interface List Dialog Box, page 2-112 appears, showing all OSPF interfaces in the area.

View Attributes of an OSPF Router

To view attributes of an OSPF router in the Topology Viewer:

Step 1 Right-click the router for which you want to view attributes.

Step 2 Click **Show OSPF Attributes**.

The Attributes for OSPF Router Dialog Box, page 2-119 appears.

To view attributes of an OSPF router:

- From the Domain OSPF Router List Dialog Box, page 2-113, click the Router ID in the Router Name column. The Attributes for OSPF Router Dialog Box, page 2-119 appears.
- From any Route Advertisement for Router dialog box, click the name of the router in the Advertising Router Name column. The Attributes for OSPF Router Dialog Box, page 2-119 appears.
- From any Advertising Routers for Route dialog box, click the name of the router in the Advertising Router Name column. The Attributes for OSPF Router Dialog Box, page 2-119 appears.
- From the All Interfaces for Router Dialog Box, page 2-127, click the Destination or Source value of the router. The Attributes for OSPF Router Dialog Box, page 2-119 appears.

View Attributes of a BGP Router

To view attributes of a BGP router from the Topology Viewer:

Step 1 Right-click the router for which you want to view attributes.

Step 2 Click **Show BGP Attributes**.

The BGP Router Details Dialog Box on page 2-121 is opened showing the attributes of the BGP router.

To view attributes of a BGP router from the BGP Router List Dialog Box, page 2-108, click a link in the BGP Router Name column. The BGP Router Details Dialog Box on page 2-121 is opened showing the attributes of the BGP router.

View All IPV4 Prefixes Within an AS for a BGP Router

To view all IPv4 prefixes within an AS for a BGP router from the Topology Viewer:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears.

Step 2 Click the value for IPv4 Prefix Count.

The IPV4 Prefix List Dialog Box, page 2-141 appears.

View All IPV4 Multicast Prefixes Within an AS for a BGP Router

To view all IPv4 multicast prefixes within an AS for a BGP router from the Topology Viewer:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears.

Step 2 Click the value for IPv4 Multicast prefix Count.

The IPV4 Multicast Prefix List Dialog Box, page 2-142 appears.

View All VPN Prefixes Within an AS for a BGP Router

To view all VPN prefixes within an AS for a BGP router from the Topology Viewer:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears.

Step 2 Click the value for VPN Prefix Count.

The VPN Prefix List Dialog Box, page 2-146 appears.

View All IPV4 Routes Within an AS for a BGP Router

To view all IPv4 routes within an AS for a BGP router from the Topology Viewer:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears.

Step 2 Click the value (More Statistics) for IPv4 Multicast Routes.

The BGP Statistics Dialog Box, page 2-140 appears.

View All IPV4 Multicast Routes Within an AS for a BGP Router

To view all IPv4 multicast routes within an AS for a BGP router from the Topology Viewer:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears.

Step 2 Click the value (More Statistics) for IPv4 Multicast Routes.

The BGP Statistics Dialog Box, page 2-140 appears.

View All VPN Routes Within an AS for a BGP Router

To view all VPN routes within an AS for a BGP router from the Topology Viewer:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears.

Step 2 Click the value (More Statistics) for VPN Routes.

The BGP Statistics Dialog Box, page 2-140 appears.

View the Interfaces of a Specific OSPF Router

To view the interfaces of a specific OSPF router from the Topology Viewer:

Step 1 Right-click an OSPF router.

Step 2 Click **Show Interfaces**.

The All Interfaces for Router Dialog Box on page 2-127 appears.

For more information about a router interface, click a link in the Identifier column of a router interface type to display an Attributes for Interface dialog box.

To view the interfaces of a specific OSPF router from the Attributes for OSPF Router Dialog Box, page 2-119, click the link displayed in any of the following fields:

- **NP2P Interference Count—**The NP2P Interfaces for Router Dialog Box, page 2-128 opens, listing all NP2P Interfaces of the router.
- **UP2P Interference Count—**The UP2P Interfaces for Router Dialog Box, page 2-129 opens, listing all UP2P Interfaces of the router.
- **Transit Interference Count**—The Transit Interfaces for Router Dialog Box, page 2-130 opens, listing all Transit Interfaces of the router.

  If the router has no interfaces of a particular type, the value "0" is displayed in the field.

  Example: If a selected router has no NP2P Interfaces, the value "0" is displayed in the NP2P field.

View All OSPF Routes in an AS

To view all OSPF routes in an autonomous system:

Step 1 Use the procedure in View Details of an Autonomous System, page 2-55.

The BGP Domain Details Dialog Box, page 2-106 appears, showing details about the AS domain you selected.

Step 2 Click the link displayed in the IGP Domain column.

The OSPF Domain Details Dialog Box, page 2-104 appears.

Step 3 Click the value in the Total OSPF Route Count column.

The Domain OSPF Route List Dialog Box, page 2-114 appears, showing all OSPF routes in the autonomous system.

View All OSPF Routes in an Area

To view all OSPF routes in an area:

Step 1 Use the procedure in View Details of an Area, page 2-56.

The Area Overview Dialog Box, page 2-117 opens, listing metrics for the autonomous system.

Step 2 Click the value in the Total Route Count field.

The Area OSPF Route List Dialog Box, page 2-110 appears, showing all routes in the area.

View Route Advertisements Announced by a Specific Router

To view route advertisements announced by a specific router from the Topology Viewer:

Step 1 Right-click an OSPF router.

Step 2 Select one of the following options from the menu:

Note Options vary depending on the type of router.

- **Show External Route Advertisements—**Opens the External Route Advertisements for OSPF Router Dialog Box, page 2-133, which lists statistics about all external route advertisements of the ASBR. ASBRs announce summaries of external routes in Type 5 Link State Advertisements (LSAs).
- **Show Stub Route Advs**—Opens the Stub Route Advertisements for OSPF Router Dialog Box, page 2-135, which lists statistics about all stub route advertisements of other router.
- **Show T3 Summary Route Advertisements—**Opens the T3 Summary Route Advertisements for OSPF Router Dialog Box, page 2-131, which lists statistics about all T3 Summary route advertisements of the ABR.
- **Show T4 Summary Route Advertisements—**Opens the T4 Summary Route Advertisements for OSPF Router Dialog Box, page 2-132, which lists statistics about all T4 Summary route advertisements of the ABR.

To view route advertisements announced by a specific router from the Attributes for OSPF Router Dialog Box, page 2-119, click the link displayed in any of the following fields:

- **T3 Summary Route Advertisements—**The T3 Summary Route Advertisements for OSPF Router Dialog Box, page 2-131 opens, listing all T3 Summary route advertisements the selected ABR announces.
- **T4 Summary Route Advertisements**— The T4 Summary Route Advertisements for OSPF Router Dialog Box, page 2-132 opens, listing all T4 Summary route advertisements the selected ABR announces.
- **Stub Route Advertisement Count**— The Stub Route Advertisements for OSPF Router Dialog Box, page 2-135 opens, listing all stub route advertisements the router announces.
- **External Route Advertisements—**The External Route Advertisements for OSPF Router Dialog Box, page 2-133 opens, listing all external route advertisements the selected ASBR announces in Type 5 LSAs.

View OSPF Attributes of an Area Node

To view OSPF attributes of an area node from the Topology Viewer, right-click an OSPF router, then select **Show OSPF Attributes**.

The Attributes for OSPF Router Dialog Box, page 2-119 appears, presenting attributes of that router.

To view OSPF attributes of an area node from the Area Overview dialog box:

Step 1 Click the Total Router Count link.

The Area OSPF Router List Dialog Box, page 2-109 appears.

Step 2 Click a Router Name link.

The Attributes for OSPF Router Dialog Box, page 2-119 appears, presenting details about ABR interfaces in the area.

To view OSPF attributes of an area node from the Domain OSPF Router List dialog box, click a Router Name link.

The Attributes for OSPF Router Dialog Box, page 2-119 appears, presenting attributes of that router.

View Attributes of a Transit Interface

To view attributes of a transit interface from the Topology Viewer:

Step 1 Right-click the transit interface link, which is displayed as an arrow pointing from a router to a Transit network.

Step 2 Click **Show Attributes**.

The Attributes for Transit Interface Dialog Box, page 2-124 appears.

To view attributes of a transit interface from the Attributes for OSPF Router Dialog Box, page 2-119:

Step 1 Click the Transit Interface Count value.

The Transit Interfaces for Router Dialog Box, page 2-130 appears.

Step 2 Click an Identifier link.

The Attributes for Transit Interface Dialog Box, page 2-124 appears.

View Attributes of a Transit-to-Router Link

To view attributes of a transit-to-router link from the Topology Viewer:

Step 1 Right-click the transit-to-router interface link, which is displayed as an arrow pointing from the Transit network to a router.

Step 2 Click **Show Attributes**.

The Attributes for Transit to Router Link Dialog Box, page 2-122 appears.

View Attributes of a Numbered Point-to-Point (NP2P) Interface

To view attributes of a numbered P2P interface from the Topology Viewer:

Step 1 Right-click an NP2P interface.

Step 2 Click **Show OSPF Attributes**.

The Attributes for Numbered Point-to-Point Interface Dialog Box on page 2-122 appears.

To view attributes of a numbered P2P interface from a Router:

Step 1 Right-click the router and select **Show Interfaces**.

Step 2 Click on the value for the NP2P Interface Count field.

The All Interfaces for Router Dialog Box, page 2-127 appears.

Step 3 Click on a value in the Identifier field for an N2P2 router.

The Attributes for Numbered Point-to-Point Interface Dialog Box, page 2-122 appears.

View Attributes of an Unnumbered Point-to-Point (UP2P) Interface

To view attributes of an unnumbered P2P interface from the Topology Viewer:

Step 1 Right-click the UP2P interface.

Step 2 Click **Show OSPF Attributes.**

The Attributes for Unnumbered Point-to-Point Interface Dialog Box, page 2-123 appears.

To view attributes of an unnumbered P2P interface from a Router:

Step 1 Right-click the router and select **Show Interfaces**.

Step 2 Click on the value for the UP2P Interface Count field.

The All Interfaces for Router Dialog Box, page 2-127 appears.

Step 3 Click on a value in the Identifier field for an UP2P router.

The Attributes for Unnumbered Point-to-Point Interface Dialog Box, page 2-123 appears.

View Routers Attached to a Transit Network

To view routers attached to a Transit network:

Step 1 Right-click on a Transit Network and select **Show Attributes**.

The Attributes for Transit Network Dialog Box, page 2-125 appears.

Step 2 Click the No. Attached Routers link in the Attributes for Transit Network Dialog Box, page 2-125.

The Attached Routers for Transit Network Dialog BoxAttached Routers for Transit Network Dialog Box, page 2-135 appears.

Pivoting to the Event Log

Right-clicking a router or a Transit network in the Topology Viewer enables you to investigate changes that affected the selected router or network and changed routing patterns across the larger network during the last 24 hours. These changes, are called *events* and they are displayed in the Event Log.

For more information on the Event Log see, Monitoring Changes in Routing, on page 4-1.

If a router is configured with both BGP and OSPF router stacks, options are displayed to view BGP or OSPF events.

Investigate Events

To investigate events on a router configured with an OSPF or BGP router stack:

Step 1 Right-click the router.

Step 2 Select **Investigate Recent Events**.

The Event Log appears.

To investigate events on a router configured with both an OSPF or BGP stack:

Step 1 Right-click the router.

Step 2 Select **Investigate Recent OSPF Events**.

The Event Log appears.

or

Select **Investigate Recent BGP Events**.

The Event Log appears.

To investigate events on a Transit network:

Step 1 Right-click the Transit network.

Step 2 Select **Investigate Recent Events**.

The Event Log appears.

Using the Topology Filter Wizard for BGP Entities

BGP entities can be queried using the **Specify the Filter for the Current Table** icon in a Topology Table Dialog box.

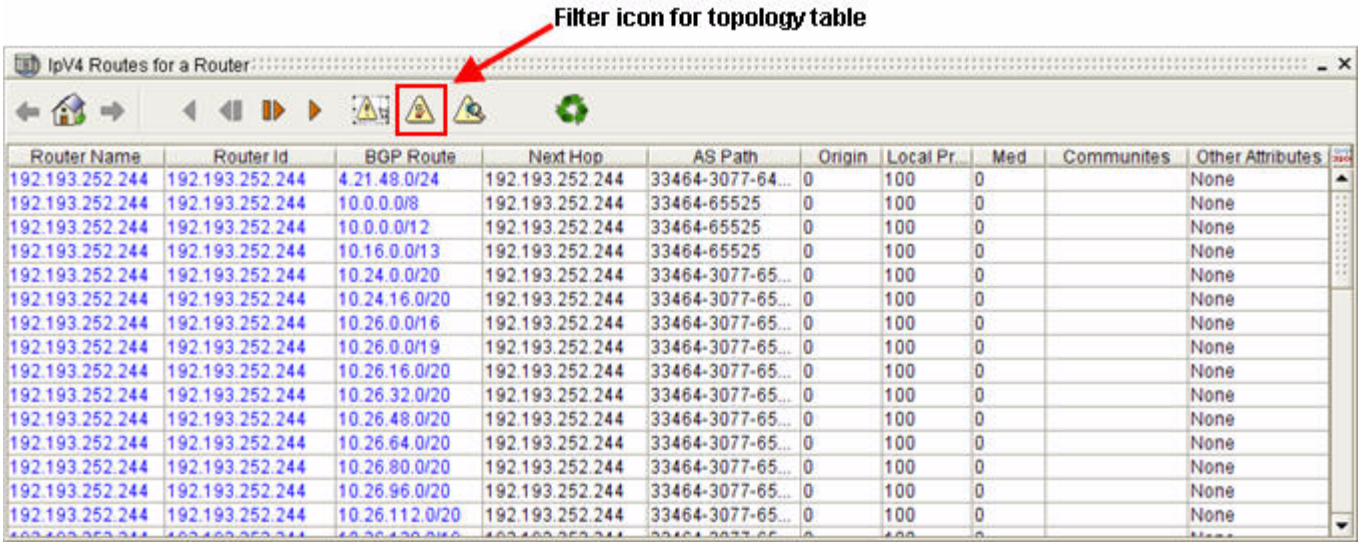
See Navigating in Topology Browser Dialog Boxes, page 2-48.

The following tables can be queried:

- Router Table
- IPV4 Prefix List
- IPV4 Multicast Prefix List
- IPV4 VPN Prefix List
- IPV4 Route List
- VPN Route List (Figure 2-34 on page 2-66)
- VRFs

Clicking on the **Specify a Filter for the Current Table** icon (see Figure 2-34) will open the Topology Filter wizard. A series of screens are presented in which specific constraints can be applied to the query. These screens will vary from table to table. See Table 2-9 for a complete listings of query types and constraints.

Figure 2-34 Topology Filter Icon



BGP Query Types and Constraints

The Topology Filter wizard for BGP entities supports the query types and constraints displayed in Table 2-9.

Table 2-9 BGP Query Types and Constraints

Query Type	Constraints
Router Table	Router ID
IP4 Prefix List Table	IP Prefix IP Prefix Mask
IP4 Multicast Prefix List Table	IP Prefix IP Prefix Mask
IP4 VPN Prefix List Table	VPN IP Prefix VPN IP Prefix Mask
IP4 Route List Table	Router ID IP Prefix P Prefix Mask AS Path AS Path Length Next Hop Origin Local Preference Multi-Exit Discriminator (MED) Community

Table 2-9 BGP Query Types and Constraints

Query Type	Constraints
VPN Route List Table	Router ID
	VRF ID
	VPN IP Prefix
	VPN Prefix Mask Length
	Route Target
	Next Hop
	AS Path
	AS Path Length
	Origin
	Local Preference
	Multi-Exit Discriminator (MED)
	Community
	Site of Origin
VRF Table	Router ID
	VRF ID

BGP Filtering Example: VPN Route List

To see how the BGP filtering processing works, we will look at an example showing the screens presented for filtering a VPN Route List.

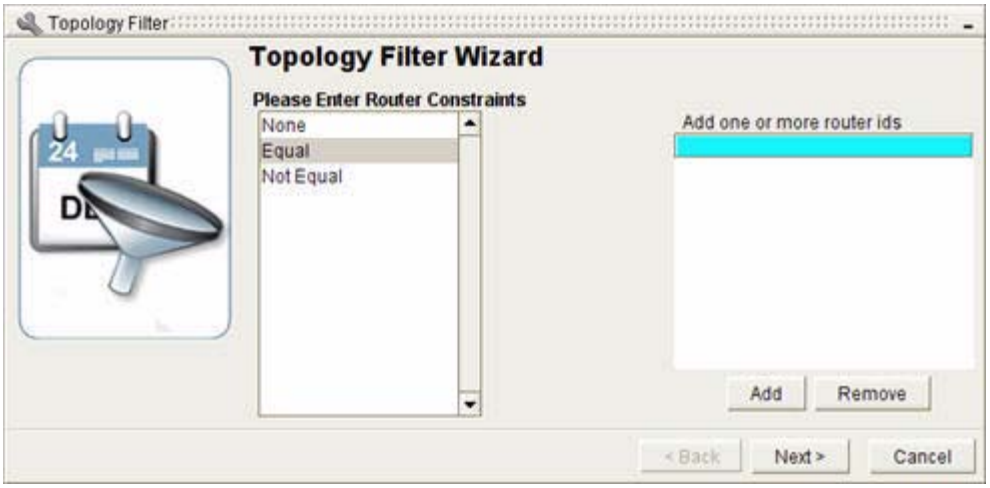
The data input formats used to enter constraints in the blue boxes on Topology Filter wizard pages are shown in Table 2-9.

Using a Topology Filter

To use a topology filter from the Topology Browser toolbar, click the **Specify a Filter for the Current Table** icon.

The Enter Router Constraints Topology Filter wizard screen appears (see Figure 2-35).

Figure 2-35 Enter Router Constraints Screen in Topology Filter Wizard



Enter Router Constraints

To enter router constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by Router ID, select **None** and click **Next**.

  or

- If you wish to filter by Router ID you have the following choices:
  - **Equal—**Will return all entries that contain the specified Router ID(s)
  - **Not Equal—**Will return all entries that do not contain the specified Router ID(s)

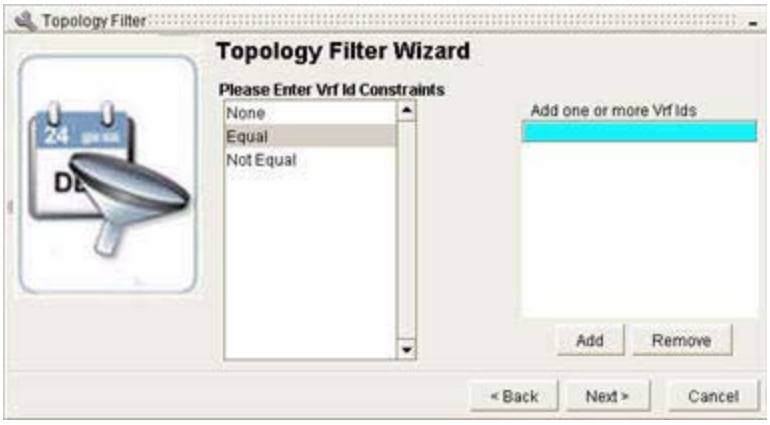
Note If you wish to remove a constraint you have entered in the Topology Filter wizard, click the **Remove** button.

Step 2 Select one of these options, enter one or more Router ID(s) or a range of Router IDs and click **Add**.

Step 3 Click **Next**.

The Enter VRF ID Constraints screen appears (see Figure 2-36).

Figure 2-36 Enter VRF ID Constraints Screen in Topology Filter Wizard



Enter VRF Constraints

To enter VRF constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by VRF ID, select **None** and click **Next**.

  or

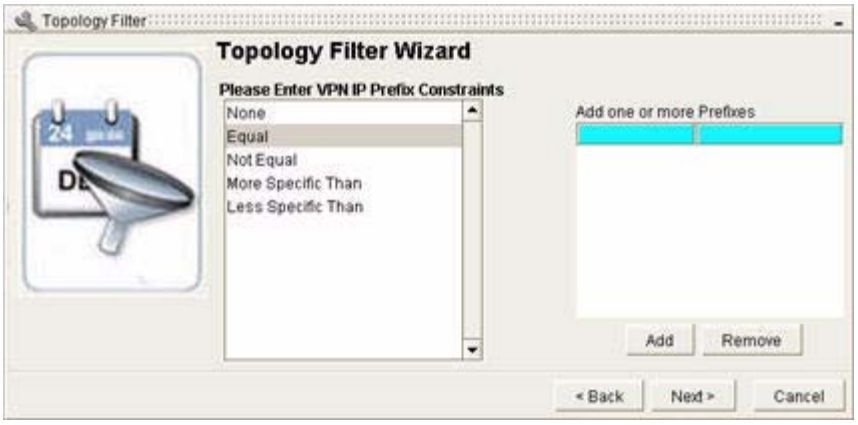
- If you wish to filter by VRF ID you have the following choices:
  - **Equal—**Will return all entries that contain the specified VRF ID(s)
  - **Not Equal—**Will return all entries that do not contain the specified VRF ID(s)

Step 2 Select one of these options, enter one or more VRF ID(s), and click **Add**.

Step 3 Click **Next**.

The Enter VPN IP Prefix Constraints screen appears (see Figure 2-37).

Figure 2-37 Enter VPN IP Prefix Constraints Screen in Topology Filter Wizard



Enter VPN IP Prefix Constraints

To enter VPN IP constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by VPN IP Prefix, select **None** and click **Next**.

  or

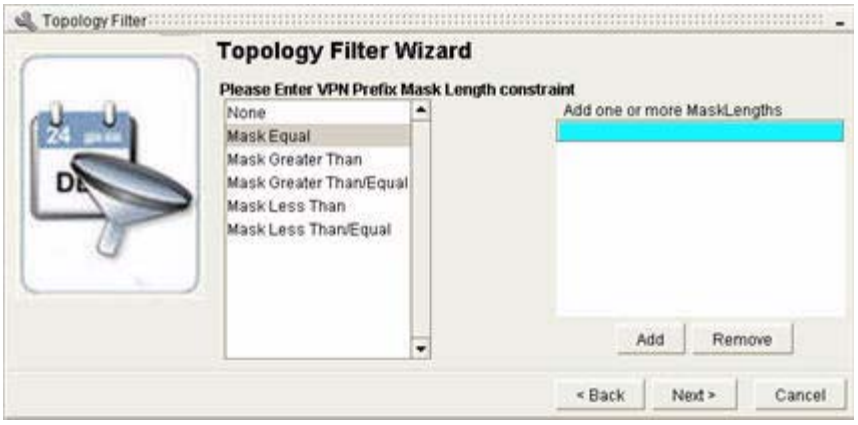
- If you wish to filter by VPN IP Prefix you have the following choices:
  - **Equal—**Will return all entries that contain the specified VPN IP prefix(es)
  - **Not Equal—**Will return all entries that do not contain the specified VPN IP prefix(es)
  - **More Specific Than—**Will return all entries that are more specific than the specified range

    Example: If you enter 10:10 192.168.0.0/24, the filter might return values between 10:10 192.168.0.1 and 10:10 192.168.0.254, or any subnets of 10:10 192.168.0.0/ in the range /25 to /32).
  - **Less Specific Than—**Will return all entries that are less specific than the specified range

Step 2 Select one of these options, enter one or more VPN IP prefix(es), and click **Add**. Then click **Next**.

The Enter VPN Prefix Mask Length Constraint screen appears (see Figure 2-38).

Figure 2-38 Enter VPN Prefix Mask Length Constraints Screen in Topology Filter Wizard



Enter VPN Prefix Mask Length Constraints

To enter VPN prefix mask length constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by VPN Prefix Mask Length, select **None** and click **Next**.

  or

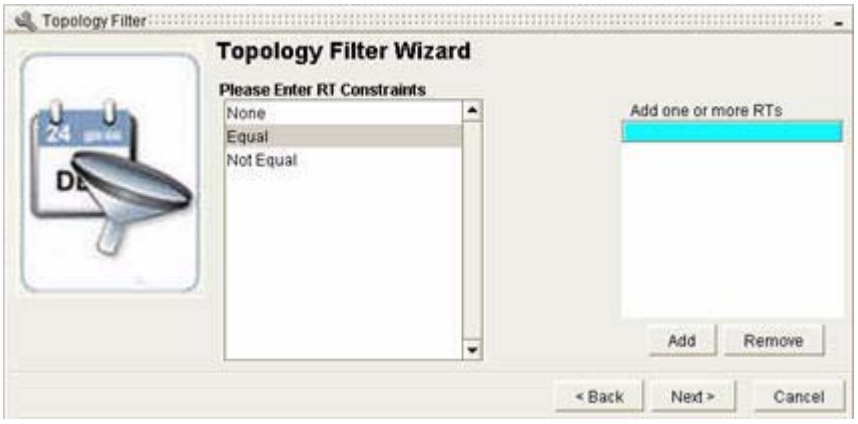
- If you wish to filter by VPN Prefix Mask Length you have the following choices:
  - **Mask Equal—**Will return all entries that contain the specified VPN Prefix Mask Length(s)
  - **Mask Greater Than—**Will return all entries that contain a value greater than the specified VPN Prefix Mask Length(s)
  - **Mask Greater Than/Equal—**Will return all entries that contain a value greater than or equal to the specified VPN Prefix Mask Length(s)
  - **Mask Less Than—**Will return all entries that contain a value less than the specified VPN Prefix Mask Length(s)
  - **Mask Less Than/Equal—**Will return all entries that contain a value less than or equal to the specified VPN Prefix Mask Length(s)

Step 2 Select one of these options, enter one or more VPN Prefix Mask Length(s) and click **Add**.

Step 3 Click **Next**.

The Enter Route Target Constraints screen appears (see Figure 2-39).

Figure 2-39 Enter Route Target Constraints Screen in Topology Filter Wizard



Enter Route Target Constraints

To enter route target constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by Route Target, select **None** and click **Next**.

  or

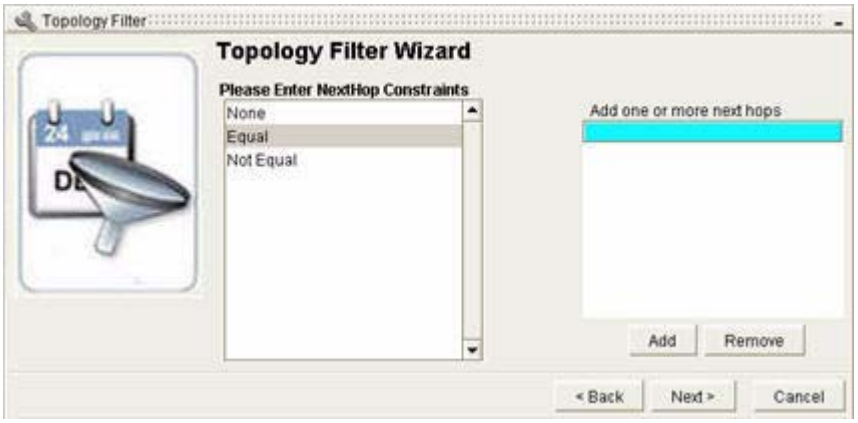
- If you wish to filter by Route Target you have the following choices:
  - **Equal—**Will return all entries that are equal to the specified Route Target(s)
  - **Not Equal—**Will return all entries that are not equal to the specified Route Target(s)

Step 2 Select one of these options, enter one or more Route Target(s) and click **Add**.

Step 3 Click **Next**.

The Next Hop Constraints screen appears (see Figure 2-40).

Figure 2-40 Enter Next Hop Constraints Screen in Topology Filter Wizard



Enter Next Hop Constraints

To enter next hop constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by Next Hop select **None** and click **Next**.

  or

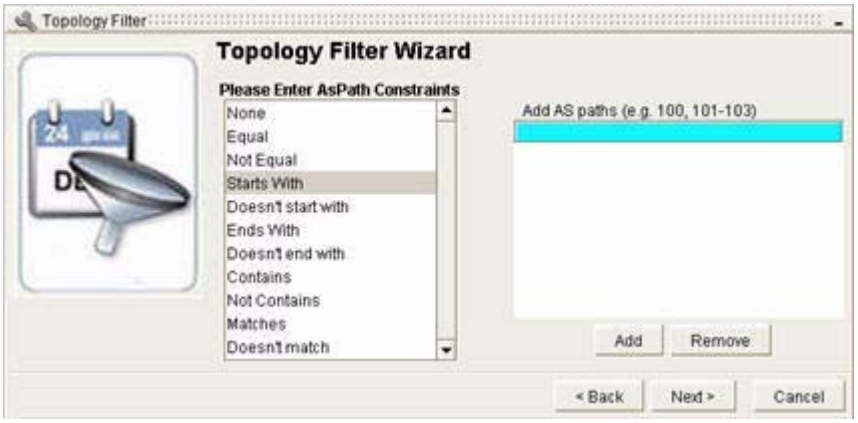
- If you wish to filter by Next Hop you have the following choices:
  - **Equal—**Will return all entries that are equal to the specified Next Hop(s)
  - **Not Equal—**Will return all entries that are not equal to the specified Next Hop(s)

Step 2 Select one of these options, enter one or more Next Hop(s) and click **Add**.

Step 3 Click **Next**.

The AS Path Constraints screen appears (see Figure 2-41).

Figure 2-41 Enter AS Path Constraints Screen in Topology Filter Wizard



Enter AS Path Constraints

To enter AS path constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by AS Path select **None** and click **Next**.

  or

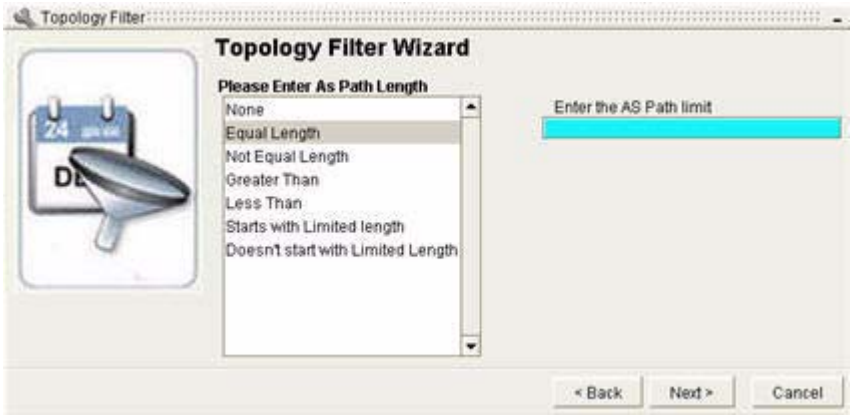
- If you wish to filter by AS Path you have the following choices:
  - **Equal—**Will return all entries that are equal to the specified AS path(s), in any combination
  - **Not Equal—**Will return all entries that are not equal to the specified AS path(s)
  - **Starts with—**Will return all entries that start with the specified AS path(s)
  - **Doesn't start with—**Will return all entries that do not start with the specified AS path(s)
  - **Ends with—**Will return all entries that end with the specified AS path(s)

- **Doesn't end with—**Will return all entries that do not end with the specified AS path(s)
- **Contains—**Will return all entries that contain at least one of the specified AS path(s)
- **Not contains—**Will return all entries that do not contain any of the specified AS path(s)
- **Matches—**Will return all entries that match any of the Java regular expression you entered
- **Doesn't match—**Will return all entries that do not match any of the Java regular expression you entered

Step 2 Select one of these options, enter one or more AS path(s) or Java regular expression and click **Add**. Then click **Next**.

The AS Path Length Constraints screen appears (see Figure 2-42).

Figure 2-42 Enter AS Path Length Constraints Screen in Topology Filter Wizard



Enter AS Path Length Constraints

To enter AS length constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by AS Path Length select **None** and click **Next**.

  or

- If you wish to filter by AS Path Length you have the following choices:
  - **Equal Length—**Will return all entries that have the specified number of AS's in their path
  - **Not Equal Length—**Will return all entries that do not have the specified number of AS's in their path
  - **Greater Than—** Will return all entries that have a greater number of AS's in their path than the number specified here
  - **Less Than—**Will return all entries that have fewer AS's in their path than the number specified here

  The next two options have two fields to complete: **Enter the AS Path**, and **Enter the AS Path Length**.

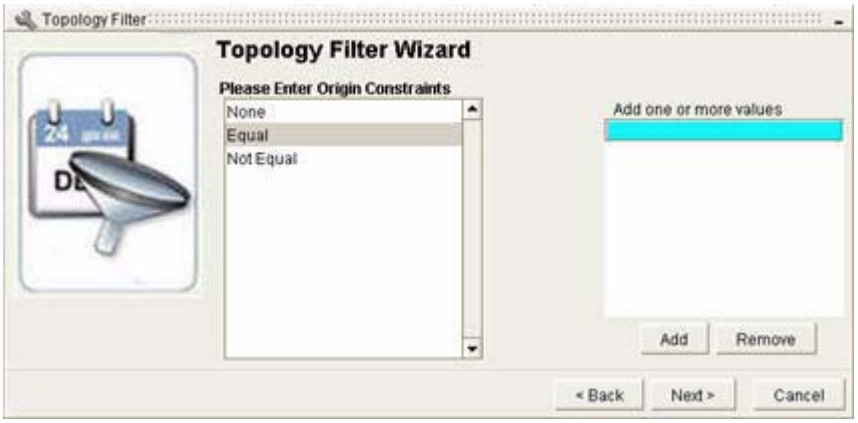
- **Starts with limited length—**Will return all entries that start with the specified AS path but have the specified AS path length.
- **Doesn't start with limited length—**Will return all entries that do not start with the specified AS path but have the specified AS path length.

Step 2 Select one of these options, enter one or more AS Path Length(s) and click **Add**.

Step 3 Click **Next**.

The Origin Constraints screen appears (see Figure 2-43).

Figure 2-43 Enter Origin Constraints Screen in Topology Filter Wizard



Enter Origin Constraints

To enter origin constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by Origin select **None** and click **Next**.

  or

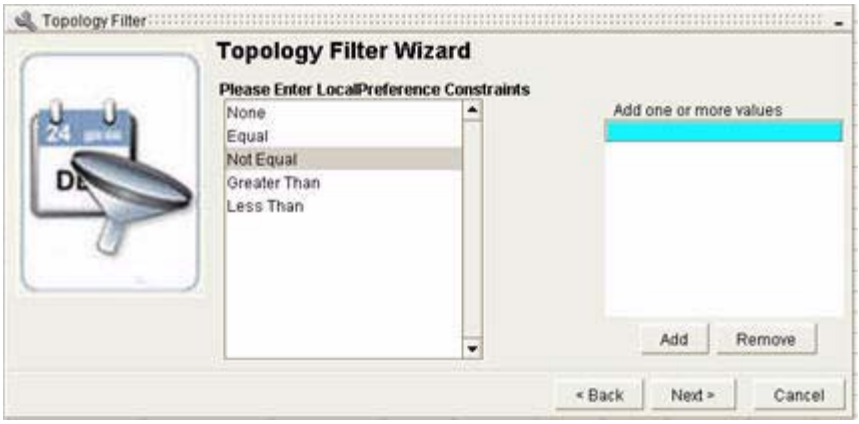
- If you wish to filter by Origin you have the following choices:
  - **Equal—**Will return all entries that have the specified Origin(s). (Options are Incomplete, IGP, and EGP).
  - **Not Equal—**Will return all entries that do not have the specified Origin(s)

Step 2 Select one of these options, enter one or more Origin(s) and click **Add**.

Step 3 Click **Next**.

The Local Preference Constraints screen appears (see Figure 2-44).

Figure 2-44 Enter Local Preference Constraints Screen in Topology Filter Wizard



Enter Local Preference Constraints

To enter local preference constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by Local Preference select **None** and click **Next**.

  or

- If you wish to filter by Local Preference you have the following choices:
  - **Equal—**Will return all entries that equal the Local Preference value you entered. (For example, "8".)
  - **Not Equal—**Will return all entries that do not equal the Local Preference value you entered.
  - **Greater Than—**Will return all entries that have a value greater than the Local Preference value you entered
  - **Less Than—**Will return all entries that have a value less than the Local Preference value you entered

Step 2 Select one of these options, enter one or more Local Preference values and click **Add**.

Step 3 Click **Next**.

The Enter Multi-Exit Discriminator (MED) Constraints screen appears (see Figure 2-45).

Figure 2-45 Enter MED Constraints Screen in Topology Filter Wizard

Enter Multi-Exit Discriminator (MED) Constraints

To enter MED constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by MED select **None** and click **Next**.

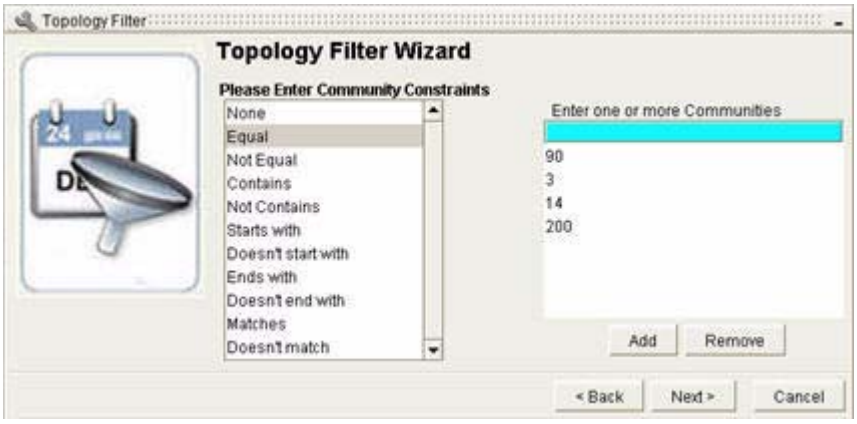
  or

- If you wish to filter by MED you have the following choices:
  - **Equal—**Will return all entries that equal the MED value you entered. (For example, "12".)
  - **Not Equal—**Will return all entries that do not equal the MED value you entered
  - **Greater Than—**Will return all entries that have a value greater than the MED value you entered
  - **Less Than—**Will return all entries that have a value less than the MED value you entered

Step 2 Select one of these options, enter one or more MED values and click **Add**. Then click **Next**.

The Enter Community Constraints screen appears (see Figure 2-46).

Figure 2-46 Enter Community Constraints Screen in Topology Filter Wizard



Enter Community Constraints

To enter community constraints for a topology filter:

Step 1 Select one of the following options:

- If you do not wish to filter by Community, select **None** and click **Next**.

  or

- If you wish to filter by Community, select one of the following options:
  - **Equal—**Will return all entries that contain all the communities you entered.
  - **Not Equal—**Will return all entries that do not contain the communities you entered.
  - **Contains—**Will return all entries that contain any of the communities you entered.
  - **Not contains—**Will return all entries that do not contain any of the communities you entered.
  - **Starts with—**Will return all entries that start with any community you entered.
  - **Doesn't start with—**Will return all entries that do not start with any community you entered.
  - **Ends with—**Will return all entries that end with any community you entered.
  - **Doesn't end with—**Will return all entries that do not end with any community you entered.
  - **Matches—**Will return all entries that match any of the Java regular expression you entered
  - **Doesn't match—**Will return all entries that do not match any of the Java regular expression you entered

Note Communities are used to define routing policies. A *community attribute* is a set of *communities*. Each community is defined by a number.

Step 2 Enter each Community number and click **Add**.

Example: 90 **Add** 3 **Add** 14 **Add** 200 **Add**

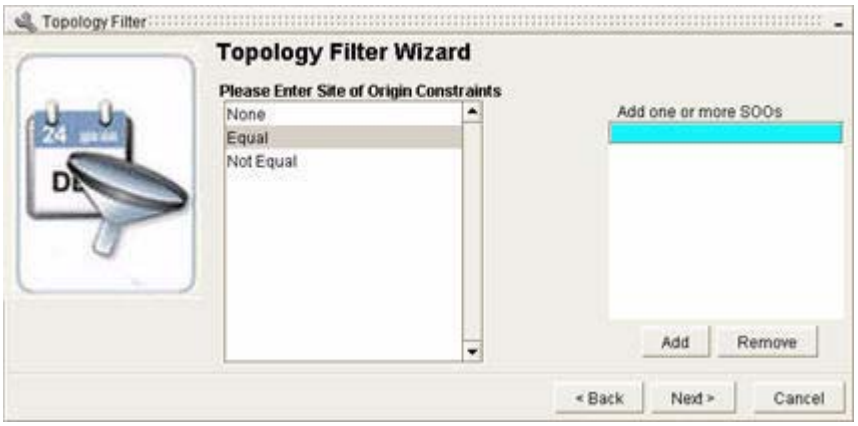
or

Step 3 Enter a Java regular expression and click **Add**.

Step 4 Click **Next**.

The Enter Site of Origin screen appears (see Figure 2-47).

Figure 2-47 Enter Site of Origin Constraints Screen in Topology Filter Wizard



Enter Site of Origin Constraints

To enter site of origin constraints for a topology filter:

Step 1 Select one of the following options:

- If you don't wish to filter by Site of Origin, select **None** and click **Next**.

  or

- If you wish to filter by Site of Origin you have the following choices:
  - **Equal—**Will return all entries that are equal to the Site of Origin value(s) you entered
  - **Not Equal—**Will return all entries that are not equal to the Site of Origin value(s) you entered

Step 2 Select one of these options, enter one or more Site of Origin value(s) and click **Add**.

Step 3 Click **Next**.

Finish the Topology Filter Wizard

After a few moments, you will receive the message: "Your filter parameters have been created. These settings will be applied to the current table." Click **Finish**.

A Topology Browser results dialog box appears with your query results, or a message that there are no matching results.

Data Entry Format for BGP Topology Filter Constraints

The Topology Filter Wizard for BGP allows you to query seven different types of tables using different constraints. See Table 2-9 for a listed of supported query types and their associated constraints.

A Topology Wizard screen lets you enter the search parameters for each type of constraint. Table 2-10 shows the acceptable data entry format(s) for each type of constraint.

Table 2-10 Data Entry Formats for BGP Topology Filter Constraints

Constraint Types	Data Entry Formats
Router ID	Example: 192.168.30.1 (used with Equal and Not equal) Example: 192.168.30.1/24 (Used with Included and Not included)
IP Prefix	Example: 192.168.30.1/24
IP Prefix Mask	Example: 24
VPN IP Prefix	Example: 10:10 192.168.30.1/24
VPN Prefix Mask Length	Example: 24
AS Path	Example: 100 Example: 101-102-103-104 Example: 2.–60136 (Java regular expression)
AS Path Length	Example: 3 Example: 23,149,2,3 (The second example is used with **Starts with Limited Length** and **Doesn't Start with Limited Length** options)
Next Hop	Example: 172.16.4.1
Origin	Example: Incomplete Example: IGP Example: EGP
Local Preference	Example: 6
Multi-Exit Discriminator (MED)	Example: 8
Community	Example: 100 Example: 2.–60136 (Java regular expression)
VRF ID	Example: 3:34
Route Target	Example: 2:30
Site of Origin	Example: 30:30

Making Routing Information Base (RIB) Comparisons for BGP Routes

You can compare routing tables for the following kinds of routes:

- IPv4 routes
- IPv4 multicast routes
- IPv4 VPN routes

within a specific domain, using the **RIB Comparison** icon in a Topology Browser Dialog box table.

See Navigating in Topology Browser Dialog Boxes, page 2-48.

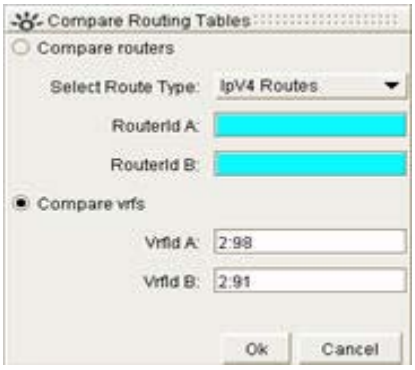
RIB Comparison Example: IPv4 Routes for VRFs

To see how a Routing Information Base (RIB) Comparison is performed, we will compare IPv4 routes for VRFs within a VPN Route List.

Step 1 Click the **RIB Comparison** icon in the Topology Browser toolbar:

The Compare Routing Tables screen appears (see Figure 2-48).

Figure 2-48 Compare Routing Tables Screen



Step 2 Click the **Compare vrfs** radio button.

Step 3 Select **IpV4 Routes** from the Select Route Type drop-down menu.

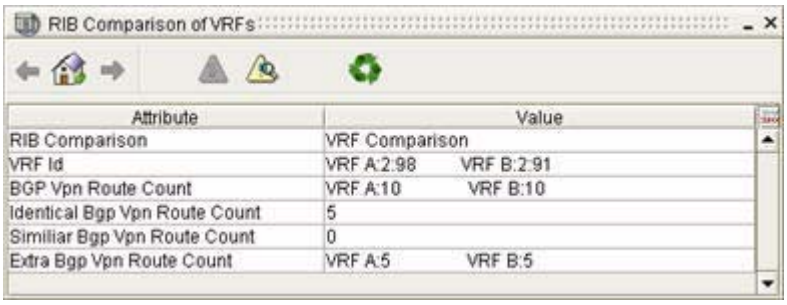
Step 4 Enter a valid VRF ID in the Vrfid A field.

Step 5 Enter a second valid VRF ID in the Vrfid B field.

Step 6 Click **OK**.

After the short time, a Topology Browser results dialog box appears with your query results, or a message that there are no matching results.

Figure 2-49 RIB Comparison Query Results Screen



The RIB Comparison results screen (see Figure 2-49) provides the following information:

- **RIB Comparison—**The type of comparison you selected: Router or VRF
- **VRF ID—**The VRFs you compared, shown as A: VRF ID and B: VRF ID
- **BGP VPN Route Count—**The total number of VPN routes in each VRF routing table.
- **Identical BGP VPN Route Count—**The total number of BGP VPN routes that have identical prefixes and attributes in both VRF tables.
- **Similar BGP VPN Route Count—**The total number of BGP VPN routes that have identical prefixes in both VRF tables.
- **Extra BGP VPN Route Count—**The total number of BGP VPN routes in one VRF table (A or B) not identical or similar to those in the other.

Querying for Network Elements (for OSPF Entities)

The Investigative Topology Browser wizard allows you to query enterprise-wide for a specific OSPF router, OSPF interface, or OSPF route advertisement.

Information returned can assist in determining:

- Connections to or from an interface
- Area in which an interface or route exists
- Metric of an interface or route
- Router that advertises a route

You can complete a fast, enterprise-wide query for information about a selected router, interface, or router advertisement. See Issue a Fast Query, page 2-83.

You can also issue a more detailed query across multiple routing domains to find information about one or more interfaces and route advertisements.

Related Tasks

- Issue a Fast Query, page 2-83
- Query for OSPF Interfaces, page 2-85
- Query for an OSPF Route Advertisement, page 2-90

Issue a Fast Query

To issue a fast query:

Step 1 Click **Start > Topology Browser > Investigative** from the Topology Browser toolbar.

Step 2 (Optional) Click the **Do not show this screen again** check box.

Step 3 Click **Next** in the initial wizard page.

The Select Type and Protocol Wizard Page of the Investigative Topology Browser Wizard appears (see Figure 2-50).

Figure 2-50 Select Type and Protocol in Investigative Topology Browser Wizard

Step 4 Click the **Enterprise Wide Search** radio button in the Choose Query Type field.

Step 5 Select the topology element to query:

- **Interface**—See Query for an OSPF Interface, page 2-84.
- **Route Advertisement**—See Query for a Route Advertisement, page 2-85.

Step 6 Select **Router** from the Enterprise Wide Search menu.

Step 7 Enter the unique identifier of the router you want to query in the Enter Router Name field. The unique identifier may include any of the following:

- Router ID
- DNS Name
- Router Name that your Path Analyzer administrator assigned to the router in the Domain Administration module

Example: `10.10.100.2`.

Note Don't click on the Advanced Interface Query or Advanced Route Advertisement Query radio buttons. These queries are discussed later. See Query for OSPF Interfaces, page 2-85 and Query for an OSPF Route Advertisement, page 2-90.

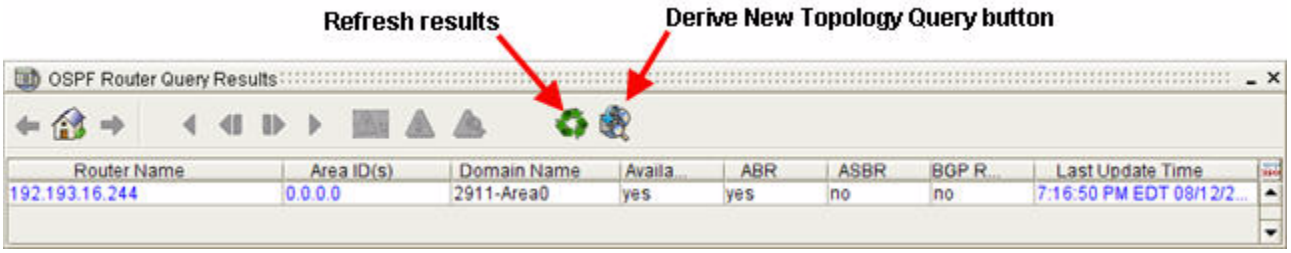
Step 8 Select **OSPF** (the protocol the selected router uses to advertise routing changes) in the Choose Protocol for Results field.

Step 9 Click **Next**.

Step 10 Click **Finish**.

The OSPF Router Query Results Wizard Page, page 2-146 appears, showing detailed information about the router (see Figure 2-51).

Figure 2-51 OSPF Router Query Results Wizard Page



Query for an OSPF Interface

To query for an OSPF interface:

Step 1 From the **Enterprise Wide Search** menu, select **Interface**.

Step 2 In the Enter IP Address or MIB Number field, enter the IP address or MIB index number of the interface you want to query.

Example: `10.10.100.21`.

Note Don't click on the Advanced Interface Query or Advanced Route Advertisement Query radio buttons. These queries are discussed later. See Query for OSPF Interfaces, page 2-85 and Query for an OSPF Route Advertisement, page 2-90.

Step 3 In the Choose Protocol for Results field, select the protocol the selected router uses to advertise routing changes: **OSPF**.

Step 4 Click **Next**.

Step 5 Click **Finish**.

The OSPF Interface Query Results Wizard Page, page 2-147 appears, showing detailed information about the interface.

Query for a Route Advertisement

To query for a route advertisement:

Step 1 Select **Advertisement** from the Enterprise Wide Search menu.

Step 2 Enter the prefix of the route advertisement you want to query in the Enter Prefix field.

Example: `10.10.100.2/24`.

Note Don't click on the Advanced Interface Query or Advanced Route Advertisement Query radio buttons. These queries are discussed later. See Query for OSPF Interfaces, page 2-85 and Query for an OSPF Route Advertisement, page 2-90.

Step 3 Select **OSPF** (the protocol the selected router uses to advertise routing changes) in the Choose Protocol for Results field.

Step 4 Click **Next**.

Step 5 Click **Finish**.

The OSPF Route Advertisement Query Results Wizard Page, page 2-148 appears, showing detailed information about the route.

Query for OSPF Interfaces

- Start the OSPF Interface Query, page 2-85
- Select the OSPF Domain, page 2-86
- Select OSPF Routers, page 2-87
- Specify the Interface or its Prefix, page 2-88
- (Optional) Specify Additional OSPF Interface Query Constraints, page 2-89
- Finish the Wizard, page 2-88

Start the OSPF Interface Query

To start the OSPF query:

Step 1 Click **Start** > **Topology Browser** > **Investigative**.

Step 2 (Optional) Click the **Do not show this screen again** check box.

Step 3 Click **Next** in the initial wizard page.

The Select Type and Protocol Wizard Page of the Investigative Topology Browser Wizard opens.

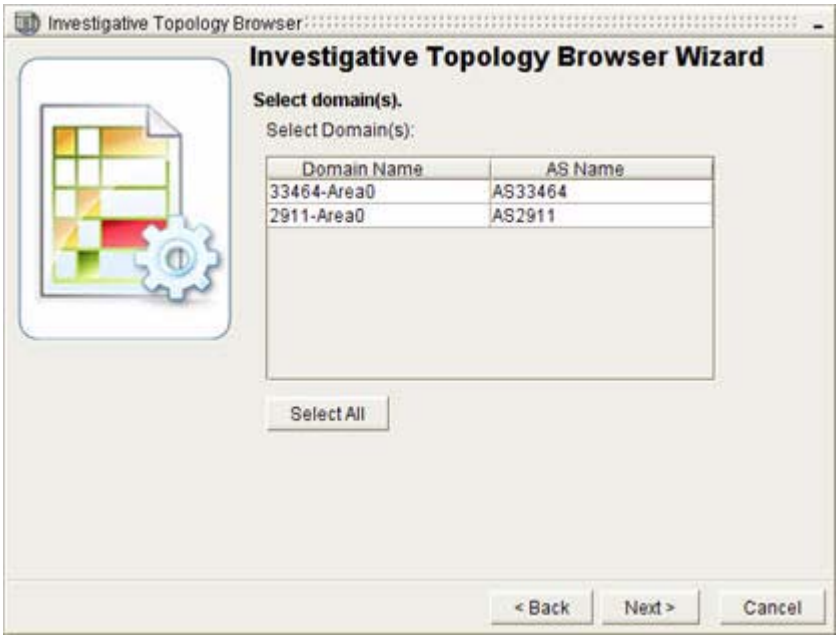
Step 4 Select **Advanced Interface Query** in the Choose Query Type field.

Step 5 Select **OSPF** in the Choose Protocol for Results field.

Step 6 Click **Next**.

The Domain Selection Wizard appears (see Figure 2-52).

Figure 2-52 Select Domain in Investigative Topology Browser Wizard



Select the OSPF Domain

To select the OSPF domain:

Step 1 Select one or more domains in the Select Domain(s) field:

- Keep all selections.

  or

- Click **Deselect All** to deselect all listed domains.

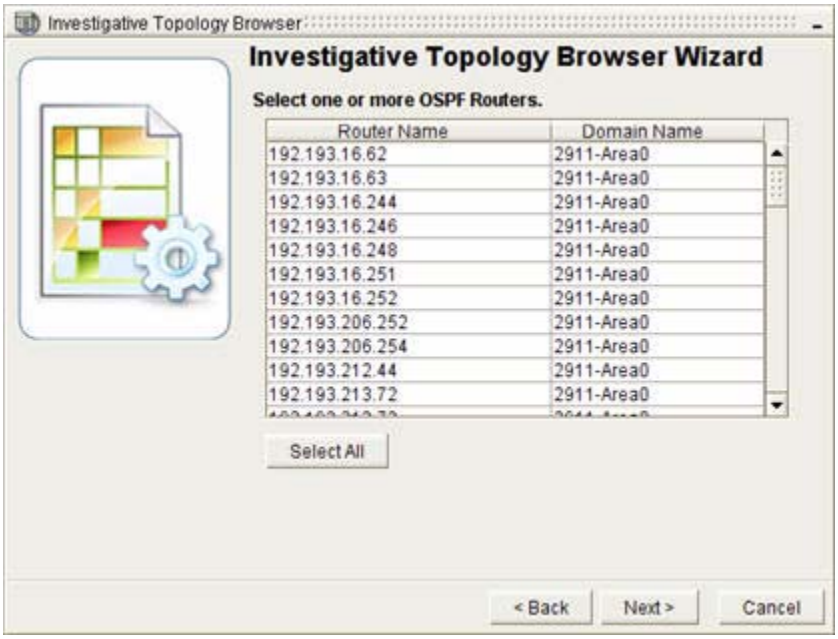
  Press Ctrl and click more than one domain to select specific domains.

Note Selecting routing domains reduces the amount of data the Path Anaylzer Server returns, which in turn, reduces the amount of bandwidth and processing power required by the Path Anaylzer Server to retrieve the data and by the Management Console to present it. The fixed set of data returned allows you to view and analyze a smaller, more specific set of information.

Step 2 Click **Next**.

The OSPF Routers Selection Wizard Page appears (see Figure 2-53).

Figure 2-53 Select OSPF Routers in Investigative Topology Browser Wizard



Select OSPF Routers

To select OSPF routers:

Step 1 Select one or more routers in the Select OSPF Router(s) field:

- Keep all selections.

  or

- Click **Deselect All** to deselect all listed routers.

  Press Ctrl and click more than one router to select specific routers.

Step 2 Click **Next**. The OSPF Interface Query Wizard Page appears (see Figure 2-54).

Figure 2-54 Specify and OSPF Interface Query in Investigative Topology Browser Wizard

Specify the Interface or its Prefix

To specify the interface or its prefix:

Step 1 In the Choose Interface Query Mode field:

- Select **Is An Exact IP Address/MIB No. Match** if you know the IP address or MIB index number of the interface.
- In the Enter IP Address or MIB No. field, enter the IP address or MIB index number of the interface.

  Example: `10.10.100.1`

  or
- Select **IP Address Falls Within Prefix** if you are certain about the prefix but uncertain about the actual IP address of the interface.
- In the Enter Prefix field, enter the prefix that includes the interface.

  Example: `10.10.2.1/24`

Step 2 (Optional) Specify Additional OSPF Interface Query Constraints, page 2-89.

Finish the Wizard

To finish the wizard:

Step 1 Click **Next**.

Step 2 Click **Finish**.

The OSPF Interface Query Results Wizard Page, page 2-147 page appears, showing detailed information about the interface (see Figure 2-55).

Specify Additional OSPF Interface Query Constraints

The Qualify Interface Query By Attributes Wizard Page allows you to query for granular details of an OSPF interface.

Figure 2-55 Qualify OSPF Interface Query in Investigative Topology Browser Wizard

Note You can set the query to ignore an attribute by selecting **Not Applied** from the menu of an attribute.

To specify additional OSPF interface query constraints:

Step 1 Select **Is One Of** from the OSPF Interface Types menu, if you know the type of interface you want to query.

Step 2 Select one or more of the following options by click the associated check box(s):

- **NP2P Interface**
- **UP2P Interface**
- **Transit Interface**

Step 3 Select **Equal To** from the Availability menu, if you know the status of the interface.

Step 4 Select one of the following options:

- **Available**
- **Unavailable**

Step 5 Select one of the following options from the Metric menu, if you know the metric of the interface:

- **Equal To**

- **Less Than**
- **Greater Than**
- **Less Than Or Equal To**
- **Greater Than Or Equal To**
- **Within Range—**Enter the **Within Range** value following the format *<Number - Number>*.

  Example: 1 - 5

Step 6 Enter the value of the metric or range in which the metric falls in the Metric field.

Step 7 Click **Next**.

Step 8 Click **Finish**.

The OSPF Interface Query Results Wizard Page, page 2-147 page appears, showing detailed information about the interface.

Query for an OSPF Route Advertisement

- Start the OSPF Route Query, page 2-90
- Select the OSPF Domain, page 2-90
- Select OSPF Routers, page 2-91
- Specify the OSPF Route Prefix or Range, page 2-92
- **Optional:** Specify Additional Advertisement Query Constraints, page 2-93
- Finish the Wizard, page 2-92

Start the OSPF Route Query

To start the OSPF route query:

Step 1 Click **Start > Topology Browser > Investigative.**

Step 2 (Optional) Click the **Do not show this screen again** check box.

Step 3 Click **Next** in the initial wizard page.

The Select Type and Protocol Wizard Page of the Investigative Topology Browser Wizard opens.

Step 4 Select **Advanced Route Advertisement Query** in the Choose Query Type field.

Step 5 Select **OSPF** in the Choose Protocol for Results field.

Step 6 Click **Next**.

The Domain Selection Wizard Page appears.

Select the OSPF Domain

To select the OSPF domain:

Step 1 Select one or more domains in the Select Domain(s) field:

- Keep all selections.

  or

- Click **Deselect All** to deselect all listed domains.

  Press Ctrl and click more than one domain to select specific domains.

Note Selecting routing domains reduces the amount of data the Path Anaylzer Server returns, which in turn, reduces the amount of bandwidth and processing power required by the Path Anaylzer Server to retrieve the data and by the Management Console to present it. The fixed set of data returned allows you to view and analyze a smaller, more specific set of information.

Step 2 Click **Next**.

The OSPF Routers Selection Wizard Page appears.

Select OSPF Routers

To select OSPF routers:

Step 1 Select one or more routers in the Select OSPF Router(s) field:

- Keep all selections.

  or

- Click **Deselect All** to deselect all listed routers.

  Press Ctrl and click more than one router to select specific routers.

Step 2 Click **Next**.

The OSPF Route Advertisement Query Wizard Page appears (see Figure 2-56).

Figure 2-56 Specify OSPF Route Advertisement in Investigative Topology Browser Wizard

Specify the OSPF Route Prefix or Range

To specify the OSPF prefix or range:

Step 1 In the Choose Route Advertisement Query Mode field:

- Select **All OSPF Route Advertisements**.

  or

- Select **Is An Exact Prefix Match For** if you know the prefix of the route advertisement.

  or

- Select **Is the Longest Prefix Match:**
  - **By Router**
  - **By Domain**

  or

- Select **Is a [More | Less] Specific Prefix Than**
  - In the **Enter Prefix** field, enter the prefix.

    Example: `10.10.100.0/24`

Step 2 (Optional) See Specify Additional Advertisement Query Constraints, page 2-93.

Finish the Wizard

To finish the wizard:

Step 1 Click **Next**.

Step 2 Click **Finish**.

The OSPF Route Advertisement Query Results Wizard Page, page 2-148 appears, showing detailed information about the interface returned by the query.

Specify Additional Advertisement Query Constraints

The Qualify Advertisement Query By Attributes Wizard Page allows you to query for granular details of an OSPF route advertisement. You can set the query to ignore an attribute by selecting **Not Applied** from the menu of an attribute (see Figure 2-57).

Figure 2-57 Quality OSPF Route Advertisement Query by Attributes in Investigative Topology Browser Wizard

To specify additional query constraints:

Step 1 Select **Is One Of** from the OSPF Advertisement Types menu, if you know the type of advertisement you want to query.

Step 2 Select one or more of the following options:

- **Transit Network**
- **Stub Route Advertisement**
- **External Route Advertisement**
- **T3 Summary Route Advertisement**
- **T4 Summary Route Advertisement**

Step 3 Select one of the following options from the Metric menu, if you know the metric announced in the route advertisement:

- **Equal To**

- **Less Than**
- **Greater Than**
- **Less Than Or Equal To**
- **Greater Than Or Equal To**
- **Within Range** (No.- No.)—Enter the Within Range value following the format <Number - Number>.

  Example: 1- 5

Step 4 Enter the value of the metric or range in which the metric falls in the Metric field.

Step 5 Click **Next**.

Step 6 Click **Finish**.

The OSPF Interface Query Results Wizard Page, page 2-147 dialog box appears, showing detailed information about the interface returned by the query.

Use a Query as a Template for a New Query

You can use an existing query as the template for a new query.

If you are using an existing OSPF Interface query, you will complete the following steps:

- Start the OSPF Interface Query, page 2-85
- Select the OSPF Domain, page 2-86
- Select OSPF Routers, page 2-87
- Specify the Interface or its Prefix, page 2-88
- (Optional) Specify Additional OSPF Interface Query Constraints, page 2-89
- Finish the Wizard, page 2-88

If you are using an existing OSPF route advertisement query, you will complete the following steps:

- Start the OSPF Route Query, page 2-90
- Select the OSPF Domain, page 2-90
- Select OSPF Routers, page 2-91
- Specify the OSPF Route Prefix or Range, page 2-92
- **Optional:** Specify Additional Advertisement Query Constraints, page 2-93
- Finish the Wizard, page 2-92

Derive a Query

To derive a query:

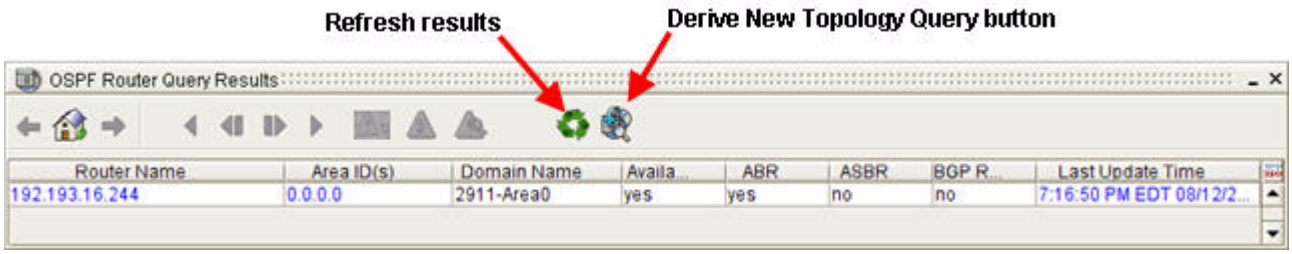
Step 1 Click the **Derive New Topology Query** button from the toolbar of the Topology Browser dialog box that presents the results of your query (see Figure 2-58).

The Investigative Topology Browser Wizard appears, enabling you to create a new query.

Step 2 Select the type of query:

- Query for an OSPF Interface, page 2-84
- Query for a Route Advertisement, page 2-85

Figure 2-58 OSPF Router Query Results



Refresh Values in a Topology Browser Dialog Box

To refresh values in a Topology Browser dialog box, click the **Refresh Results** button in the toolbar of the Topology Browser dialog box that presents the results of your query.

The Topology Browser dialog box is updated with the latest values returned for options you selected to query.

Previewing and Printing a Topology

You can preview and print maps from the Topology Viewer:

- Creating a Map File, page 2-95
- Preview a Map, page 2-95
- Print the Map, page 2-96

Creating a Map File

You can save a configuration displayed in the Flat or Hierarchical Topology Viewer as a map file. After you save the map configuration, you can preview and print it.

For information about saving the topology as a map, see Save a Topological Layout, page 2-42.

Preview a Map

To preview a map, click **Print Preview** in the Topology Viewer Toolbar, page 2-97. The Print Preview dialog box appears, showing a preview image of the Topology Viewer or a Topology Browser dialog box.

View the map before printing to determine whether you want to print the map based on its layout and appearance.

Print the Map

The print feature requires that a printer is configured for your system. If you try to print and a printer is not configured, a message is displayed, indicating that the printer is not available.

To print the map:

Step 1 Click **Print** in the Topology Viewer Toolbar, page 2-97.

The Print dialog box appears.

Step 2 Select the print properties you want to use, then click **OK**.

The document is sent to the printer.

Related Forms

This section contains tables that detail the various forms, fields, buttons, icons, and other components of the Topology Viewer.

Topology Viewer

The Topology Viewer is divided into the following three tabs:

- Hierarchical Topology Viewer
- Flat Topology Viewer
- Service Viewer

The Topology Viewer displays your network's topology and the state of configured areas, routers, and other network elements.

In the Topology Viewer, you can complete the following tasks:

- Starting the Topology Viewer, page 2-4
- Viewing Your Network Topology, page 2-6
- Viewing Changes of Status, page 2-13
- Identifying Topology Viewer Elements, page 2-14
- Navigating in the Topology Viewer, page 2-32
- Viewing Services in the Service Viewer, page 2-45
- Getting Detailed Information About Topology Viewer Elements, page 2-45
- Navigating in Topology Browser Dialog Boxes, page 2-48
- Viewing Metrics and Attributes, page 2-54
- Pivoting to the Event Log, page 2-64
- Querying for Network Elements (for OSPF Entities), page 2-82
- Previewing and Printing a Topology, page 2-95

Topology Viewer Toolbar

Figure 2-59 Topology Viewer Toolbars

Buttons provided in Flat Topology Viewer and Hierarchical Viewer

Buttons provided in Service Viewer only

Clicking the buttons on the Topology Viewer toolbar (see Figure 2-59), you can complete the following tasks:

- View an Exploratory Path, page 2-9
- Zoom from the Toolbar, page 2-37

Table 2-11 provides descriptions of the buttons provided in the Topology Viewer toolbar.

Table 2-11 Topology Viewer Toolbar Button Descriptions

Button	Name	Description
	Apply Layout Apply Service	Opens the Choose a Layout to Apply Dialog Box, page 2-102 in which you can select a layout of topology elements that you saved previously to apply in the Flat or Hierarchical Topology Viewer. **Note:** In the Service Viewer, this button is labeled Apply Service. See Set the Default Flat Layout, page 1-25 and Set the Default Hierarchical Layout, page 1-26.
	Save Current Layout	Opens the Choose a Layout to Save Dialog Box, page 2-102 in which you can save a layout from the Flat or Hierarchical Topology Viewer. See Save the Layout, page 2-42 and Remove a Topological Layout, page 2-42.
	Remove Layout	Opens the Choose a Layout to Remove Dialog Box, page 2-103 in which you can remove a layout. See Remove a Layout, page 2-42 and Remove a Topological Layout, page 2-42
	Select Mode	Allows you to select a topology element, such as a network, router, or link in the Topology Viewer.

Table 2-11 Topology Viewer Toolbar Button Descriptions (continued)

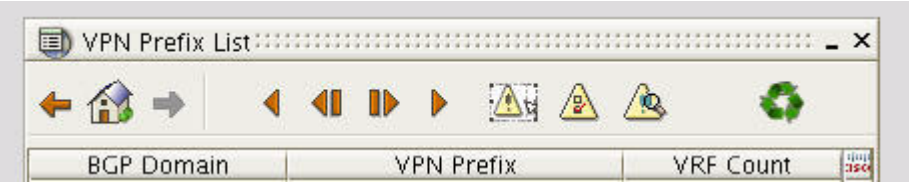
Button	Name	Description
	Zoom Mode	Allows you to zoom in on a selected portion of the Topology Viewer to view the area in more detail. See Zoom from the Toolbar, page 2-37.
	Interactive Zoom Mode	Allows you to zoom in or out from the Topology Viewer to change your viewing perspective. Generally, dragging the zoom cursor in a downwards motion zooms in on the Topology Viewer. Dragging the zoom cursor in an upwards motion zooms out from the Topology Viewer. See Zoom from the Toolbar, page 2-37.
	Print Preview Topology	Previews an image of your network map before printing it. See View All OSPF Routers in an AS, page 2-56.
	Print Topology	Prints the Topology Viewer. See Print the Map, page 2-96.
The following buttons are available in the toolbar of the Flat and Hierarchical Topology Viewers, but not in the Service Viewer:		
	Refresh Layout	Arranges your network topology in a symmetrical manner and refreshes the Topology Viewer layout with the latest real-time view. See Refresh the Layout, page 2-41.
	Configure Exploratory Path	Opens the Exploratory Path Configuration dialog box in which you enter the originating gateway and final destination of a path to view it graphically in the Topology Viewer. See View an Exploratory Path, page 2-9.
	Hide Unavailable Elements	Causes unavailable routers or networks to be hidden when they become unavailable.
	Show Unavailable Elements	Shows unavailable routers or networks in the Flat or Hierarchical Topology Viewer.
	Hide Edge Routers	Causes edge routers to be hidden in the Flat or Hierarchical Topology Viewer. This option is useful for reducing the number of routers displayed and to focus on a specific set of routers.
	Show Edge Routers	Shows edge routers. This option is useful when you want to see all the routers in your network topology.

Topology Browser Dialog Boxes

The Topology Browser dialog boxes provide you with attributes and values of one topology element, such as a selected router, or of a list of topology elements, such as all routers in the map. See Navigating in Topology Browser Dialog Boxes, page 2-48.

Topology Browser Toolbar

Figure 2-60 Toolbar of Topology Browser Dialog Boxes



By clicking the icons on the Topology Browser toolbar (Figure 2-60) and on the column heads, you can complete the following tasks:

- Browse Backward, page 2-48
- Browse Forward, page 2-48
- Enterprise Overview, page 2-50
- Get First, Previous, Last, and Next Entities, page 2-49
- Select the Number of Rows to Display, page 2-50
- Specify the Filter for the Current Table, page 2-50
- Router Information Base (RIB) Comparison, page 2-50
- Refresh Results, page 2-51
- Derive New Topology Query, page 2-51
- Sort Data in a Column, page 2-52
- Sort Rows by Increasing Value, page 2-54
- Sort Rows by Decreasing Value, page 2-54
- Move the Sort Arrow, page 2-54

Table 2-12 provides descriptions of the buttons provided in the toolbar of the Topology Browser dialog boxes.

Table 2-12 Topology Browser Toolbar Button Descriptions

Button	Name	Description
 	Browse Backward (Active) Browse Backward (Inactive)	Browses backward through a series of open Topology Browser dialog boxes. Functions in the same manner as the **Previous** or **Back** button in a Web browser. The **Browse Backward** icon is inactive until you click a link in a Topology Browser dialog box, which starts a new series. See Browse Backward, page 2-48.
	Home—Go to Enterprise Overview	Opens the BGP Router List Dialog Box, page 2-108, in which you can view attributes, such as the number of routers or routes, in the entire network.
 	Browse Forward (Active) Browse Forward (Inactive)	Browses forward through a series of open dialog boxes. Functions in the same manner as the **Next** or **Forward** button in a Web browser. The **Browse Forward** icon is inactive until you click the active Topology Browser icon. Both icons can be active at the same time when a series of dialog boxes is open, with the possibility to browse forward or backward through the series. See Browse Forward, page 2-48 and Browse Backward, page 2-48.
 	Get First Entities (Active) Get First Entities (Inactive)	Displays the first "x" entities, where x is the number of entities specified using the **Select the Number of Rows to Display** icon (see below).
 	Get Previous Entities (Active) Get Previous Entities (Inactive)	Displays the previous "x" entities, where x is the number of entities specified using the **Select the Number of Rows to Display** icon (see below).

Table 2-12 Topology Browser Toolbar Button Descriptions (continued)

Button	Name	Description
 	Get Last Entities (Active) Get Last Entities (Inactive)	Display the last "x" entities where x is the number of entities specified using the **Select the Number of Rows to Display** icon (see below).
 	Get Next Entities (Active) Get Next Entities (Inactive)	Displays the next "x" entities, where x is the number of entities specified using the **Select the Number of Rows to Display** icon (see below).
	Select the Number of Rows to Display	Allows you to enter the number of rows to display (5-100).
	Specify a Filter for the Current Table	Lets you filter the table for the specific information you are seeking. The particular screens that appear will depend on the nature of the table you are viewing. See Using the Topology Filter Wizard for BGP Entities, page 2-65.
	Router Information Base (RIB) Comparison	You can compare routing tables for the following kinds of routes within a specific domain: IPv4 routes IPv4 multicast routes IPv4 VPN routes See Making Routing Information Base (RIB) Comparisons for BGP Routes, page 2-81.

Table 2-12 Topology Browser Toolbar Button Descriptions (continued)

Button	Name	Description
	Derive New Topology Query	Issues a new query from the Topology Browser dialog box that presents results of a previous query. This button only appears in query result dialog boxes. See Derive a Query, page 2-94.
	Refresh Results	Refreshes values displayed in a Topology Browser dialog box. See Refresh Results, page 2-51.

Choose a Layout to Apply Dialog Box

In the Choose a Layout to Apply dialog box, you can select a layout to apply in the Flat or Hierarchical Topology Viewer.

See Set the Default Flat Layout, page 1-25 and Set the Default Hierarchical Layout, page 1-26.

Table 2-13 describes the fields of the Choose a Layout to Apply dialog box.

Table 2-13 Choose a Layout to Apply Dialog Box

Field or Button	Description
Default Layout	Provides a default layout and space for newly-configured and saved layouts.
Layout Name	Allows you to enter the name of a layout to restore.
Apply	Saves your selections.
Cancel	Cancels your selections without saving changes.

Choose a Layout to Save Dialog Box

In the Choose a Layout to Save dialog box, you can select a layout to save in the Flat or Hierarchical Topology Viewer.

See Apply a Topological Layout, page 2-43 and Hide and Show Routers and Topology Elements, page 2-43.

Table 2-14 describes the fields of the Choose a Layout to Save dialog box.

Table 2-14 Choose a Layout to Save Dialog Box

Field or Button	Description
Default Layout	Provides a default layout and space for newly configured and saved layouts.
Layout Name	Allows you to enter the name of a layout to restore.

Table 2-14 Choose a Layout to Save Dialog Box (continued)

Field or Button	Description
Apply	Saves your selections.
Cancel	Cancels your selections without saving changes.

Choose a Layout to Remove Dialog Box

In the Choose a Layout to Remove dialog box, you can select a layout to remove in the Flat or Hierarchical Topology Viewer.

See Remove a Layout, page 2-42 and Remove a Topological Layout, page 2-42.

Table 2-15 describes the fields of the Choose a Layout to Remove dialog box.

Table 2-15 Choose a Layout to Remove Dialog Box

Field or Button	Description
Default Layout	Provides a default layout and space for newly-configured and saved layouts.
Layout Name	Allows you to enter the name of a layout to remove.
Apply	Saves your selections.
Cancel	Cancels your selections without saving changes.

Enterprise Overview Dialog Box

When you select **Start > Topology Browser > Real-time** the Enterprise Overview dialog box opens. This dialog box provides a high-level summary of your enterprise.

Also, in any Topology Browser dialog box, click the **Home** icon to return to the Enterprise Overview dialog box.

In the Enterprise Overview dialog box, you can View Details of the Enterprise Network, page 2-54.

Table 2-16 describes the fields and buttons of the Enterprise Overview dialog box.

Table 2-16 Enterprise Overview Dialog Box

Field	Description
Enterprise ID	Shows the identifier of your enterprise network.
Total Bgp Domain Count	Shows the total number of BGP domains in the enterprise. Clicking on the Total Bgp Domain Count value opens the Autonomous System List Dialog Box, page 2-104.
Total BGP Router Count	Shows the total number of BGP routers in the enterprise. Clicking the Total BGP Router Count value opens the BGP Router List Dialog Box, page 2-108.

Autonomous System List Dialog Box

When you click the Total Bgp Domain Count value in the Enterprise Overview Dialog Box, page 2-103, the Autonomous System List dialog box opens. This dialog box lists the autonomous systems that make up your enterprise network.

From the Autonomous System List dialog box, you can View All Autonomous Systems in the Enterprise Network, page 2-55.

Table 2-17 describes the fields and buttons of the Autonomous System List dialog box.

Table 2-17 Autonomous System List Dialog Box

Field	Description
BGP Domain	Shows the name of the domain. Clicking the BGP Domain link opens the BGP Domain Details Dialog Box, page 2-106.
BGP Router Count	Shows the number of routers in each domain. Clicking the BGP Router Count link opens the BGP Router List Dialog Box, page 2-108.
IPV4 Prefix Count	Shows the number of IPV4 prefixes in each domain. Clicking the IPV4 Prefix Count link opens the IPV4 Prefix List Dialog Box, page 2-141.
IPV4 Multicast Prefix Count	Shows the number of IPV4 multicast prefixes in each domain. Clicking the IPV4 Multicast Prefix Count link opens the IPV4 Multicast Prefix List Dialog Box, page 2-142.
VPN Prefix Count	Shows the number of VPN prefixes in each domain. Clicking the VPN Prefix Count link opens the VPN Prefix List Dialog Box, page 2-146.

OSPF Domain Details Dialog Box

When you click the IGP Domain value in the BGP Domain Details Dialog Box, page 2-106, the OSPF Domain Details dialog box open, showing summary information about the routers, routes, and interfaces within the domain.

Also, click the Domain Name attribute in any Topology Browser dialog box that has it, to return to the OSPF Domain Details dialog box.

In the OSPF dialog box, you can View Details of an Autonomous System, page 2-55.

Table 2-18 describes the fields and buttons of the OSPF Domain Detail dialog box.

Table 2-18 OSPF Domain Details Dialog Box

Field	Description
The (Available / Total) parameter after any of the following fields indicates that the two attribute values show the number of available entities out of all entities. For example, if the No. ABRs (Available / Total) value is 5 / 7, it indicates that 5 ABRs are available out of a total of 7 ABRs.	
AS ID	Shows the unique identifier of the autonomous system. Clicking the AS Id link opens the BGP Router List Dialog Box, page 2-108.
Total Area Count (Available/Total)	Shows the available number of areas contained in the autonomous system's domain out of the total number of area contained in the autonomous system's domains. Clicking the Total Area Count value for the number of Areas opens the Area List for Domain Dialog Box, page 2-109.
Total OSPF Router Count	Shows the total number of OSPF routers in the autonomous system. Clicking the Total OSPF Router Count link opens the Domain OSPF Router List Dialog Box, page 2-113.
Avg. OSPF Router Count	Shows the average number of available OSPF routers in the autonomous system.
Avg. OSPF Router Event Rate	Shows the baseline rate of OSPF router events in the autonomous system over a span of time.
Current OSPF Router Event Rate	Shows the instantaneous rate of OSPF router events on routers in the autonomous system. This value indicates the number of events that "just happened" in real-time.
No. ABR's	Shows the number of available ABRs compared to the total number of ABRs in the autonomous system.
No. ASBR's	Shows the number of available ASBRs compared to the total number of ASBRs in the autonomous system.
No. Internal Routers (Available/Total)	Shows the number of available internal routers compared to the total number of internal routers in the autonomous system.
Total OSPF Interface Count (Available/Total)	Shows the available number of OSPF interfaces in the autonomous system compared to the total number of OSPF interfaces in the autonomous system. Clicking the Total OSPF Interface Count link opens the Domain OSPF Interface List Dialog Box, page 2-115.
Avg. OSPF Interface Count	Shows the average number of available OSPF interfaces in the autonomous system.
Avg. OSPF Interface Event Rate	Shows the baseline rate of OSPF interface events in the autonomous system over a span of time.

Table 2-18 OSPF Domain Details Dialog Box (continued)

Field	Description
Current OSPF Interface Event Rate	Shows the instantaneous rate of OSPF interface events on routers in the autonomous system. This value indicates the number of events that "just happened" in real-time.
No. NP2P IFs	Shows the number of available Numbered Point-to-Point (NP2P) interfaces compared to the total number of NP2P interfaces in the autonomous system.
No. UP2P IFs	Shows the number of available Unnumbered Point-to-Point (UP2P) interfaces compared to the total number of UP2P interfaces in the autonomous system.
No. Transit IFs (Available/Total)	Shows the number of available transit interfaces compared to the total number of transit interfaces in the autonomous system.
No. Transit to Router Links (Available/Total)	Shows the number of available Transit-to-Router links compared to the total number of Transit-to-Router links in the autonomous system.
Total OSPF Route Count	Shows the total number of OSPF routes in the autonomous system. Clicking the Total Route Count link opens the Domain OSPF Route List Dialog Box, page 2-114.
Avg. OSPF Route Count	Shows the average number of available OSPF routes in the autonomous system.
Avg. OSPF Route Event Rate	Shows the baseline rate of OSPF route events in the autonomous system over a span of time.
Current OSPF Route Event Rate	Shows the instantaneous rate of OSPF route events on routers in the autonomous system. This value indicates the number of events that "just happened" in real-time.
No. Stub Routes	Shows the number of available Stub routes compared to total number of Stub routes in the autonomous system.
No. External Routes	Shows the number of External routes in the autonomous system. These routes are advertised in Type 5 LSAs by all ASBRs in the autonomous system.
No. Transit Networks (Available/Total)	Shows the number of available Transit networks compared to the total number of Transit networks in the autonomous system.

BGP Domain Details Dialog Box

When you right-click on an Autonomous System and select **Show Overview**, the BGP Domain Details dialog box opens. You can also open this dialog box by clicking on an entry in the BGP Domain column in the Autonomous System List dialog box on Autonomous System List Dialog Box, page 2-104.

The BGP Domain Details dialog box provides an overview of your BGP routers and routes, as well as a link to OSPF domain details.

Table 2-19 describes the fields of the BGP Domain Details dialog box.

Table 2-19 BGP Domain Details Dialog Box

Field	Description
BGP Domain Name	Shows the name of the BGP domain.
IGP Domain	Provides a link to the OSPF domain. Clicking the IGP Domain link opens the OSPF Domain Details Dialog Box, page 2-104.
BGP Router Count	Shows the number of routers in the domain. Clicking the BGP Router Count link opens the BGP Router List Dialog Box, page 2-108.
IPv4 Prefix Count	Shows the number of IPV4 prefixes in the domain. Clicking the IPv4 Prefix Count link opens the IPV4 Prefix List Dialog Box, page 2-141.
IPv4 Route Count	Shows the number of IPV4 routes in the domain.
IPv4 Mask Map	Links to a list showing the number of routes for each IPV4 mask map length (1-32). Clicking the IPv4 Mask Map link opens the opens the BGP Mask Length Map Dialog Box, page 2-109.
IPv4 Routes	Links to more statistics about IPV4 routes. Clicking the IPv4 Routes link opens the BGP Statistics Dialog Box, page 2-140.
IPv4 Multicast prefix Count	Shows the number of IPV4 multicast prefixes in the domain. Clicking the IPv4 Multicast Prefix Count link opens the IPV4 Multicast Prefix List Dialog Box, page 2-142.
IPv4 Multicast Route Count	Shows the number of IPV4 multicast routes in the domain.
IPv4 Multicast Mask Map	Links to a list showing the number of routes for each IPV4 multicast mask map length (1-32). Clicking the IPv4 Multicast Mask Map link opens the BGP Mask Length Map Dialog Box, page 2-109.
IPv4 Multicast Routes	Links to more statistics about IPV4 multicast routes. Clicking the IPv4 Multicast Routes link opens the BGP Statistics Dialog Box, page 2-140.
VPN Prefix Count	Shows the number of IPV4 prefixes in the domain. Clicking the VPN Prefix Count link opens the VPN Prefix List Dialog Box, page 2-146.
VPN Route Count	Shows the number of VPN routes in the domain.
VPN Mask Map	Links to a list showing the number of routes for each VPN mask map length (1-32). Clicking the VPN Mask Map link opens the BGP Mask Length Map Dialog Box, page 2-109.

Table 2-19 BGP Domain Details Dialog Box

Field	Description
VPN Routes	Shows the number of VPN routes in the domain. Clicking the VPN Routes link opens the BGP Statistics Dialog Box, page 2-140.
VRF Count	Shows the number of VRFs in the domain.
Last Update Time	Shows the date and time of the most recent change to the router in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

BGP Router List Dialog Box

When you click the BGP Router Count value in the BGP Domain Details Dialog Box, page 2-106, the BGP Router List dialog box opens, showing information about all routers that advertise a destination route over BGP.

Table 2-20 describes the fields and buttons of the BGP Router List dialog box.

Table 2-20 BGP Router List Dialog Box

Field	Description
BGP Domain Name	Shows the unique identifier of the autonomous system in which the BGP speaker resides and advertises the route. Clicking the AS Name link opens the BGP Domain Details Dialog Box, page 2-106.
BGP Router Name	Shows the Router ID, DNS Name, or user-defined router name that advertises the destination route over BGP. Clicking the Router Name link opens the BGP Router Details Dialog Box, page 2-121.
BGP Router Id	Shows the Router ID of the BGP router.
IPV4 Route Count	Shows the number of IPV4 routes associated with each router. Clicking the IPV4 Route Count value opens the IPV4 Routes for a Router Dialog Box, page 2-142.
VPN Route Count	Shows the number of VPN routes associated with each router. Clicking the IPV4 Route Count value opens the VPN Route List Dialog Box, page 2-145.

BGP Mask Length Map Dialog Box

When you click the IPV4, IPV4 Multicast, or VPN Mask Map value in the BGP Domain Details Dialog Box, page 2-106, the BGP Mask Length dialog box opens, showing you the associated number of IPV4 unicast routes for each mask length (1–32).

Table 2-21 describes the fields of the BGP Mask Length Map dialog box.

Table 2-21 BGP Mask Length Map Dialog Box

Field	Description
Mask Lengths	Shows the number of digits in the subnet mask (1–32).
The field below will vary depending on whether the IPV4, IPV4 Multicast, or VPN Mask Map value in the BGP Domain Details Dialog Box, page 2-106 was selected.	
IPV4-UNICAST Route Count	Shows the number of IPV4 unicast routes associated with each subnet mask length.
IPV4-MULTICAST Route Count	Shows the number of IPV4 multicast routes associated with each subnet mask length.
IPV4-VPN Route Count	Shows the number of IPV4 VPN routes associated with each subnet mask length.

Area List for Domain Dialog Box

Clicking the Area ID link in the Area Overview Dialog Box, page 2-117 opens the Area List for Domain dialog box, which lists the Area Identifiers of all areas in the autonomous system.

You can also open the Area List for Domain dialog box by clicking the Total Area Count value in the OSPF Domain Details Dialog Box, page 2-104.

Table 2-22 describes the fields of the Area List for Domain dialog box.

Table 2-22 Area List for Domain Dialog Box

Field	Description
Area ID(s)	Shows the unique identifier of the OSPF area in which the router resides.

Area OSPF Router List Dialog Box

When you click the Total Router Count value in the Area Overview Dialog Box, page 2-117, the Area OSPF Router List dialog box appears, showing information about all routers in the area.

From the Area OSPF Router List dialog box, you can View All OSPF Routers in an AS, page 2-56.

For information about the types of routers displayed in the area, see Routers, page 2-21.

For information about viewing routes of a selected router, see View Route Advertisements Announced by a Specific Router, page 2-61.

Table 2-23 describes the fields and buttons of the Area OSPF Router List dialog box.

Table 2-23 Area OSPF Router List

Field	Description
Router Name	Shows the Router Id, DNS name, or user-defined name of a router in the area. Clicking the Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area ID(s)	Shows the unique identifier of the OSPF area in which the router resides. Clicking an Area ID link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the identifier of the autonomous system in which the router resides.
Available	Shows the status of the router: **Yes**—Router is forwarding packets. **No**—Router is incapable of forwarding packets.
ABR	Shows whether the given router is an ABR: **Yes**—Indicates that the router is an ABR. **No**—Indicates that the router is not an ABR.
ASBR	Shows whether the selected router is an ASBR **Yes**—Indicates that the router is an ASBR. **No**—Indicates that the router is not an ASBR.
BGP Router	Shows whether the router is configured with a BGP interface, enabling it to advertise and receive routing changes over BGP. **Yes**—Indicates that the router is configured with a BGP interface. **No**—Indicates that the router is not configured with a BGP interface
Last Update Time	Shows the date and time of the most recent change to the router in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Area OSPF Route List Dialog Box

When you click the Total Route Count value in the Area Overview Dialog Box, page 2-117, the Area OSPF Route List dialog box appears, showing information about all routes in the area.

From the Area OSPF Route List dialog box, you can View All OSPF Routes in an AS, page 2-60 of OSPF routers in the OSPF area.

For information about the types of routes displayed in the area, see Routers, page 2-21.

For information about viewing routes of a selected router, see View Route Advertisements Announced by a Specific Router, page 2-61.

Table 2-24 describes the fields and buttons of the Area OSPF Route List dialog box.

Table 2-24 Area OSPF Route List Dialog Box

Field	Description
Type	Shows the type of route. Options include: • Numbered Point-to-Point (NP2P) • Unnumbered Point-to-Point (UP2P) • Transit Network (Adjacent/Attached) • T3 Summary Route • T4 Summary Route • Stub Route • External Route
Prefix	Shows the IP address and prefix of the route.
Domain Name	Shows the identifier of the autonomous system in which the OSPF router resides. Clicking the Domain Name link opens OSPF Domain Details Dialog Box, page 2-104.
No. Advertising Routers	Shows the number of advertising routers out of the total number of routers in the area. For a Transit Network, clicking the No. of Advertising Routers link opens Attached Routers for Transit Network Dialog Box, page 2-135. For a T3 Summary Route, clicking the No. of Advertising Routers link opens Advertising Routers for T3 Summary Route Dialog Box, page 2-136. For a T4 Summary Route, clicking the No. of Advertising Routers link opens Advertising Routers for T4 Summary Route Dialog Box, page 2-137. For a Stub Route, clicking the No. of Advertising Routers link opens Advertising Routers for Stub Route Dialog Box, page 2-139. For a External Route, clicking the No. of Advertising Routers link opens Advertising Routers for External Route Dialog Box, page 2-138.
Last Update Time	Shows the date and time of the most recent change to the route in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Area OSPF Interface List Dialog Box

When you click an Total Interface Count value in the Area Overview Dialog Box, page 2-117, the Area OSPF Interface List dialog box appears, showing information about all OSPF interfaces in the area.

From the Area OSPF Interface List dialog box, you can View OSPF Interfaces for All Routers in an AS, page 2-57.

Table 2-25 describes the fields and buttons of the Area OSPF Interface List dialog box.

Table 2-25 Area OSPF Interface List Dialog Box

Field	Description
Type	Shows the type of interface. Options include: • NP2P • UP2P • Transit IF
Identifier	Shows the IP address of the interface. Clicking the link for an NP2P interface opens the Attributes for Numbered Point-to-Point Interface Dialog Box, page 2-122. Clicking the link for a UP2P interface opens the Attributes for Unnumbered Point-to-Point Interface Dialog Box, page 2-123. Clicking the link for a Transit IF opens the Attributes for Transit Interface Dialog Box, page 2-124.
Destination	Shows the identifier of the topology element that shares the connection. Options include: Name of the router that shares an NP2P link IP address and subnet of the network connects to a transit interface Clicking the Destination link of NP2P or UP2P interfaces opens the Attributes for OSPF Router Dialog Box, page 2-119. Clicking the Destination link of a Transit Interface interfaces opens the Attributes for Transit Network Dialog Box, page 2-125.
Available	Shows the status of the interface. Options include: **Yes**—Indicates that the interface is available. **No**—Indicates that the interface is unavailable.

Table 2-25 Area OSPF Interface List Dialog Box (continued)

Field	Description
Metric	Shows the cost metric assigned to the interface.
Source	Shows the identifier of the topology element that originates the connection. Options include: IP address of the source router Name of the source router Clicking a Source value opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area ID	Shows the identifier of the area in which the originating interface resides. Clicking the Area ID link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the name of the domain in which the originating interface resides. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the route in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Domain OSPF Router List Dialog Box

When you click a Total OSPF Router Count value in the OSPF Domain Details Dialog Box, page 2-104, the Domain OSPF Router List dialog box appears, showing information about all routers in the autonomous system.

From the Domain OSPF Router List dialog box, you can View All OSPF Routers in an AS, page 2-56.

For information about the types of routers displayed in the Graphical and Topology Browsers, see Routers, page 2-21.

For information about viewing routes of a selected router, see View Route Advertisements Announced by a Specific Router, page 2-61.

Table 2-26 describes the fields and buttons of the Domain OSPF Router List dialog box.

Table 2-26 Domain OSPF Router List

Field	Description
Router Name	Shows the Router Id, DNS name, or user-defined name of each router in the autonomous system. Clicking the Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area ID(s)	Shows the unique identifier of the OSPF area in which the router resides. Clicking the Area ID(s) link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the identifier of the domain in which the OSPF router resides.
Available	Shows the status of the router. Options include: **Yes**—Router is forwarding packets. **No**—Router is incapable of forwarding packets.
ABR	Shows whether the given router is an ABR. Options include: **Yes**—Indicates that the router is an ABR. **No**—Indicates that the router is not an ABR.
ASBR	Shows whether the selected router is an ASBR. Options include: **Yes**—Indicates that the router is an ASBR. **No**—Indicates that the router is not an ASBR.
BGP Router	Shows whether the router is configured with a BGP interface, enabling it to advertise and receive routing changes over BGP. Options include: **Yes**—Indicates that the router is a BGP speaker. **No**—Indicates that the router is not a BGP speaker.
Last Update Time	Shows the date and time of the most recent change to the router in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Domain OSPF Route List Dialog Box

When you click a Total OSPF Route Count value in the OSPF Domain Details Dialog Box, page 2-104, the Domain OSPF Route List dialog box appears, showing information about all routes in the autonomous system.

From the Domain OSPF Route List dialog box, you can View All OSPF Routes in an AS, page 2-60 in the autonomous system.

For information about viewing routes of a selected router, see View Route Advertisements Announced by a Specific Router, page 2-61.

Table 2-27 describes the fields and buttons of the Domain OSPF Route List dialog box.

Table 2-27 Domain OSPF Route List Dialog Box

Field	Description
Type	Shows the type of route. Options include: • External Route • Transit Network • Stub Network
Prefix	Shows the prefix of the route in the format `IP address/subnet mask`, for example: `1.1.1.1/24`.
Domain Name	Shows the unique identifier of the routing domain in which the destination route resides. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
No. Advertising Routers	Shows the number of routers that advertised a stub, transit, or external route into the domain. Clicking the Number of Advertising Routers link for a Stub Route opens Advertising Routers for Stub Route Dialog Box, page 2-139. Clicking the Number of Advertising Router link for a Transit Network opens Attached Routers for Transit Network Dialog Box, page 2-135. Clicking the Number of Advertising Router link for an External Route opens Advertising Routers for External Route Dialog Box, page 2-138.
Last Update Time	Shows the date and time of the most recent change to the route in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. Pivoting to the Event Log, page 2-64.

Domain OSPF Interface List Dialog Box

When you click a Total OSPF Interface Count value in the OSPF Domain Details Dialog Box, page 2-104, the Domain OSPF Interface List dialog box appears, showing information about all interfaces in the domain.

From the Domain OSPF Interface List dialog box, you can View OSPF Interfaces for All Routers in an AS, page 2-57 in the autonomous system.

Table 2-28 describes the fields and buttons of the Domain OSPF Interface List dialog box.

Table 2-28 Domain OSPF Interface List Dialog Box

Field	Description
Type	Shows the type of interface. Options include: • NP2P • UP2P • Transit interface
Identifier	Shows the name or IP address of the interface. Clicking the link for an NP2P interface opens the Attributes for Numbered Point-to-Point Interface Dialog Box, page 2-122. Clicking the link for a UP2P interface opens the Attributes for Unnumbered Point-to-Point Interface Dialog Box, page 2-123. Clicking the link for a Transit interface opens the Attributes for Transit Interface Dialog Box, page 2-124.
Destination	Shows the identifier of the topology element that shares the connection. Options include: Name or IP address of the router that shares an NP2P link IP address and subnet of the network connects to a Transit Interface Clicking the Destination link of NP2P or UP2P interfaces opens the Attributes for OSPF Router Dialog Box, page 2-119. Clicking the Destination link of a Transit Interface opens the Attributes for Transit Interface Dialog Box, page 2-124.
Available	Shows the status of the interface. Options include: **Yes**—Indicates that the interface is available. **No**—Indicates that the interface is unavailable.
Metric	Shows the cost metric assigned to the interface.
Source	Shows the identifier of the topology element that originates the connection. Options include: • Name of the source router • IP address of the source router Clicking the Source link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area Id	Shows the identifier of the area in which the originating interface resides. Clicking the Area Id link opens the Area Overview Dialog Box, page 2-117.

Table 2-28 Domain OSPF Interface List Dialog Box (continued)

Field	Description
Domain Name	Shows the name of the domain in which the originating interface resides. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the route in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Area List for Domain Dialog Box

When you click the Total Area Count value in the OSPF Domain Details Dialog Box, page 2-104, the Area List for Domain dialog box appears, showing the unique identifiers of all areas in the domain.

From the Area List for Domain dialog box, you can View Areas in a Domain, page 2-55.

Table 2-29 describes the fields of the Area List for Domain dialog box.

Table 2-29 Area List for Domain Dialog Box

Field	Description
Area ID	Shows the unique identifier for all areas in the domain. Clicking an Area ID value opens the Area Overview Dialog Box, page 2-117.

Area Overview Dialog Box

When you click the Area ID link in the Area List for Domain Dialog Box, page 2-109, the Area Overview dialog box opens. This dialog box provides information about the total number of network elements, such as routers, interfaces, and routes, in the selected OSPF area.

From the Area Overview dialog box, you can View Details of an Area, page 2-56.

Table 2-30 describes the fields and buttons of the Area Overview dialog box.

Table 2-30 Area Overview

Field	Description
Area ID	Shows the unique identifier of the area. Clicking the Area ID value opens the Area List for Domain Dialog Box, page 2-109.
Domain Name	Shows the identifier of the domain. Clicking the Domain Name value opens the OSPF Domain Details Dialog Box, page 2-104.

Table 2-30 Area Overview (continued)

Field	Description
Total Router Count	Shows the number of routers with an Available status compared to the total number of routers in the area. Clicking the Total Router Count value opens the Area OSPF Route List Dialog Box, page 2-110.
No. ABR's	Shows the number of ABRs with an Available status compared to the total number of ABRs that have an area node in the area.
No. ASBR's	Shows the number of ASBRs with an Available status compared to the total number of ASBRs in the area.
No. Internal Routers	Shows the number of Internal Routers with an Available status compared to the total number of Internal Routers in the area.
Total Interface Count	Shows the total number of interfaces with an Available status compared to the total number of interfaces in the area. Clicking the Total Interface Count value opens the Area OSPF Interface List Dialog Box, page 2-112.
No. NP2P IFs	Shows the total number of Numbered Point-to-Point (NP2P) interfaces with an Available status compared to the total number of NP2P interfaces in the area.
No. UP2P IFs	Shows the total number of Unnumbered Point-to-Point (UP2P) interfaces with an Available status compared to the total number of UP2P interfaces in the area.
No. Transit IFs	Shows the total number of Numbered Point-to-Point (NP2P) interfaces with an Available status compared to the total number of NP2P interfaces in the area.
No. Transit to Router Links	Shows the total number of transit to router links with an Available status compared to the total number of transit-to-router links in the area.
Total Route Count	Shows the total number of routes in the area. Clicking a Total Route Count value opens the Area OSPF Route List Dialog Box, page 2-110.
No. Stub Routes	Shows the total number of stub routes in the area.
No. External Routes	Shows the total number of external routes in the area. These routes are received in Type 5 LSAs advertised by ASBRs in the area.
No. T3 Summary Routes	Shows the total number of T3 Summary routes to destinations in other areas that ABRs advertise in the area.
No. T4 Summary Routes	Shows the total number of T4 Summary routes to an ASBR that ABRs advertise in the area.
No. Transit Networks	Shows the total number of Transit networks with an Available status compared to the total number of Transit networks in the area.

Attributes for OSPF Router Dialog Box

When you right-click an OSPF router, then click **Show OSPF Attributes**, the Attributes for OSPF Router dialog box opens to show information about the router's attributes.

The Attributes for OSPF Router dialog box shows information about a selected router in an area or a domain.

From the OSPF Router Attributes dialog box, you can View Attributes of an OSPF Router, page 2-58.

Dialog box fields vary depending on the type of router you select. For example, an ASBR or combined ABR/ASBR provides links to External, Transit, and Stub routes. ABRs provide links to Transit, Stub, T3 Summary, and T4 Summary routes.

Note In the Topology Viewer, an ABR can appear as a non-ABR router if its interfaces in all but one configured area become unavailable.

Table 2-31 describes the fields and buttons of the Attributes for OSPF Router dialog box.

Table 2-31 Attributes for OSPF Router Dialog Box

Field	Description
OSPF Router ID	Shows the Router ID of the router. Clicking the Router Name link opens the Domain OSPF Router List Dialog Box, page 2-113.
DNS Name	Shows the name of the router, translated by the Domain Name Service.
User Defined Name	Shows the name assigned to the router by your Path Anaylzer administrator from the Domain Administration module.
Area ID(s)	Shows the name of the area in which the router has an interface.
Domain Name	Shows the routing domain in which the router has an interface. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Available	Shows the availability of the router: **Yes**—Router is available and forwarding packets on at least one interface. **No**—Router is unavailable and incapable of forwarding packets.
ABR	Shows whether the given router is an ABR: **Yes**—Indicates that the router is an ABR. **Yes**—Indicates that the router is not an ABR.
ASBR	Shows whether the selected router is an ASBR **Yes**—Indicates that the router is an ASBR. **Yes**—Indicates that the router is not an ASBR.

Table 2-31 Attributes for OSPF Router Dialog Box (continued)

Field	Description
AS Name	Shows the unique identifier of the autonomous system in which the router advertises changes in routes.
BGP Router ID	Shows the unique identifier of the BGP speaker configured on the physical router. Clicking the BGP Router ID link opens the BGP Router Details Dialog Box, page 2-121.
NP2P If Count	Shows the number of numbered point-to-point (NP2P) interfaces configured on the router. Clicking the NP2P Interface Count link opens the NP2P Interfaces for Router Dialog Box, page 2-128.
UP2P If Count	Shows the number of unnumbered point-to-point (UP2P) interfaces configured on the router. Clicking the UP2P Interface Count link opens the UP2P Interfaces for Router Dialog Box, page 2-129.
Transit If Count	Shows the number of transit interfaces configured on the router. Clicking the Transit Interface Count link opens the Transit Interfaces for Router Dialog Box, page 2-130.
Stub Route Adv Count	Shows the number of stub route advertisements announced by the router. Clicking the Stub Route Advertisement Count link opens the Stub Route Advertisements for OSPF Router Dialog Box, page 2-135.
T3 Summary Route Adv Count	Shows the number of T3 Summary route advertisements announced by the ABR. Clicking the T3 Summary Route Advertisement Count link opens the T3 Summary Route Advertisements for OSPF Router Dialog Box, page 2-131.
T4 Summary Route Adv Count	Shows the number of T4 Summary route advertisements announced by the ABR. Clicking the T4 Summary Route Advertisement Count link opens the T4 Summary Route Advertisements for OSPF Router Dialog Box on page 2-132.
Static Route Count	Shows the total number of static routes advertised by the router.

Table 2-31 Attributes for OSPF Router Dialog Box (continued)

Field	Description
External Route Advertisement Count	Shows the number of external route advertisements announced by an ASBR in Type 5 LSAs. Clicking the External Route Advertisement Count link opens the External Route Advertisements for OSPF Router Dialog Box, page 2-133.
Last Update Time	Shows the date and time of the most recent change in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

BGP Router Details Dialog Box

When you right-click a BGP router, then click **Show BGP Attributes**, the BGP Router Details dialog box opens to show information about the router's attributes.

This dialog box shows information about a selected router in an area or a domain.

From the OSPF Router Attributes dialog box, you can View Attributes of a BGP Router, page 2-58.

Table 2-32 describes the fields and buttons of the BGP Router Details dialog box.

Table 2-32 BGP Router Details Dialog Box

Field	Description
Router Name	Shows the Router ID, DNS name, or user-defined name of the router.
BGP Domain Name	Shows the routing domain in which the router has an interface. Clicking the Domain Name link opens the BGP Domain Details Dialog Box, page 2-106.
BGP Router ID	Shows the Router ID of the router.
IPV4 Route Count	Shows the number of IPV4 routes on this router. Clicking the IPV4 Route Count value opens the IPV4 Routes for a Router Dialog Box, page 2-142.
VRF Count	Shows the number of VRFs on this router.
VPN Route Count	Shows the number of VPN routes on this router. Clicking the VPN Route Count value opens the VPN Route List Dialog Box, page 2-145.
Last Update Time	Shows the date and time of the most recent change in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. Pivoting to the Event Log, page 2-64.

Attributes for Transit to Router Link Dialog Box

When you right-click a link from a Transit network to a router and click **Show Attributes**, the Attributes for Transit to Router Link dialog box opens. This dialog box shows attributes and details of a selected transit to router link from a Transit network or subnet to a router.

For information about the types of links displayed in the Topology Viewer, see Interfaces and Links, page 2-30.

For information about showing details, see View Attributes of a Transit-to-Router Link, page 2-63.

Table 2-33 describes the fields and buttons of the Attributes for Transit to Router Link dialog box.

Table 2-33 Attributes for Transit to Router Link

Field	Description
Prefix	Shows the prefix of the transit-to-router link in the format of an IP address and subnet mask. Example: 10.10.12.0/24 Clicking on the Prefix value opens the Attributes for Transit Network Dialog Box, page 2-125.
Router Name	Shows the Router ID, DNS name, or user-defined name of the router that receives data from the Transit network. Clicking the Router Name value opens the Attributes for OSPF Router Dialog Box, page 2-119.
Availability	Shows the status of the transit-to-router link. Options include: **Yes**—The transit-to-router link is available. Data is forwarded from the Transit network to the router. **No**—The transit-to-router link is unavailable. Data is not forwarded from the Transit network to the router.
Area Id	Shows the OSPF area in which the transit to area node link resides. Click the Area ID value opens the Area Overview Dialog Box, page 2-117.
Domain Id	Shows the domain in which the transit-to-router link resides. Click on the Domain Id value opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Attributes for Numbered Point-to-Point Interface Dialog Box

When you right-click a Numbered Point-to-Point (NP2P) link between two routers and select **Show Attributes**, the Attributes for Numbered Point-to-Point Interface dialog box opens. This dialog box shows attributes and details of the Numbered Point-to-Point (NP2P) interface you selected.

You can also open the Attributes for a Numbered Point-to-Point Interface dialog box from the Area OSPF Interface List Dialog Box, page 2-112 by clicking an NP2P IF link in the Identifier column.

For information about the types of links displayed in the Topology Viewer, see Interfaces and Links, page 2-30.

For information about showing details, see View Attributes of a Numbered Point-to-Point (NP2P) Interface, page 2-63.

Table 2-34 describes the fields and buttons of the Attributes for Numbered Point-to-Point Interface dialog box.

Table 2-34 Attributes for NP2P Interface

Field	Description
Identifier	Shows the IP address of the NP2P interface
Source	Shows the Router ID of the forwarding router. Clicking the Source value opens the Attributes for OSPF Router Dialog Box, page 2-119, which provides details about the forwarding router.
Destination	Shows the Router ID of the receiving router. Clicking the Destination value opens the Attributes for OSPF Router Dialog Box, page 2-119, which provides details about the receiving router.
Available	Shows the availability of the link **Yes—**Link is available; packets are forwarded over the link. **No—**Packet is not forwarded over link.
Metric	Shows the cost of the link.
Area ID	Shows the OSPF area in which the NP2P link resides. Clicking on an Area ID value opens the Area Overview Dialog Box, page 2-117
Domain Name	Shows the domain in which the NP2P link resides. Clicking on the Domain Name value opens the OSPF Domain Details Dialog Box, page 2-104
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Attributes for Unnumbered Point-to-Point Interface Dialog Box

When you right-click an Unnumbered Point-to-Point (UP2P) link between two routers, and select **Show Attributes**, the Attributes for UP2P Interface dialog box opens. This dialog box shows details of a selected Unnumbered Point-to-Point (UP2P) interface.

For information about the types of links displayed in the Topology Viewer, see Interfaces and Links, page 2-30.

Table 2-35 describes the fields and buttons of the Attributes for Unnumbered Point-to-Point Interface dialog box.

Table 2-35 Attributes for UP2P Interface Dialog Box

Field	Description
Identifier	Shows the Management Information Base (MIB) Index of the interface on the router that forwards packets over the link.
Source	Shows the Router Id, DNS name, or user-defined name of the forwarding router. Clicking the Source link opens the Attributes for OSPF Router Dialog Box, page 2-119, which provides details about the forwarding router.
Destination	Shows the Router Id, DNS name, or user-defined name of the receiving router. Clicking the Destination link opens the Attributes for OSPF Router Dialog Box, page 2-119, which provides details about the receiving router.
Available	Shows the availability of the link: **Yes**—Link is available; packets are forwarded over the link. **No**—Packet is not forwarded over link.
Metric	Shows the cost of the link.
Area ID	Shows the OSPF area in which the UP2P link resides. Clicking the Area ID link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the domain in which the UP2P link resides. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Attributes for Transit Interface Dialog Box

When you click the Identifier of a transit interface in the All Interfaces for Router Dialog Box, page 2-127, the Attributes for Transit Interface dialog box appears.

You can also open the Attributes for Transit Interface dialog box by clicking on the Designated Interface value on the Attributes for Transit Network Dialog Box, page 2-125.

The Attributes for Transit Interface dialog box shows attributes and details of a selected transit interface link from a router to a host on a Transit network or subnet.

For information about the types of links displayed in the Topology Viewer, see Interfaces and Links, page 2-30.

For information about showing details of a transit interface, see View Attributes of a Transit Interface, page 2-62.

Table 2-36 describes the fields and buttons of the Attributes for Transit Interface dialog box.

Table 2-36 Attributes for Transit Interface

Field	Description
Identifier	Shows the IP address of the transit interface.
Source	Shows the name of the router that forwards data over the selected transit interface. Clicking the Source value opens the Attributes for OSPF Router Dialog Box on page 2-119.
Destination	Shows the IP address and subnet mask of the Transit network that receives data over the selected transit interface. Clicking the Destination value opens the Attributes for Transit Network Dialog Box, page 2-125.
Available	Shows the availability of the link: **Yes**—Packets are forwarded over the link. **No**—Packets are not forwarded over the link.
Metric	Shows the cost of the link.
Area ID	Shows the OSPF area in which the transit interface resides. Click the Area ID value opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the name of the domain in which the transit interface resides. Clicking the Domain Name value opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Attributes for Transit Network Dialog Box

When you right-click a Transit network, then click **Show Attributes**, the Attributes for Transit Network dialog box appears.

- Clicking the Destination link in the Attributes for Transit Interface Dialog Box, page 2-124 causes the Attributes for Transit Network dialog box to open.
- Additionally, clicking the Destination link in the Area OSPF Interface List Dialog Box, page 2-112 causes the Attributes for Transit Network dialog box to open.

For information about Transit networks and subnets displayed in the Topology Viewer, see Networks and Subnets, page 2-29.

Table 2-37 describes the fields and buttons of the Attributes for Transit Network dialog box.

Table 2-37 Attributes for Transit Network

Field	Description
Prefix	Shows the prefix of the route in the format `IP address/mask`, for example: `1.1.1.1/24`.
Area ID	Shows the unique identifier of the OSPF area in which the Transit network resides. Clicking the Area ID link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the unique identifier of the domain in which the Transit network resides. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Available	Shows the availability of the Transit network. Options include: **Yes**—The network or subnet is available and functioning properly as part of the enterprise-wide network. **No—**The network or subnet is not available on the enterprise-wide network.
No. Adjacent Routers	Shows number of available routers that connect to the Transit network.
No. Attached Routers	Shows total number of available and unavailable routers that connect to the Transit network. Clicking the No. Attached Routers value opens the Interfaces for Router Dialog Boxes, page 2-127.
Designated Router Name	Shows the router ID, DNS name, or user-defined name of the Designated Router (DR) that advertises the Transit network to an area. Clicking the Designated Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119 of the DR.
Designated Interface	Shows the IP address of the interface on the DR that sends and receives data to the Transit network. Clicking the Designated Interface link opens the Attributes for Transit Interface Dialog Box, page 2-124.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Interfaces for Router Dialog Boxes

The Interfaces for Router dialog boxes provide information about the transit, NP2P, UP2P, or stub interfaces of a selected router:

Table 2-38 describes the fields and buttons of the Interfaces for Router dialog box.

Table 2-38 Interfaces for Router Dialog Boxes

Interface type	Find information on Dialog Box
All Interfaces	See All Interfaces for Router Dialog Box, page 2-127.
NP2P Interfaces	See NP2P Interfaces for Router Dialog Box, page 2-128.
UP2P Interfaces	See UP2P Interfaces for Router Dialog Box, page 2-129.
Transit Interfaces	See Transit Interfaces for Router Dialog Box, page 2-130.

All Interfaces for Router Dialog Box

The All Interfaces for Router dialog box shows information about the interfaces of a selected router.

Right-clicking a router, then clicking **Show Interfaces** causes this dialog box to open.

For information about viewing the interfaces of a selected router, see View the Interfaces of a Specific OSPF Router, page 2-60.

Table 2-39 describes the fields and buttons of the All Interfaces for Router dialog box.

Table 2-39 All Interfaces for Router

Field	Description
Type	Shows the type of interface. Options include: • Transit • NP2P • UP2P
Identifier	Shows any of the following identifiers that describe the interface: • IP address of a transit interface • IP address of an NP2P interface • Management Information Base (MIB) index number of a UP2P interface Clicking the Identifier link opens the corresponding Interface Attribute dialog box.
Destination	Shows the IP address of a connected router or the IP address and network mask of a connected network. Clicking the Destination link opens the corresponding Interface Attribute dialog box.

Table 2-39 All Interfaces for Router (continued)

Field	Description
Available	Shows the status of the interface: **Yes**—Packets are forwarded over the interface. **No**—Packets are not forwarded over the interface.
Metric	Shows the metric assigned to the router interface.
Source	Shows the IP address of the connected router. Clicking the Source link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area ID	Shows the OSPF area in which the interface resides. Clicking the Area ID link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the name of the domain in which the interface resides. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

NP2P Interfaces for Router Dialog Box

When you click the NP2P Interface Count link in the Attributes for OSPF Router Dialog Box, page 2-119, the NP2P Interfaces for Router dialog box opens. This dialog box shows information about the NP2P interfaces of a selected router.

For information about viewing the interfaces of a selected router, see View the Interfaces of a Specific OSPF Router, page 2-60.

For related information, see View Attributes of a Numbered Point-to-Point (NP2P) Interface, page 2-63.

Table 2-40 describes the fields and buttons of the NP2P Interfaces for Router dialog box.

Table 2-40 NP2P Interfaces for Router

Field	Description
Type	Shows the type of interface.
Identifier	Shows the IP address of the transit interface. Clicking on an Identifier opens the Attributes for Numbered Point-to-Point Interface Dialog Box, page 2-122.
Destination	Shows the IP address of the router that forwards data over the NP2P interface. Clicking on a Destination link opens the Attributes for OSPF Router Dialog Box, page 2-119

Table 2-40 NP2P Interfaces for Router (continued)

Field	Description
Available	Shows the status of the interface: **Yes**—Packets are forwarded over the interface. **No**—Packets are not forwarded over the interface.
Metric	Shows the metric assigned to the router interface.
Source	Shows the IP address of the router that receives data over the selected NP2P interface. Clicking on a Source link opens the Attributes for OSPF Router Dialog Box, page 2-119
Area ID	Shows the OSPF area in which the interface resides. Clicking the Area ID link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the domain in which the interface resides. Clicking a Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

UP2P Interfaces for Router Dialog Box

When you click the UP2P Interface Count link in the Attributes for OSPF Router Dialog Box, page 2-119, the UP2P Interfaces for Router dialog box opens. This dialog box shows information about the UP2P interfaces of a selected router.

For information about viewing the interfaces of a selected router, see View the Interfaces of a Specific OSPF Router, page 2-60.

For related information, see View Attributes of an Unnumbered Point-to-Point (UP2P) Interface, page 2-63.

Table 2-41 describes the fields and buttons of the UP2P Interfaces for Router dialog box.

Table 2-41 UP2P Interfaces for Router Dialog Box

Field	Description
Type	Shows the type of interface.
Identifier	Shows the unique identifier of the UP2P interface. Clicking the Identifier link opens the Attributes for Unnumbered Point-to-Point Interface Dialog Box on page 2-123.

Table 2-41 UP2P Interfaces for Router Dialog Box (continued)

Field	Description
Destination	Shows the IP address of the router that forwards data over the selected UP2P interface. Clicking the Destination link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Available	Shows the status of the interface: **Yes**—Packets are forwarded over the interface. **No**—Packets are not forwarded over the interface.
Metric	Shows the metric assigned to the interface.
Source	Shows the IP address of the router that receives data over the selected UP2P interface. Clicking the Source link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area ID	Shows the OSPF area in which the interface resides. Clicking the Area ID link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the domain in which the interface resides. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Transit Interfaces for Router Dialog Box

When you click the Transit Interface Count link in the Attributes for OSPF Router Dialog Box, page 2-119, the Transit Interfaces for Router dialog box opens. This dialog box shows information about the transit interfaces of a selected router.

For information about viewing the interfaces of a selected router, see View the Interfaces of a Specific OSPF Router, page 2-60.

For related information, see View Attributes of a Transit Interface, page 2-62.

Table 2-42 describes the fields and buttons of the Transit Interfaces for Router dialog box.

Table 2-42 Transit Interfaces for Router Dialog Box

Field	Description
Type	Shows the type of interface.
Identifier	Shows the unique identifier of the transit interface. Clicking the Identifier link opens the Attributes for Transit Interface Dialog Box, page 2-124.

Table 2-42 Transit Interfaces for Router Dialog Box (continued)

Field	Description
Destination	Shows the IP address and subnet mask of the Transit network that forwards data over the selected transit interface. Clicking the Destination link opens the Attributes for Transit Network Dialog Box, page 2-125.
Available	Shows the status of the interface: **Yes**—Packets are forwarded over the interface. **No**—Packets are not forwarded over the interface.
Metric	Shows the metric assigned to the interface.
Source	Shows the IP address of the router that receives data over the selected transit interface. Clicking the Source link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area ID	Shows the OSPF area in which the interface resides. Clicking the Area ID link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the domain in which the interface resides. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

T3 Summary Route Advertisements for OSPF Router Dialog Box

When you right-click an ABR or combined ABR/ASBR, then click **Show T3 Summary Route Advs**, the T3 Summary Route Advertisements for OSPF Router dialog box opens. This dialog box shows information about the T3 Summary route advertisements of a selected Area Border Router (ABR).

Clicking the T3 Summary Route Adv Count link in the Attributes for OSPF Router Dialog Box, page 2-119 also opens the T3 Summary Route Advertisements for OSPF Router dialog box.

For information about viewing routes of a selected router, see View Route Advertisements Announced by a Specific Router, page 2-61.

Table 2-43 describes the fields and buttons of the T3 Summary Route Advertisements for OSPF Router dialog box.

Table 2-43 T3 Summary Route Advertisements for OSPF Router Dialog Box

Field	Descriptions
Prefix	Shows all Type 3 Summary Routes advertised by the selected ABR. Clicking the Prefix link opens the Advertising Routers for T3 Summary Route Dialog Box, page 2-136.
Metric	Shows the cost of reaching the route from the ABR that advertised the T3 summary route.
Advertising Router Name	Shows the Router Id, DNS name, or user-defined name of the ABR that announces the Type 3 Summary route. Clicking the Advertising Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area Id	Shows the OSPF routing domain in which the ABR advertises the Type 3 Summary Route. Clicking the Area Id link opens the Area Overview Dialog Box, page 2-117.
Domain Id	Shows the domain in which the destination route resides. Clicking the Domain Id link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

T4 Summary Route Advertisements for OSPF Router Dialog Box

When you right-click an ABR or combined ABR/ASBR, then click **Show T4 Summary Route Advs**, the T4 Summary Route Advertisements for OSPF Router dialog box opens. This dialog box shows information about the T4 Summary route advertisements of a selected Area Border Router (ABR).

Clicking the T4 Summary Route Adv Count link in the Attributes for OSPF Router Dialog Box, page 2-119 also opens the T4 Summary Route Advertisements for OSPF Router dialog box.

For information about viewing routes of a selected router, see View Route Advertisements Announced by a Specific Router, page 2-61.

Table 2-44 describes the fields and buttons of the T4 Summary Route Advertisements for OSPF Router dialog box.

Table 2-44 T4 Summary Route Advertisements for OSPF Router Dialog Box

Field	Descriptions
ASBR Id	Shows the IP address of the ASBR that the ABR advertises. Clicking the ASBR link opens the Advertising Routers for T4 Summary Route Dialog Box, page 2-137.
Metric	Shows the cost of reaching the ASBR from the ABR that advertised the Type 4 Summary route.
Advertising Router Name	Shows the Router Id, DNS name, or user-defined name of the ABR that announces the Type 4 Summary route. Clicking the Advertising Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area Id	Shows the area in which the ABR advertises the T4 Summary Route. Clicking the Area Id link opens the Area Overview Dialog Box.
Domain Id	Shows the domain in which the destination route resides. Clicking the Domain Id link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

External Route Advertisements for OSPF Router Dialog Box

When you right-click an Autonomous System Boundary Router (ASBR) or a combined ABR/ASBR, and select **Show External Route Advs**, the External Route Advertisements for OSPF Router dialog box opens. This dialog box shows information about the external route advertisements (Type 5 LSAs) of a selected ASBR.

Clicking the External Route Advertisement Count link in the Attributes for OSPF Router Dialog Box, page 2-119 also causes this dialog box to open.

For information about viewing routes of a selected router, see View Route Advertisements Announced by a Specific Router, page 2-61.

Table 2-45 describes the fields and buttons of the External Route Advertisements for OSPF Router dialog box.

Table 2-45 External Route Advertisements for OSPF Router Dialog Box

Field	Description
Prefix	Shows the IP address and subnet mask of the external route, which is advertised in a Type 5 LSA. Clicking the Prefix link opens the Advertising Routers for External Route Dialog Box, page 2-138.
Metric	Shows the cost of the Type 1 or Type 2 metric of the destination route.
Metric Type	Shows the metric type of the destination route. The Autonomous System Boundary Router (ASBR) advertises the metric type and cost to all routers in the autonomous system.
Forwarding Address	Shows the IP address of a router sent by an ASBR in a Type 5 *Link State Advertisement (LSA)* to inform routers in the same domain of a better exit point for traffic to the advertised destination.
LSA Type	Type 5 Type 7
Pbit	Type 7 LSAs have a propagate (P) bit in the header which is used to flag an Area Border Router (ABR) to translate a Type-7 LSA into a Type-5 LSA. **Yes**—P bit is on. **No**—P bit is off.
Advertising Router Name	Shows the Router ID, DNS name, or user-defined name of the ASBR that announces the external route in the autonomous system. Clicking the Advertising Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area Id	Shows the area in which the external route is advertised. Clicking the Area Id link opens the Area Overview Dialog Box, page 2-117.
Domain Id	Shows the domain in which the destination route resides. Clicking the Domain Id link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Stub Route Advertisements for OSPF Router Dialog Box

When you right-click a router that advertises a route to Transit network, then click **Show Stub Route Advs**, the Stub Route Advertisements for OSPF Router dialog box opens.

Clicking the Stub Route Advertisement Count link in the Attributes for OSPF Router Dialog Box, page 2-119 also opens the Stub Route Advertisements for OSPF Router dialog box.

For information about viewing routes of a selected router, see View Route Advertisements Announced by a Specific Router, page 2-61.

Table 2-46 describes the fields and buttons of the Stub Route Advertisements for OSPF Router dialog box.

Table 2-46 Stub Route Advertisements for OSPF Router Dialog Box

Field	Description
Prefix	Shows the IP address and subnet mask of the route. Clicking the Prefix link opens the Advertising Routers for Stub Route Dialog Box, page 2-139.
Metric	Shows the cost of the link between the router and the Stub network.
Advertising Router Name	Shows the Router ID, DNS name, or user-defined name of the router that advertises the Transit network. Clicking the Advertising Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area Id	Shows the area in which the Transit network resides. Clicking the Area Id link opens the Area Overview Dialog Box, page 2-117.
Domain Id	Shows the name of the domain in which the destination route resides. Clicking the Domain Id link opens OSPF Domain Details Dialog Box, page 2-104
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Attached Routers for Transit Network Dialog Box

When you click the No. Attached Routers link in the Attributes for Transit Network Dialog Box, page 2-125, the Attached Routers for Transit Network dialog box appears. In this dialog box, you can View All Routers Attached to a Transit Network.

For information about Transit networks and subnets displayed in the Topology Viewer, see Networks and Subnets, page 2-29.

Table 2-47 describes the fields and buttons of the Attached Routers for Transit Network dialog box.

Table 2-47 Attached Routers for Transit Network

Field	Description
Attached Router Name	Shows the Router ID, DNS name, or user-defined name of the router.
Attached in Area	Shows the unique identifier of the area in which each attached router resides. Clicking the Attached in Area link opens the Area Overview Dialog Box, page 2-117.
Adjacent	Shows whether a router is connected to the selected Transit network. Options include: **Yes**—The router is connected. **No**—The router is disconnected from the network.
Domain Name	Shows the name of the domain in which the router resides. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Advertising Routers for T3 Summary Route Dialog Box

When you click the Number of Advertising Routers link for a T3 Summary Route in the Area OSPF Route List Dialog Box, page 2-110, the Advertising Routers dialog box opens to show information about a selected T3 Summary route.

You can also open this dialog box by clicking the route link in the T3 Summary Route Advertisements for OSPF Router Dialog Box, page 2-131.

In the Advertising Routers for T3 Summary Route dialog box, you can view details about the Area Border Routers (ABRs) or combined ABR/ASBRs that advertise a selected T3 Summary route.

Table 2-48 describes the fields and buttons of the Advertising Routers for T3 Summary Route dialog box.

Table 2-48 Advertising Router for T3 Summary Route

Field	Description
Advertising ABR Name	Shows the Router ID, DNS name, or user-defined name of the ABR that announces the T3 Summary route within the OSPF area. Clicking the Advertising ABR Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Metric	Shows the cost of reaching the route through the ABR.

Table 2-48 Advertising Router for T3 Summary Route (continued)

Field	Description
Advertised in Area	Shows the OSPF area in which the ABR advertises the T3 Summary route. Clicking the Advertised in Area link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the autonomous system in which the ABR advertises the T3 Summary route. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Advertising Routers for T4 Summary Route Dialog Box

When you click the Number of Advertising Routers link for a T4 Summary Route in the Area OSPF Route List Dialog Box, page 2-110, the Advertising Routers for T4 Summary Route dialog box opens. This dialog box shows information about a selected T4 Summary route.

You can also open this dialog box by clicking the ASBR Id link in the T4 Summary Route Advertisements for OSPF Router Dialog Box, page 2-132.

In the Advertising Routers for T4 Summary Route dialog box, you can view details about the Area Border Routers (ABRs) or combined ABR/ASBRs that advertise a selected T4 Summary route.

Table 2-49 describes the fields and buttons of the Advertising Routers for T4 Summary Route dialog box.

Table 2-49 Advertising Routers for T4 Summary Route Dialog Box

Field	Description
Advertising ABR Name	Shows the Router Id, DNS name, or user-defined name of the ABR that advertises the T4 summary route within the OSPF area. Clicking the Advertising Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Metric	Shows the cost of reaching the ASBR through the ABR that advertises the selected T4 Summary Route.
Advertised in Area	Shows the area identifier of the area in which the ABR announces the T4 Summary route. Clicking the Advertised in Area link opens the Area Overview Dialog Box, page 2-117.

Table 2-49 Advertising Routers for T4 Summary Route Dialog Box (continued)

Field	Description
Domain Name	Shows the autonomous system in which the ABR advertises the T4 Summary route. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Advertising Routers for External Route Dialog Box

When you click the Number of Advertising Routers link for an External Route in the Domain OSPF Route List Dialog Box, page 2-114, the Advertising Routers dialog box opens. This dialog box shows details about the Autonomous System Boundary Routers (ASBRs) or combined ABR/ASBRs that advertise an external route.

Clicking the **Prefix** link in the External Route Advertisements for OSPF Router Dialog Box, page 2-133 also opens the Advertising Routers for External Route dialog box.

Table 2-50 describes the fields and buttons of the Advertising Routers for External Route dialog box.

Table 2-50 Advertising Routers for External Route Dialog Box

Field	Description
Advertising ASBR Name	Shows the Router ID, DNS name, or user-defined name of each ASBR that advertises the external route within the autonomous system. Clicking the Advertising ASBR Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Metric	Shows the cost of reaching the destination in the external autonomous system over the route advertised by the ASBR.
Metric Type	Shows the metric type of the destination route. The Autonomous System Boundary Router (ASBR) advertises this metric type to all routers in the autonomous system.
Forwarding Address	Shows the IP address of a router sent by an ASBR in a Type 5 *Link State Advertisement (LSA)* to inform routers in the same domain of a better exit point to the advertised destination.
LSA Type	Type 5 Type 7

Table 2-50 Advertising Routers for External Route Dialog Box (continued)

Field	Description
Pbit	Type 7 LSAs have a propagate (P) bit in the header which is used to flag an Area Border Router (ABR) to translate a Type-7 LSA into a Type-5 LSA. **Yes**—P bit is on. **No**—P bit is off.
Advertised in Area	Shows the OSPF area in which the external route is advertised. Clicking the Advertised in Area link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the autonomous system for which the ABR advertises the T3 Summary route. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

Advertising Routers for Stub Route Dialog Box

When you click the Number of Advertising Routers link for a Stub Route in the Area OSPF Route List Dialog Box, page 2-110, the Advertising Routers dialog box opens to show information about a selected External Route.

You can also open this dialog box by clicking the Prefix value in the Stub Route Advertisements for OSPF Router Dialog Box, page 2-135.

In the Advertising Routers for Stub Route dialog box, you can view details about the routers that advertise a selected stub route.

Table 2-51 describes the fields and buttons of the Advertising Router for Stub Route dialog box.

Table 2-51 Advertising Routers for Stub Route Dialog Box

Field	Description
Advertising Router Name	Shows the Router ID, DNS name, or user-defined name of the router that advertises the stub route within the OSPF area. Clicking the Advertising Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Metric	Shows the cost of reaching the stub route through the router that advertises the Stub route.
Advertised in Area	Shows the OSPF area in which the Stub route is advertised. Clicking the Advertised in Area link opens the Area Overview Dialog Box, page 2-117

Table 2-51 Advertising Routers for Stub Route Dialog Box (continued)

Field	Description
Domain Name	Shows the autonomous system in which the Stub route is advertised. Clicking the Domain Name link opens the OSPF Domain Details Dialog Box, page 2-104.
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

BGP Statistics Dialog Box

If you open the BGP Domain Details Dialog Box on page 2-106, and click the value (More Statistics) for any of the following Attributes:

- IPv4 Routes
- IPv4 Multicast Routes
- VPN Routes

the BGP Statistics dialog box opens to show information about these routes, where you can view details about any of the route types shown above.

Table 2-52 describes the fields and buttons of the BGP Statistics dialog box.

Table 2-52 BGP Statistics Dialog Box

Field	Description
BGP Domain	Shows the routing domain in which the route exists. Clicking the BGP Domain link opens the BGP Domain Details Dialog Box, page 2-106.
Address Family	Shows the route type IPV4 unicast, IPV4 multicast, or IPV4 VPN).
Bgp Prefix Baseline Count	Shows the average number of prefixes within the AS per minute, over a 24-hour period.
Bgp Prefix Rate	Shows the rate of new/delete events for the last minute.
Bgp Prefix Baseline Rate	Shows the average rate of new/delete events per minute over a 24-hour period.
Bgp Prefix Node	Shows the current number of prefix nodes in the prefix tree.
Bgp Path Attribute Set Advertised	Shows the total number of unique path attributes within the AS.
Next Hop Count	Shows the total number of unique next hops within the AS.
AS Path Count	Shows the total number of unique AS Path attributes within the AS.
Origin Count	Shows the total number of unique origins within the AS.

Table 2-52 BGP Statistics Dialog Box (continued)

Field	Description
MED Count	Shows the total number of unique MED's within the AS.
Local Preference Count	Shows the total number of unique Local Preference attributes within the AS.
SOO Advertised	Shows the total number of unique Site of Origin attributes within the AS.
Communities	Shows the total number of unique Community attributes within the AS.
RT Count	Shows the total number of unique Route Target attributes within the AS.
Opaque Buffers	Shows the total number of other attributes within the AS.
AS Neighbor Nodes	Shows the number of AS neighbor nodes. Clicking the AS Neighbor Nodes link opens the BGP AS Neighbor Details Dialog Box, page 2-141

BGP AS Neighbor Details Dialog Box

When you click the AS Neighbor Nodes link in the BGP Statistics Dialog Box, page 2-140, the BGP AS Neighbor Details dialog box opens to show information about BGP AS neighbors.

In the BGP AS Neighbor Details dialog box, you can see the number of routes received from neighboring AS's.

Table 2-53 describes the fields and buttons of the BGP AS Neighbor Details dialog box.

Table 2-53 BGP AS Neighbor Details Dialog Box

Field	Description
Neighbor AS	Shows the AS number.
AS Route	Shows the number of routes received from the neighbor AS.

IPV4 Prefix List Dialog Box

When you click the IPv4 Prefix Count link in the BGP Domain Details Dialog Box, page 2-106, the IPV4 Prefix List dialog box opens to show information about the IPV4 prefixes and the number of routers associated with each one.

You can also open this dialog box by clicking the BGP Route link in the IPV4 Routes for a Router Dialog Box, page 2-142 or by clicking the IPV4 Prefix Count link in the Autonomous System List Dialog Box, page 2-104.

Table 2-54 describes the fields and buttons of the IPV4 Prefix List dialog box.

Table 2-54 IPV4 Prefix List Dialog Box

Field	Description
BGP Domain	Shows the Domain in which the IPV4 prefix resides. Clicking the BGP Domain link opens the BGP Domain Details Dialog Box, page 2-106.
IPv4 Prefix	Shows each IPV4 prefix.
Router Count	Shows the number of routers associated with each IPV4 prefix. Clicking the Router Count link opens the IPV4 Routes for a Router Dialog Box, page 2-142

IPV4 Multicast Prefix List Dialog Box

When you click the IPv4 Multicast Prefix Count link in the BGP Domain Details Dialog Box, page 2-106, the IPV4 Multicast Prefix List dialog box opens to show information about each IPV4 multicast prefix in the domain, including the associated router count.

You can also open this dialog box by clicking theIPv4 Multicast Prefix Count link in the Autonomous System List Dialog Box, page 2-104.

Table 2-55 describes the fields and buttons of the IPV4 Prefix List dialog box.

Table 2-55 IPV4 Multicast Prefix List Dialog Box

Field	Description
BGP Domain	Shows the Domain in which the IPV4 multicast prefixes reside. Clicking the BGP Domain link opens the BGP Domain Details Dialog Box, page 2-106.
IPv4 Prefix	Shows each IPV 4 multicast prefix in the domain.
Router Count	Shows the number of routers associated with each IPV4 multicast prefix. Clicking the Router Count link opens the IPV4 Multicast Routes for a Router Dialog Box, page 2-144.

IPV4 Routes for a Router Dialog Box

When you right-click a BGP router and select **Show Bgp IpV4 Routes**, the IPV4 Routes for a Router dialog box opens to show information about the IPV4 routes associated with the router.

You can also open this dialog box by clicking the IPV4 Route Count value on the BGP Router Details Dialog Box, page 2-121.

In the IPV4 Routes for a Router dialog box, you can view details about the IPV4 routes associated with the router.

Table 2-56 describes the fields and buttons of the IPV4 Routes for a Router dialog box.

Table 2-56 IPV4 Routes for a Router Dialog Box

Field	Description
Router Name	Shows the Router ID, DNS name, or user-defined name of the router. Clicking the Router Name link opens the BGP Router Details Dialog Box, page 2-121.
Router Id	Shows the Router ID of the router. Clicking the Router Id link opens the BGP Router Details Dialog Box, page 2-121.
BGP Route	Shows the IP address and prefix of a BGP route associated with this router. Clicking the BGP Route link opens the IPV4 Prefix List Dialog Box, page 2-141.
Next Hop	Shows the next hop in the route.
AS Path	Shows the AS path for the route. BGP speakers use the AS Path attribute to prevent routing loops. If a BGP speaker detects its own AS number in a route advertisement, it rejects the route, thus preventing a loop.
Origin	Shows the Origin value: **0** = IGP **1** = EGP **2** = Incomplete
Local Preferences	Shows the Local Preference value. The local preference attribute is used to select an exit point from the local autonomous system (AS).
Med	Shows the Multi-exit Discriminator value, which tells the router the preferred route into the AS from which the router advertisement originates. MED attribute values are advertised throughout the local AS. BGP speakers direct data over an entry point with the lowest MED attribute.
Communities	Shows the Community attribute, which lists the recipients of a route advertisement.
Other Attributes	Includes BGP attributes not shown in the preceding columns, including Site of Origin, Originating ID, and others.

IPV4 Multicast Routes for a Router Dialog Box

When you right-click a BGP router and select **Show Bgp IpV4 Multicast Routes**, the IPV4 Multicast Routes for a Router dialog box opens to show information about the IPV4 multicast routes associated with the router.

Table 2-57 describes the fields and buttons of the IPV4 Multicast Routes for a Router dialog box.

Table 2-57 IPV4 Multicast Routes for a Router Dialog Box

Field	Description
Router Name	Shows the Router ID, DNS name, or user-defined name of the router. Clicking the Router Name link opens the BGP Router Details Dialog Box, page 2-121.
Router Id	Shows the Router ID of the router. Clicking the Router Id link opens the BGP Router Details Dialog Box, page 2-121.
BGP Route	Shows the IP address and prefix of a BGP route associated with this router. Clicking the BGP Route link opens the IPV4 Prefix List Dialog Box, page 2-141.
Next Hop	Shows the next hop for the route.
AS Path	Shows the AS path for the route. BGP speakers use the AS Path attribute to prevent routing loops. If a BGP speaker detects its own AS number in a route advertisement, it rejects the route, thus preventing a loop.
Origin	Shows the Origin value: **0** = IGP **1** = EGP **2** = Incomplete
Local Preferences	Shows the Local Preference value. The local preference attribute is used to select an exit point from the local autonomous system (AS).
Med	Shows the Multi-exit Discriminator value, which tells the router the preferred route into the AS from which the router advertisement originates. MED attribute values are advertised throughout the local AS. BGP speakers direct data over an entry point with the lowest MED attribute.
Communities	Shows the Community attribute, which lists the recipients of a route advertisement.
Other Attributes	Includes BGP attributes not shown in the preceding columns, including Site of Origin, Originating ID, and others.

VPN Route List Dialog Box

When you right-click a BGP router and select **Show Bgp Vpn Routes**, the VPN Route List dialog box opens to show information about each VPN route within the AS.

You can also open the dialog box by clicking the VPN Route Count link in the BGP Router Details Dialog Box, page 2-121.

Table 2-58 describes the fields and buttons of the VPN Route List dialog box.

Table 2-58 VPN Route List Dialog Box

Field	Description
Router Name	Shows the unique Router ID, DNS name, or user-defined name of the router. Clicking the Router Name link opens the BGP Domain Details Dialog Box, page 2-106.
Router Id	Shows the Router ID of the router. Clicking the Router ID link opens the BGP Domain Details Dialog Box, page 2-106.
VRF Id	Shows the VRF ID number. Clicking the Router Count link opens the IPV4 Routes for a Router Dialog Box, page 2-142
VPN Route RDPrefix	Shows the VPN Route Distinguisher Prefix of the router. Clicking the VPN Route RDPrefix link opens the VPN Prefix List Dialog Box, page 2-146.
Route Target List	Shows the Route Target List value.
Next Hop	Shows the next hop for the route.
AS Path	Shows the AS path value.
Origin	Shows the Origin value: **0** = IGP **1** = EGP **2** = Incomplete
Local Preference	Shows the Local Preference value. The local preference attribute is used to select an exit point from the local autonomous system (AS).
Med	Shows the Multi-exit Discriminator value, which tells the router the preferred route into the AS from which the router advertisement originates. MED attribute values are advertised throughout the local AS. BGP speakers direct data over an entry point with the lowest MED attribute.
Communities	Shows the Community attribute.
SOO	Shows the Site of Origin attribute.
Other Attributes	Includes BGP attributes not shown in the preceding columns.

VPN Prefix List Dialog Box

When you click the VPN Route RDPrefix link in the VPN Route List Dialog Box, page 2-145, the VPN Prefix List dialog box opens to show information about the VPN prefixes and their associated VRFs.

You can also open this dialog box by clicking the VPN Prefix Count link in the Autonomous System List Dialog Box, page 2-104 or the BGP Domain Details Dialog Box, page 2-106.

Table 2-59 describes the fields and buttons of the VPN Prefix List dialog box.

Table 2-59 VPN Prefix List Dialog Box

Field	Description
BGP Domain	Shows the Domain in which the VPN prefix resides. Clicking the BGP Domain link opens the BGP Domain Details Dialog Box, page 2-106.
VPN Prefix	Shows each VPN prefix preceded by the VRF identifier.
VRF Count	Shows the number of VRFs associated with each VPN prefix. Clicking the VRF Count link opens the VPN Route List Dialog Box, page 2-145

OSPF Router Query Results Wizard Page

The OSPF Router Query Results wizard page appears after you Issue a Fast Query, page 2-83 on a router.

Table 2-60 describes the fields and buttons of the OSPF Router Query Results wizard page.

Table 2-60 OSPF Router Query Results Wizard Page

Field	Description
Router Name	Shows the unique Router ID, DNS name, or user-defined name of the router. Clicking the Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area(ID)s	Shows the unique identifier of the area in which the router resides. Clicking the Area ID(s) link opens the Area Overview Dialog Box, page 2-117.
Domain Name	Shows the domain in which the router resides.
Available	Shows the availability of the router. Options include: **Yes**—Router is available on the network. **No**—Router is not available on the network.
ABR	Shows whether the router is an Area Border Router (ABR). Options include: **Yes**—Router is an ABR. **No**—Router is not an ABR.

Table 2-60 OSPF Router Query Results Wizard Page (continued)

Field	Description
ASBR	Shows whether the router is an Autonomous System Boundary Router (ASBR). Options include: **Yes**—Router is an ASBR. **No—**Router is not an ASBR.
BGP Router	Shows whether the router is a BGP Speaker. Options include: **Yes**—Router is a BGP Speaker. **No**—Router is not an BGP Speaker
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

OSPF Interface Query Results Wizard Page

The OSPF Interface Query Results wizard page shows results returned after querying an OSFP interface. For information about querying for an OSPF interface, see:

- Issue a Fast Query, page 2-83
- Query for OSPF Interfaces, page 2-85

Table 2-61 describes the fields and buttons of the OSPF Interface Query Results wizard page.

Table 2-61 OSPF Interface Query Results Wizard Page

Field	Description
Type	Shows the type of interface. Options include: **NP2P**—Numbered Point-to-Point **UP2P**—Unnumbered Point-to-Point **Transit IF—**Transit interface
Identifier	Shows the unique identifier of the interface in the form of a host name or IP address. Clicking the Identifier link for an NP2P interface opens the Attributes for Numbered Point-to-Point Interface Dialog Box, page 2-122. Clicking the Identifier link for an UP2P interface opens the Attributes for Unnumbered Point-to-Point Interface Dialog Box, page 2-123. Clicking the Identifier link for a Transit interface opens the Attributes for Transit Interface Dialog Box, page 2-124.

Table 2-61 OSPF Interface Query Results Wizard Page

Field	Description
Destination	Shows the IP address of the router interface or network to which the queried interface is connected. Clicking the Destination link for an NP2P interface opens the Attributes for OSPF Router Dialog Box, page 2-119. Clicking the Destination link for an UP2P interface opens the Attributes for OSPF Router Dialog Box, page 2-119. Clicking the Destination link for a Transit interface opens the Attributes for Transit Network Dialog Box, page 2-125.
Available	Shows the availability of the interface on the network. Options include: **Yes**—Available **No**—Unavailable
Metric	Shows the metric cost of the interface.
Source	Shows the IP address of the of the interface. Clicking the Source link for an NP2P, UP2P, or Transit interface opens the Attributes for OSPF Router Dialog Box, page 2-119
Area ID	Shows the area in which the interface resides. Clicking the Area ID link for an NP2P, UP2P, or Transit interface opens the Area Overview Dialog Box, page 2-117
Domain Name	Shows the name of the domain in which the interface resides. Clicking the Domain Name link for an NP2P, UP2P, or Transit interface opens the OSPF Domain Details Dialog Box, page 2-104
Last Update Time	Shows the date and time of the most recent change to the link, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

OSPF Route Advertisement Query Results Wizard Page

The OSPF Route Advertisement Query Results wizard page shows results returned after querying an OSFP route advertisement. For information about querying for an OSPF route advertisement, see:

- Issue a Fast Query, page 2-83
- Query for an OSPF Route Advertisement, page 2-90

Table 2-62 describes the fields and buttons of the OSPF Route Advertisement Query Results wizard page.

Table 2-62 OSPF Route Advertisements Query Results Wizard Page

Field	Description
Type	Shows the type of route: **T3 Summary Route Adv**—Type 3 Summary Route advertisement **T4 Summary Route Adv**—Type 4 Summary Route advertisement **Stub Route Adv**—Stub Route advertisement **External Route Adv—**External Route advertisement **Transit Network Connection—**Transit Route advertisement
Prefix / ASBR Name	Shows the prefix of the route in the format `IP address/subnet mask`, for example: `1.1.1.1/24`. Clicking the Prefix/ASBR Name link for a T3 Summary Route Advertisement opens the Advertising Routers for T3 Summary Route Dialog Box, page 2-136 Clicking the Prefix/ASBR Name link for a T3 Summary Route Advertisement opens the Advertising Routers for T4 Summary Route Dialog Box, page 2-137 Clicking the Prefix/ASBR Name link for a Stub Route Advertisement opens the Advertising Routers for Stub Route Dialog Box, page 2-139 Clicking the Prefix/ASBR Name link for an External Route Advertisement opens the Advertising Routers for External Route Dialog Box, page 2-138 Clicking the Prefix/ASBR Name link for Transit Network Connection opens the Attached Routers for Transit Network Dialog Box, page 2-135
Advertising / Attached Router Name	Shows the Router ID, DNS name, or user-defined name of the router that advertises the route. Clicking the Advertising/Attached Router Name link opens the Attributes for OSPF Router Dialog Box, page 2-119.
Area Id	Shows the area in which the route was advertised. Clicking the Area Id link opens the Area Overview Dialog Box, page 2-117.
Domain Id	Shows the name of the domain in which the route was advertised. Clicking the Domain Id link opens the OSPF Domain Details Dialog Box, page 2-104.
Metric	Shows the cost of the route.

Table 2-62 OSPF Route Advertisements Query Results Wizard Page (continued)

Field	Description
Metric Type	Shows the Type 1 or Type 2 metric for an external route. Type 1 includes the cost of links interior to the autonomous system plus the cost of external links. Type 2 is the total cost of external links.
Forwarding Address	Shows the IP address of the router one hop from the ASBR advertised in a Type 4 Summary route.
Last Update Time	Shows the date and time of the most recent change to the route, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Clicking the Last Update Time link pivots to the Event Log. See Pivoting to the Event Log, page 2-64.

CHAPTER 3

Monitoring Unicast and Multicast Services

Monitoring Data Between Endpoints

Your network contains multiple nodes, servers and routers, which all function to deliver a service or services to your client base.

- Example: A service provided by a hospital might consist of an interconnected, globally dispersed set of databases with medical records and patient information, available 24 hours a day, 7 days a week.
- Example: A service offered by a telecommunications firm might offer e-mail, Web access, voice over Internet protocol (VoIP) telephone service, or a streaming media application.

Data within these networks moves from a point of origin to one or more destinations, through multiple links. When problems occur, it is difficult to locate the point of failure and the cause. Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) is able to monitor network services between the endpoints of each data route, for both unicast and multicast services.

Differentiating Unicast and Multicast Services

Services can use individual service paths or multiple paths to carry data between endpoints within a single, or across multiple autonomous systems (AS's) and routing domains.

- *Unicast services* are transported over a single path, from one end point, the source, to another end point, the destination.
- *Multicast services* are transported from a single source to multiple recipients.
  - *A Multicast Distribution Tree* is constructed to carry services to subscribing destinations. In multicast routing, the source sends traffic to a selected group of hosts, represented by a *multicast group* address. A set of leaf routers subscribe to this address.

Path Analyzer supports both unicast and multicast services. Users can monitor routing information for both service types using the Path Analyzer Service Monitor and Service Viewer.

Monitoring Unicast Services

In unicast services, traffic is routed through the network along a single path from the source to the destination host. A unicast router only pays attention to the destination address and the path, not the source address. The router scans the routing table for the best route and forwards a single copy of the unicast packet toward the destination.

Branches of a Unicast Service

When load balancing is in effect, the service path divides into individual, equal-cost segments or *branches* that carry data toward the destination. Each branch represents one unique route from the source to the destination.

To help you track the cause of service-related issues, the *Service Path Branches* section of Service Monitor lists the branches of a service path. A change in the branch count may indicate that an interface metric has changed, causing service data to be rerouted over an unintended path, which interrupts load balancing.

Visual, Real-time Traceroute on Multiple, Simultaneous Flows

In Service Monitor, creating unicast services and service paths allows you to monitor where information travels, ensuring that services are continuously available, and that critical data is received by the users and processes that need it. Having an up-to-date picture of service deployment allows you react to potential failures faster, with a clearer understanding of the location and cause of the problem. For information about creating unicast services in Service Monitor, see Creating Unicast Services and Related Service Paths, page 3-7.

Note Viewing the transmission of a unicast service path across your network is similar to having a visual, real-time display of the type of data you receive when you run the `traceroute` command. Viewing a unicast service in transit is equivalent to receiving a visual display of the results of multiple, simultaneous `traceroute` commands run on all service paths that make up a service.

In addition to monitoring unicast services from Service Monitor, you can select and view a unicast service and its component service paths in the Service Viewer. In the Service Viewer, you can view the status of the routers and links across which unicast service data traverses between endpoints. For information about using the Service Viewer, see Viewing Services in the Service Viewer, page 2-45.

Real-time and Historical Views of Unicast Services

You can view services and service paths in two modes:

- **Real-time**—Presents a current, dynamic display of unicast services and associated service paths across the multiple autonomous systems and routing domains of your network.
- **Historical**—Returns your network to a previous state, enabling you to review past conditions affecting unicast services and associated service paths. For information about starting the Service Monitor while running a past sequence of events, see Starting a Historical Session, page 13-3.

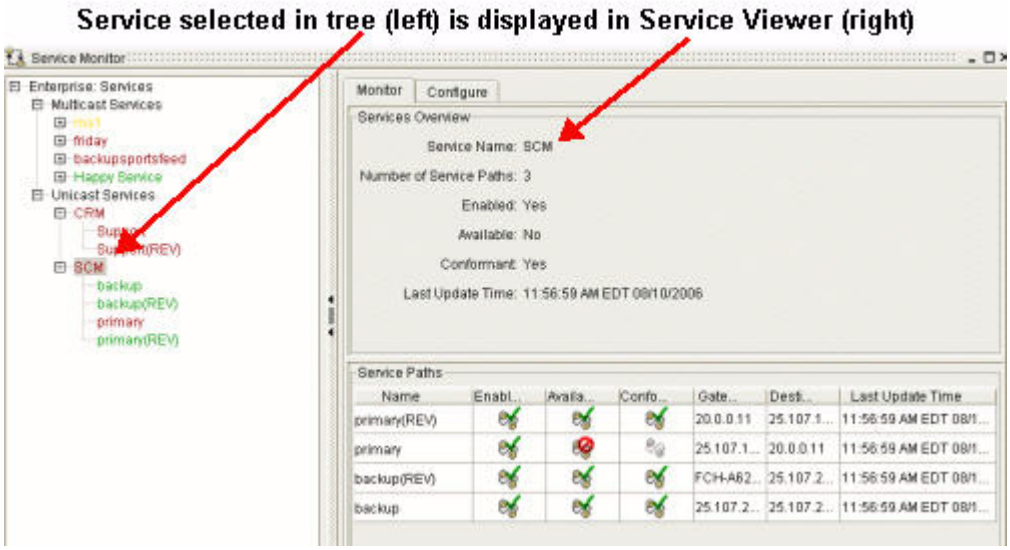
Service Monitor Tasks

- Starting Service Monitor, page 3-3
- Monitoring the Flow of Business-Critical Data, page 3-4
- Creating Unicast Services and Related Service Paths, page 3-7
- Interpreting Service Data for Unicast Services, page 3-15
- Viewing Unicast Services Graphically, page 3-19
- Viewing the Root Cause of Unicast Service Path Issues, page 3-23
- Viewing Details of Unicast Services and Unicast Service Paths, page 3-24
- Managing Baselines of Service Paths, page 3-25
- Managing Unicast Services and Service Paths, page 3-26
- Enabling and Disabling Unicast Services and Service Paths, page 3-31
- Setting Alarms on Unicast Services and Service Paths, page 3-32
- Replaying Historical Services, page 3-33

Starting Service Monitor

To start Service Monitor from the Path Analyzer taskbar, click **Start > Service Monitor**. The Service Monitor opens in the Path Analyzer Management Console (see Figure 3-1).

Figure 3-1 Service Monitor in Path Analyzer



Monitoring the Flow of Business-Critical Data

Your success depends upon your ability to maintain the applications and services you provide to your customers. Path Analyzer offers you the ability to obtain information about IP-layer routing in order to help you make routing decisions and to understand the impact of these decisions on your services.

How Data is Displayed in Service Monitor

Use Service Monitor to create abstract, visual representations of your services—the multiple connections and devices that generate, transmit, and deliver data to your end users.

Figure 3-2 Service Displayed Graphically in the Service Viewer and Service Monitor

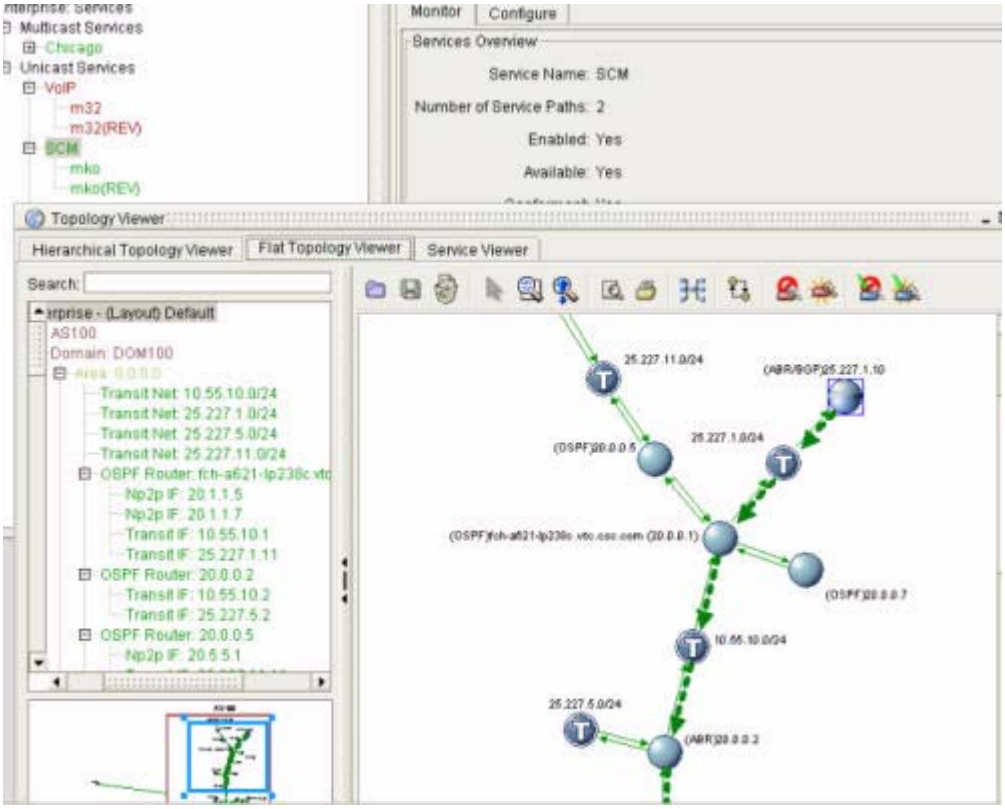


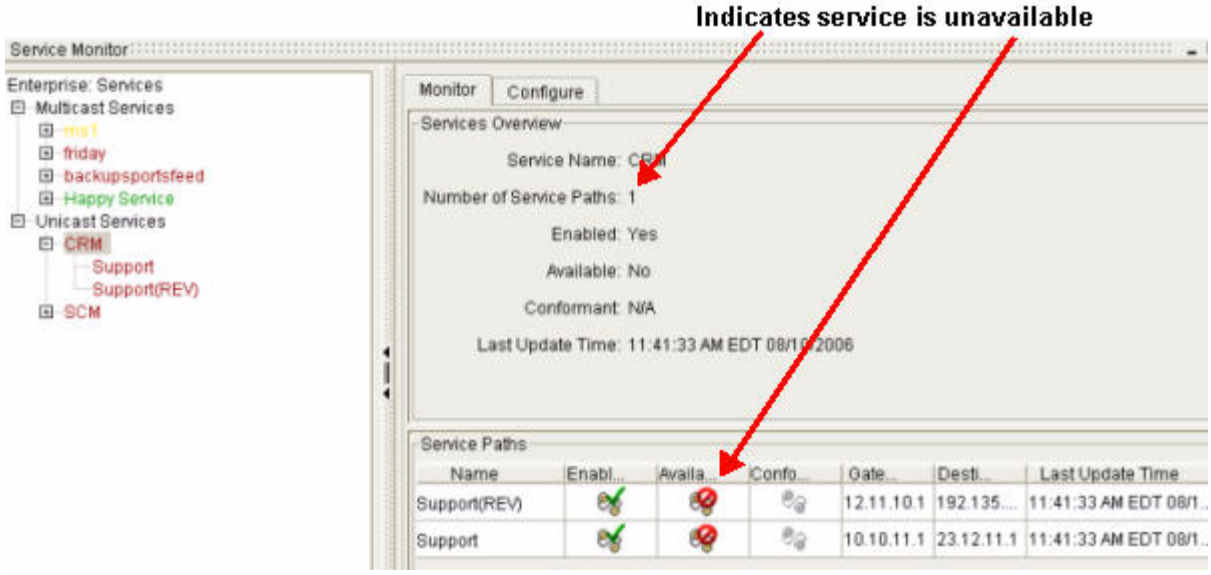
Figure 3-2 illustrates how a service is displayed using the Topology Viewer in Path Analyzer. Notice that the service is also listed hierarchically on the left side of the screen.

Unicast Service Paths: Endpoints of a Service

Each unicast service is composed of individual connections between endpoints. The endpoints are:

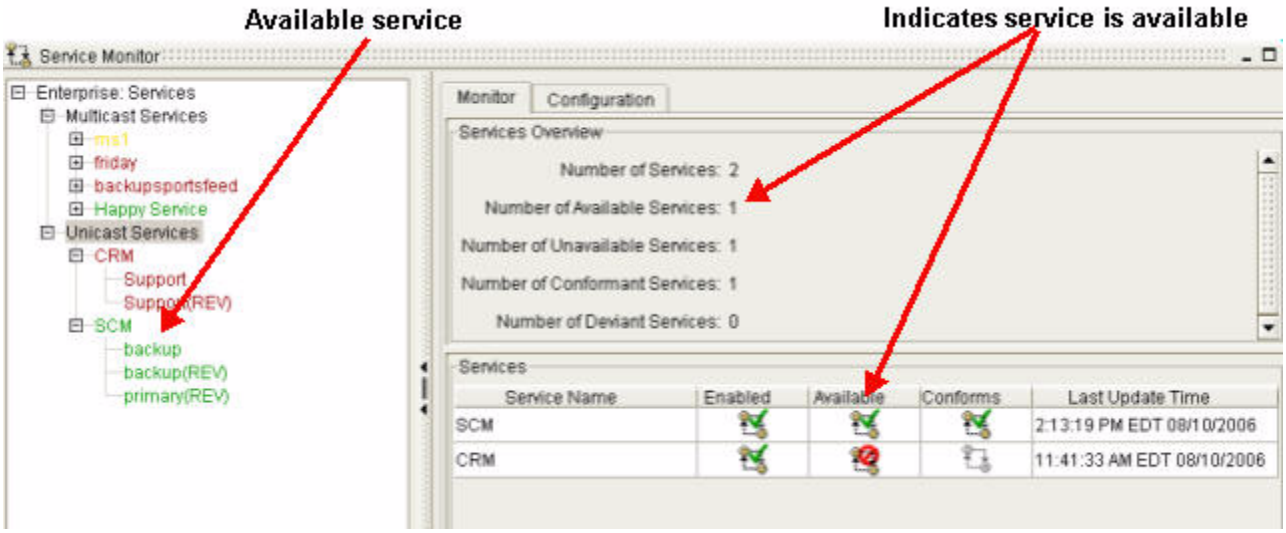
- **Primary Gateway—**the first router that receives service data from a host and passes it one hop toward the destination.
- **Destination**—the router that forwards the data to the destination host where the data is used.

Figure 3-3 Unavailable Service



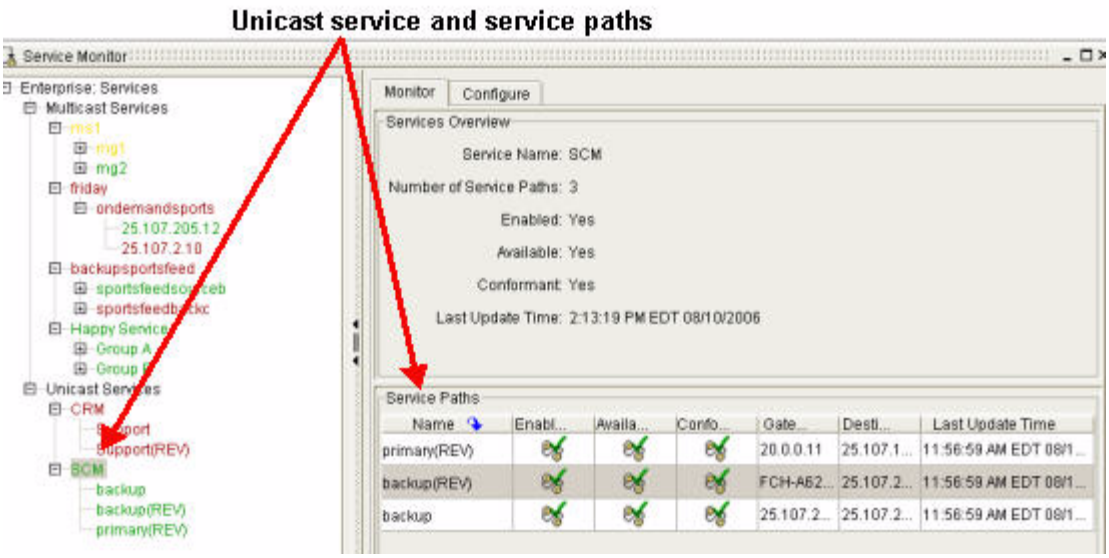
The availability and integrity of these connections, referred to as *service paths*, is vital to your business. The state of a single service path affects the state of the entire unicast service. When a service path becomes unavailable on your network, the related unicast service becomes unavailable (see Figure 3-3).

Figure 3-4 Available Service: View Unicast Service Paths



Clicking a unicast service causes its related service paths to be displayed in the Service Path section of the Service Monitor window (see Figure 3-4).

Figure 3-5 Service Paths of a Selected Unicast Service

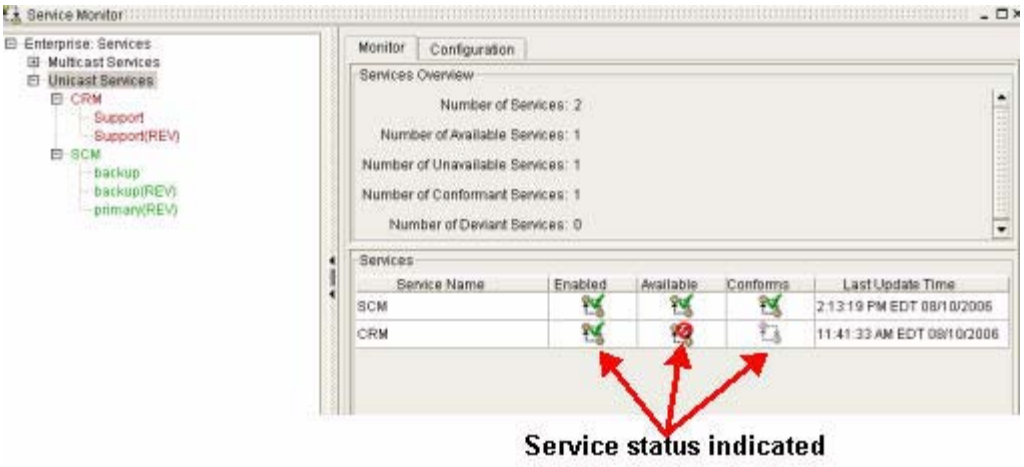


In Service Monitor, unicast services and their related service paths are displayed with icons and text that indicate:

- Status (enabled or disabled).
- Availability on the network.
- Conformity to the path engineered between a source and destination.
- Date and time of the most recent updates.
- Source, destination, and gateway of the service path (Figure 3-6).

For a full listing of these icons, see Table 3-1.

Figure 3-6 Displays Conformance, Gateway, and Destination



After creating a unicast service and its related service paths in Service Monitor, you can:

- Monitor the exact set of routers and interfaces that the unicast service relies on to deliver application traffic.

- Identify when, where, and which unicast services are affected, in what way, and why.

For more information, see Interpreting Service Data for Unicast Services, page 3-15.

Creating Unicast Services and Related Service Paths

Creating unicast services and service paths in the Service Creation Wizard enables Path Analyzer to monitor the routing patterns of unicast services in your network.

Required Information for Creating a Unicast Service or Service Path

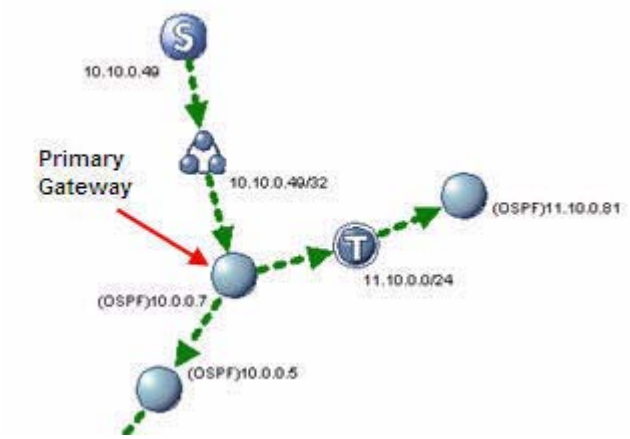
When you create a unicast service in the wizard, you must provide the following information for each service and service path:

- Name that uniquely identifies the unicast service or service path.
- Router IDs for the unicast service or service path.
  - Source Host IP address or Router ID
  - Destination Host IP address

Note All service paths begin at the router that receives packets from the host. Other protocols, such as Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) provide rules that determine a packet's travels from the host to the router that Path Analyzer uses as the source.

The *primary gateway* is one hop from the source host (see Figure 3-7).

Figure 3-7 Locating the Primary Gateway



Create Uni-Directional or Bi-Directional Service Paths for a Unicast Service

Uni-directional service paths travel in one direction between the source and the destination.

Bi-directional service paths travel in two directions:

- Initial direction between the source and the destination.

- Reverse direction from the destination back to the source.
  - By default, *the **source** of the initial direction becomes the destination of the reverse direction* (seen Figure 3-8).
  - Conversely, *the **destination** of the initial direction becomes the source of the reverse direction* (see Figure 3-9).

Note Please note that you must enter the IP address of the Gateway Router ID (shown as letter **G** below).

Figure 3-8 Bi-directional Service Path

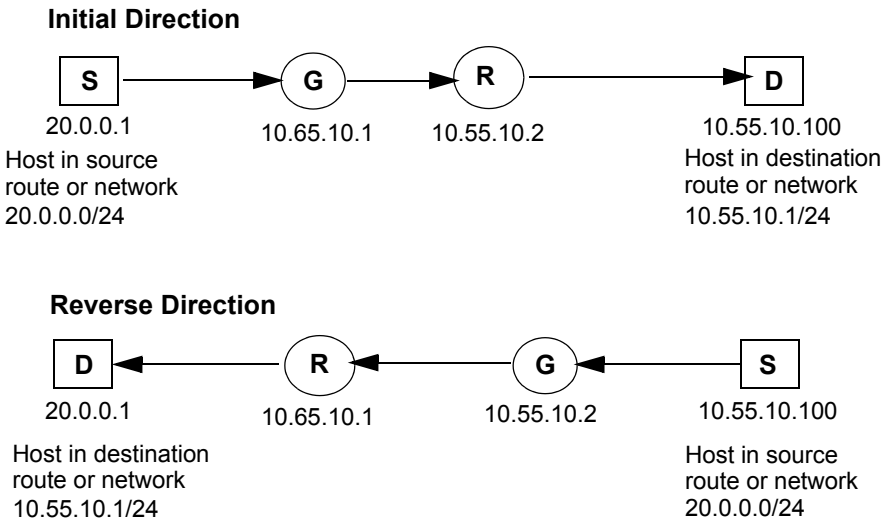
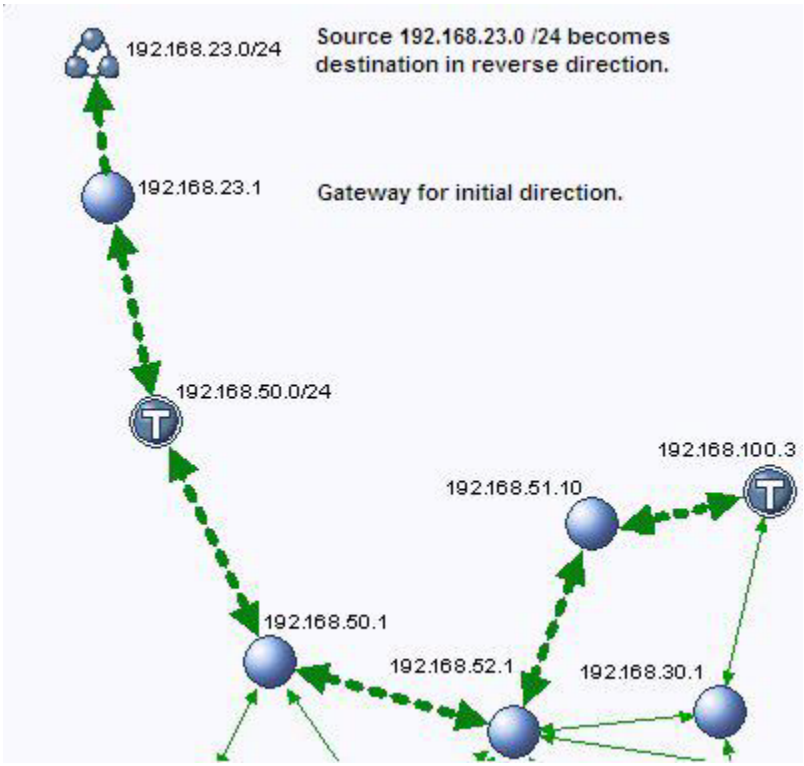


Figure 3-9 Elements of a Bi-directional Service Path



Note When you create a new unicast service or unicast service path in Service Monitor:

- Complete all mandatory fields, which are shaded blue.
- Assign a name to each unicast service or service path you create. Each name for a unicast service must be unique and each name for a service path must be unique within a unicast service.

Start the Service Creation Wizard

To start the service creation wizard:

Step 1 Use the procedure in Start Service Monitor, page 3-37.

The Service Monitor window appears.

Step 2 Click on Unicast **Services** in the left-hand pane of the Service Monitor.

Step 3 Select the **Configuration** tab.

Step 4 In the Service Creation field, click the **Create Service** button.

The Service Creation Wizard appears.

Step 5 (Optional) Click the **Do not show this screen again** check box.

Step 6 In the initial wizard page, click **Next**.

The Configure a Service screen appears (see Figure 3-10).

Figure 3-10 Configure a Service Screen in Service Creation Wizard

Provide a Name for the Unicast Service

To enter a name for the service being created:

Step 1 Type the name of the new unicast service in the Enter a Unique Service Name field. Select a name that indicates the type of application, network service, location, or department that relies heavily on the service.

Examples:

- SecurityVirusScanner
- ERP_EastCoast
- Order Processing System

Step 2 By default, the **Check to configure Service Paths for your Service** check box is selected.

a. Keep the default selection to create service paths for the unicast service.

b. Click **Next** to continue to Configure a Service Path, page 3-11.

or

a. Click the check box to deselect the option to create service paths.

b. Click **Next**.

c. Click **Finish**.

The new unicast service is listed in the Services hierarchy at the left of the Service Monitor window. You can always add service paths at a later date.

See Add Service Paths to an Existing Unicast Service, page 3-14.

Configure a Service Path

To configure a service path for the service being created:

Step 1 Enter a name for the new service path in the Service Path Name field (see Figure 3-11).

Select a name that indicates the type of application, network service, location, or department that relies heavily on the service path.

Examples:

- AcctPayable_CA-Office
- ERP_+NYCAdminGroup
- Order Processing Midwest_Distribution

Note For added ease in creating the service path, click **Start > Topology Viewer** to start the Topology Viewer. From the Flat or Hierarchical Topology Viewers of the Topology Viewer, you can identify the primary gateway of the service path and the networks where the source and destination hosts reside. You can also start the Topology Browser for more information about endpoints and intermediate points of the unicast service and its service paths.

Figure 3-11 Configure a Service Path Screen in Service Creation Wizard

Step 2 Enter the IP address of the service path source on the network in the Source IP Address field.

Step 3 In the Gateway Router ID field:

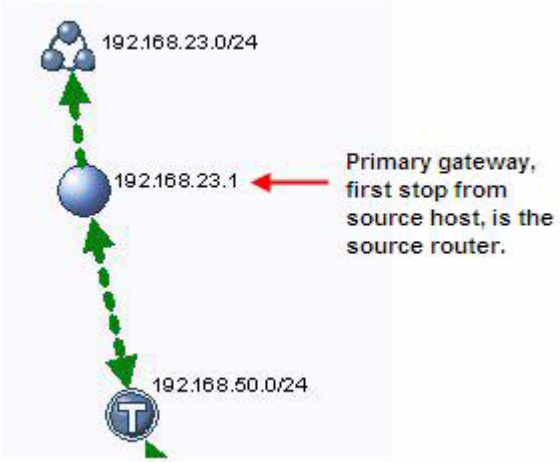
- If you previously entered the IP address of a host, enter the IP address of the router that is the first hop from the source toward the destination in the Primary Gateway field.

or

- If you previously entered a Gateway Router ID, you can override the auto-complete feature by deleting the IP address and entering the IP address of another router that is one hop from the source to the gateway.

In Figure 3-12, the source is a host in the network 192.168.50.0/24. The gateway is 192.168.23.1, which is the first hop toward the destination host 192.168.23.0/24.

Figure 3-12 Locating the Primary Gateway



Step 4 Select the autonomous system (AS) or Open Shortest Path First (OSPF) routing domain in which the source of your unicast service path resides from the Gateway AS or Domain drop-down menu.

Step 5 Enter the IP address of the destination router in the Destination IP Address field. The destination can be any IP address, whether internal or external to the managed network.

Step 6 Select one of the following choices to continue:

- Configure a Reverse Service Path, page 3-12
- Complete the Wizard, page 3-13

Configure a Reverse Service Path

The Service Creation Wizard provides a quick mechanism for configuring the service path in the reverse direction.

To configure a reverse service path:

Step 1 Select the **Check to Configure Reverse Service Path** check box.

This option is selected when a check mark is displayed in the corresponding check box.

Step 2 Click **Next**.

The Configure a Reverse Service Path screen appears (see Figure 3-13).

When you create a reverse service path, the following fields of the **Configure** tab are automatically filled in with values from the previous service path:

Reuse or Rename Service Path:

- **Reverse Service Path Name**—By default, this field lists the name you provided previously for the service path in one direction. You can reuse the name or delete it and enter a new name for the service path in the reverse direction.

  For example, if you named the original service path *Client to Server*, you can either:

- Reuse the name of the service path in the reverse direction. Service Monitor appends (REV) to the name: *Client to Server (REV)*
- Rename the reverse path: for example, change the name to *Server to Client*.

Figure 3-13 Configure a Reverse Path Screen in Service Creation Wizard

- **Reverse Source IP Address—**Shows the IP address of the reverse source. The reverse source is the IP address of the destination you specified previously, when you created the initial, uni-directional service path. *You cannot override this setting.*
- **Gateway AS or Domain**—Shows the autonomous system (AS) or OSPF routing domain in which the source of your service path resides.
- **Reverse Destination IP Address—**Shows the IP address of the reverse destination. The reverse destination is the IP address of the source you specified previously, when you created the initial, uni-directional service path. *You cannot override this setting.*

Step 3 Enter the Reverse Gateway.

- If you previously entered a host IP address for the primary gateway, in the Reverse Gateway field, enter the IP address of the router that is the first hop from the source toward the destination.

  or

- If you previously entered a Router ID for the unidirectional destination, the Router ID of the gateway is the same as the IP address of the reverse source router. This IP address is supplied for you in the Reverse Gateway field.

Step 4 Click **Next**.

Complete the Wizard

To complete the reverse service path creation wizard:

Step 1 Click **Next**.

The Following Services Path(s) will be Added screen appears (see Figure 3-14).

Figure 3-14 The Following Services Path(s) will be Added Screen in Service Creation Wizard

Step 2 If you wish to configure more service paths, keep the default selection: **Check to configure additional Service Paths for your Service**.

A check mark is displayed in the check box to indicate that the option is selected.

Step 3 Click **Next**.

You will return to the Configure a Service Path screen. See Configure a Service Path, page 3-11l.

If you don't wish to configure more service paths, deselect the check box **Check to configure additional Service Paths for your Service**.

Step 4 Click **Next.**

Step 5 Click **Finish**.

Add Service Paths to an Existing Unicast Service

To add service paths to a service at a later date:

Step 1 Select the unicast service you want to add a service path to from the Services hierarchy.

Step 2 Select the **Configure** tab in the Service Monitor window.

Step 3 Click **Create Service Path(s)**.

or

Step 1 Select **Unicast Services** from the Services hierarchy.

Step 2 Select the **Monitor** tab in the Service Monitor window.

Step 3 In the Services section, right-click a service, then click **Add Service Paths**.

Step 4 Complete the Service Path Creation Wizard.

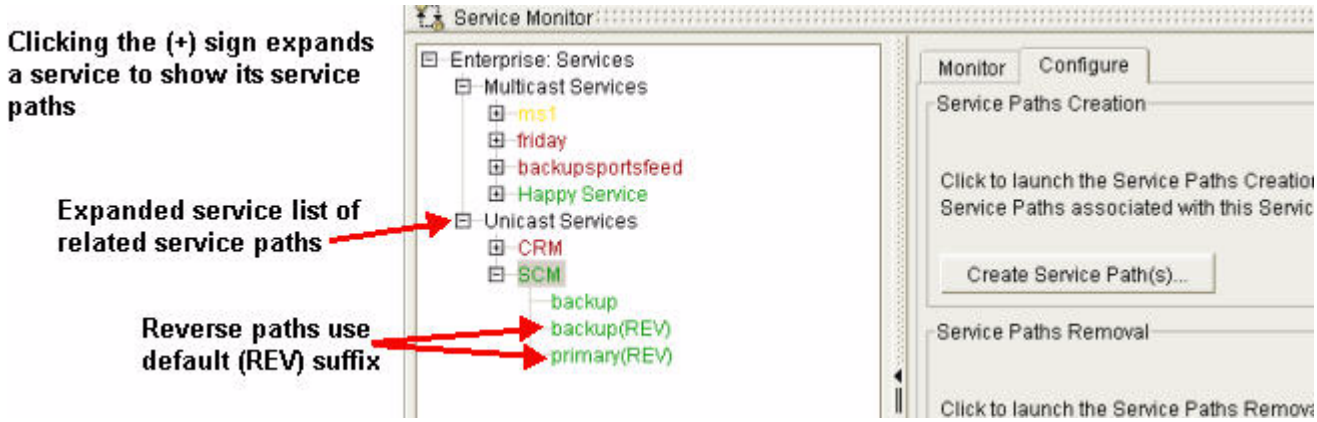
See Configure a Service Path, page 3-11 for information about creating a new service path.

View the List of Unicast Services and Related Paths

In the Enterprise Services Hierarchy, after creating a unicast service, the service is listed in the Service Monitor window, in the Services hierarchy of the enterprise.

All service paths related to a specific unicast service are listed under the unicast service to which they belong. To expand a unicast service and view its related service paths, click the plus sign (+) (see Figure 3-15).

Figure 3-15 Service Monitor Menu Hierarchy



Bi-directional service paths are listed in the enterprise hierarchy of unicast services as two separate uni-directional paths.

By default, each path in a bi-directional service path uses the same name and identifying number. The service path created in the reverse direction is displayed with the term, (REV). You can override this default and provide a different name for the service path traveling in the reverse direction.

Interpreting Service Data for Unicast Services

In the Enterprise Services tree, unicast services and paths are listed hierarchically, and are color-coded.

- Green unicast services and service paths are available on the network and conform to a *baseline*—the path configured for data to take across the network.
- Red unicast services and service paths are unavailable.
- Yellow unicast services and service paths deviate from the baseline.
- Gray unicast service and service paths are disabled.

Clicking the plus sign (+) in front of the Enterprise Services field in the network hierarchy causes information about a unicast service to be displayed in the Services section of the Monitor tab. Clicking a unicast service causes information about its related service paths to be displayed in the Service Path section (see Figure 3-16).

Figure 3-16 Unicast Service Data in Service Monitor

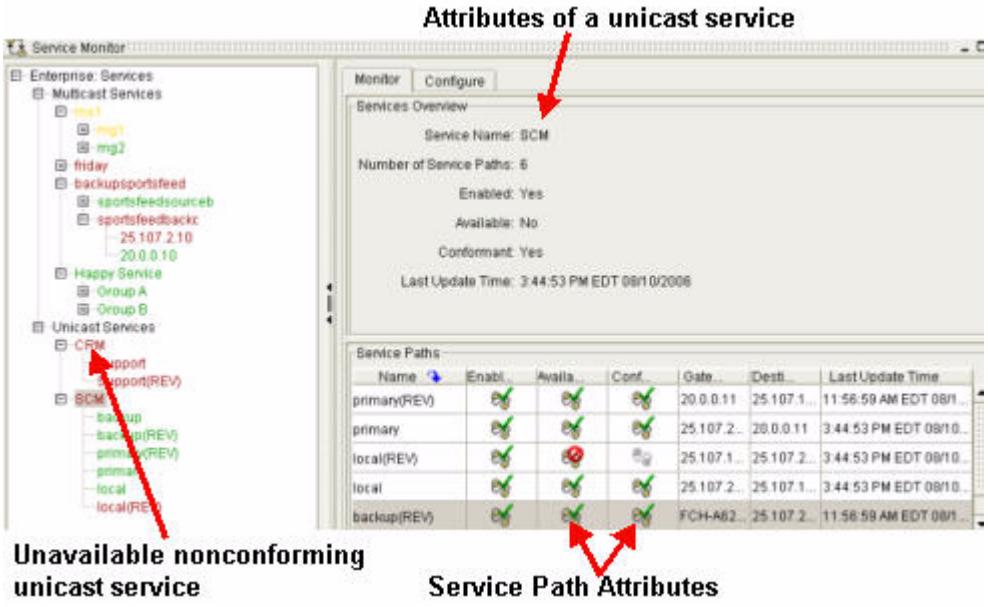
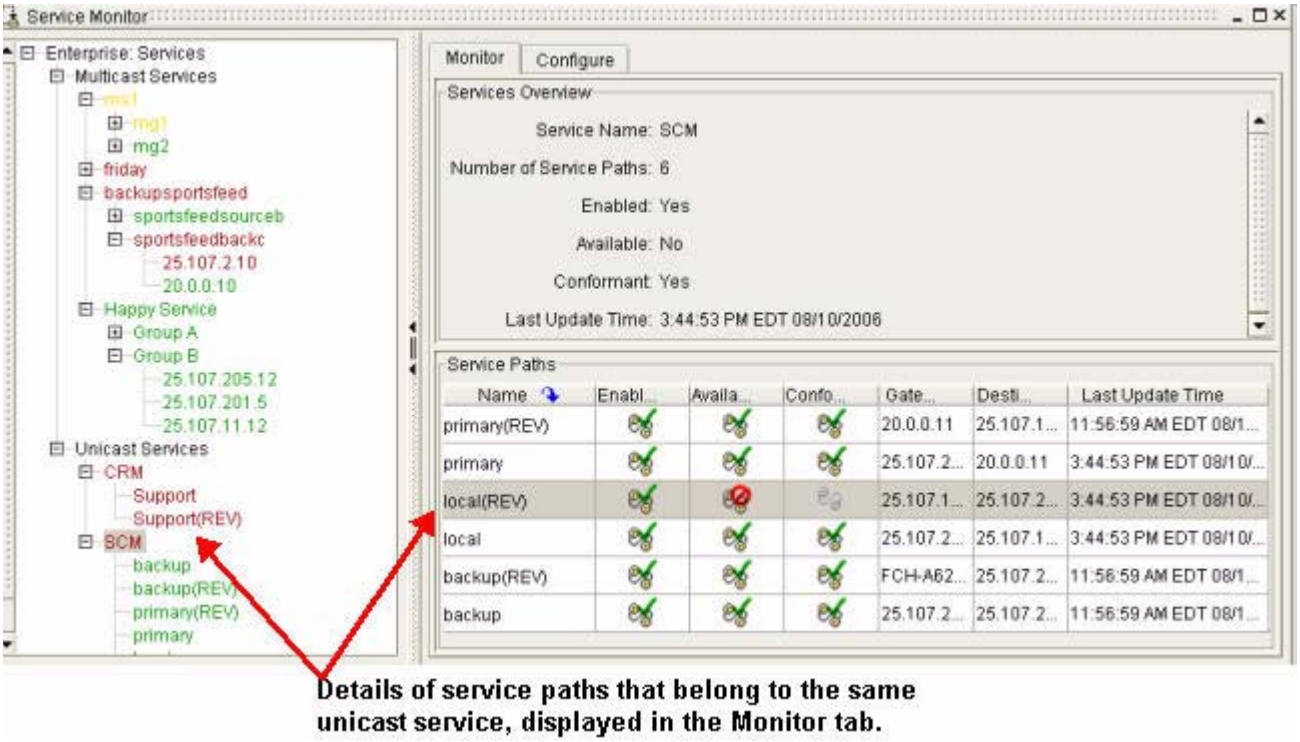


Figure 3-17 Details of a Unicast Service



When you select a unicast service from the menu hierarchy its details are displayed in the **Monitor** tab (Figure 3-17).

Figure 3-17 explains the icons and terminology used to indicate the status of unicast services and service paths.

Table 3-1 Indicators of Status, Availability, and Conformity in Service Monitor

Icon for Entity	Displayed in Service Monitor Field	Description
Services		
	Enabled	Indicates that the service is enabled and actively monitored in Service Monitor. A unicast service is enabled if any service paths are enabled. See Remove a Single Service Path, page 3-29 for detailed information about enabling and disabling services and related service paths.
	Available	Indicates that at least one segment exists for all service paths, allowing them to forward packets between the gateway and the destination. The unicast service is available on the network.
	Conforms	Indicates that all service paths of the unicast service follow the set path of transmission between source and destination that you established when you created the service. This path of transmission is referred to as the *baseline* of the service. Each service path has its own set baseline. See Viewing Unicast Services Graphically, page 3-19 for information about using the maps of the Topology Viewer to analyze the conformance of a unicast service.
	Enable	Indicates that the service is disabled in Service Monitor. The unicast service cannot be monitored until it is re-enabled on the network. All service paths are disabled if a service is disabled.
	Available	Indicates that at least one of the service paths that make up the unicast service has become unavailable on the network.
	Conforms	Indicates that at least one service path of the unicast service does not conform to its set baseline. See Viewing the Root Cause of Unicast Service Path Issues, page 3-23 on page 3-25 for information.
	Enable	Indicates that a unicast service has no service paths.

Table 3-1 Indicators of Status, Availability, and Conformity in Service Monitor

Icon for Entity	Displayed in Service Monitor Field	Description
	Available	Indicates that all related service paths are disabled or that no service paths exist for a service.
	Conforms	Indicates that baselines have not been established for any service paths of a service. It can also indicate that there is no service path or all service paths are disabled.
Service Paths		
	Enable Service Path	Indicates that the service path is enabled and actively monitored.
	Available	Indicates that at least one branch of a service path allows packet forwarding between the gateway and the destination. The service path is available on the network.
	Conforms	Indicates that the service path conforms to its set baseline. See Display Graphical Unicast Service Path, page 3-21 for information about using the maps of the Topology Viewer to analyze the conformance of a service path.
	Enable	Indicates that the service path is disabled. Monitoring is interrupted.
	Available	Indicates that all branches of a service path become unavailable, interrupting packet forwarding between the gateway and the destination.
	Conforms	Indicates that the service path does not conform to its baseline.
	Conforms	Indicates that a baseline has not been established for the unicast service path. A service path does not have a baseline if one or more intermediate routers or networks are unavailable when you create the unicast service path or if you remove it.

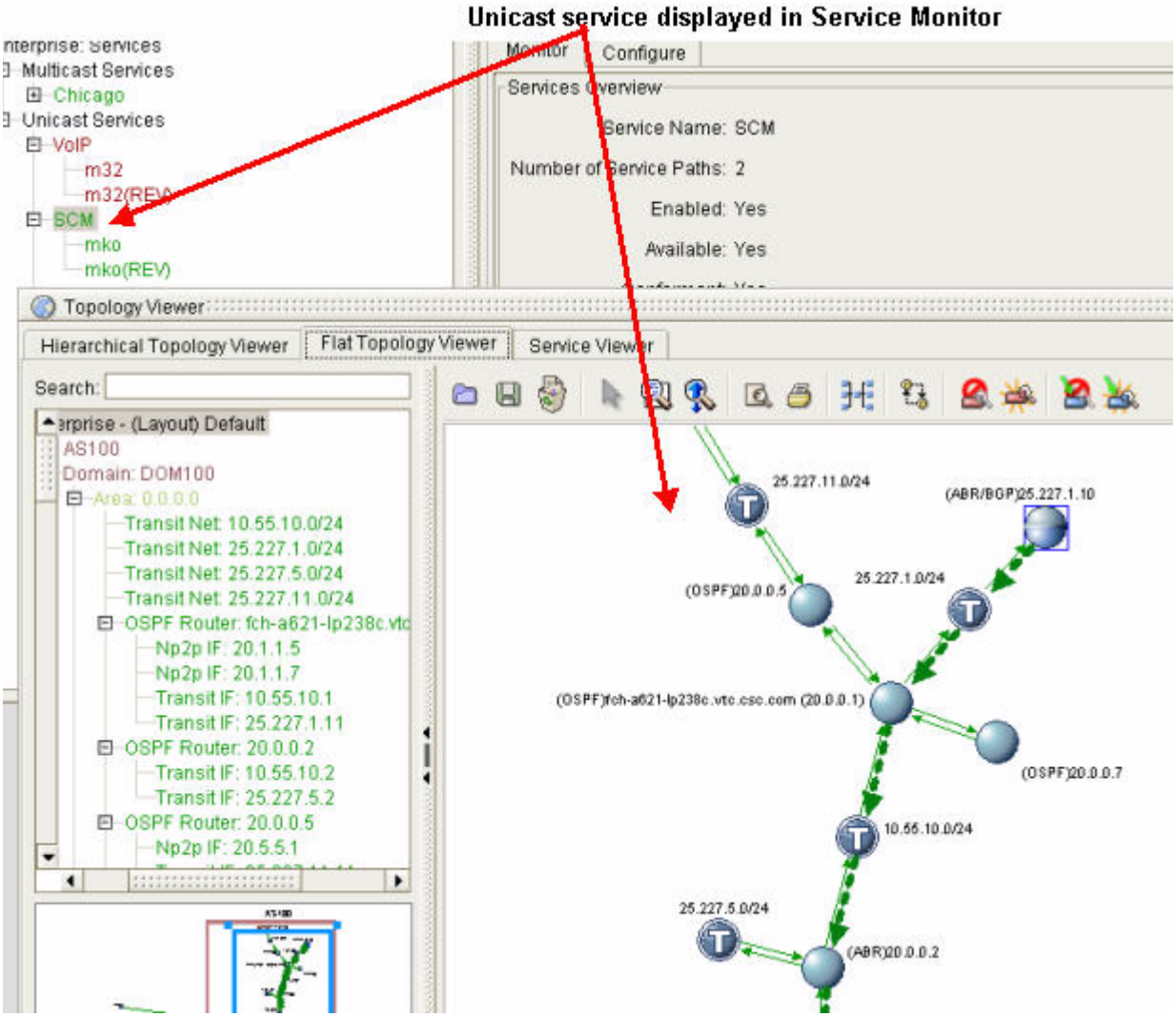
Viewing Unicast Services Graphically

You can view a unicast service or service path graphically using the Flat Topology Viewer or the Hierarchical Topology Viewer. Further, the **Service Viewer** tab in the Topology Viewer lets you see the entire service, and each of its pathways—the direction over which data travels across the network from source to endpoint.

The depiction of data pathways in the Topology Viewer correlates with the Service Monitor icons that indicate the status, availability, and conformity of the unicast service and its service paths.

For information about the status of unicast services and service paths represented by Service Monitor icons, see Interpreting Service Data for Unicast Services, page 3-15.

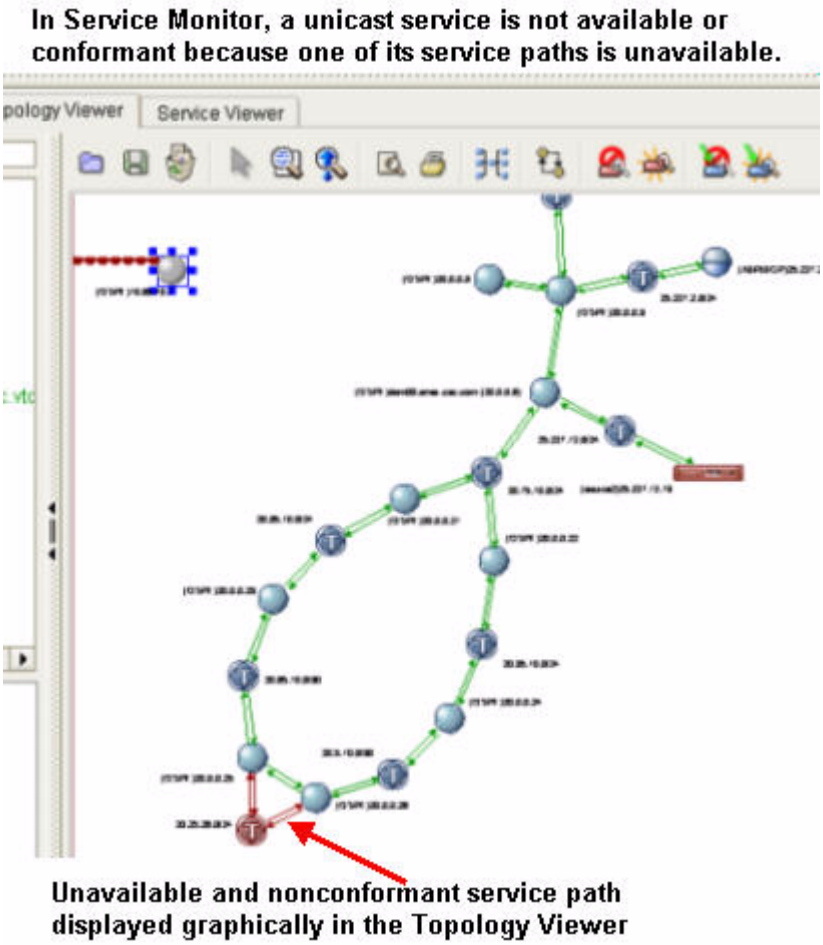
Figure 3-18 Service Displayed Graphically



The Flat Topology Viewer, Hierarchical Topology Viewer, and Service Viewer provide service views and use the following colors to indicate service status as they correspond to the **Enabled**, **Available**, and **Conforms** status icons displayed in the Service Monitor (see Figure 3-18).

Figure 3-19 shows the data flow of an unavailable and non-conforming service, shown graphically in the Topology Viewer. The graphic also shows the second set of icons you can select to display in the maps of the Topology Viewer, and individual element connections. For information about setting the display of icons and connections, see Select Topology Viewer Settings, page 1-25.

Figure 3-19 Graphical Service Path Showing an Unavailable Service



Service Monitor and the Topology Viewer indicate when a unicast service becomes unavailable or deviates from its configured baseline.

For detailed information about how to interpret the visual display of unicast services and service paths in the maps of the Topology Viewer and Service Monitor, see Interpreting Service Data for Unicast Services, page 3-15.

Display Graphical Unicast Service

To display a graphical unicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37, and click on **Unicast Services**.

The **Monitor** tab appears.

Step 2 In the Services section of the tab, right-click the unicast service you want to map.

Step 3 Click **Display Graphical Service** and select one of the following options:

- **Display Graphical Service in Flat Viewer—**Opens the Topology Viewer and presents the unicast service in the Flat Topology Viewer.
- **Display Graphical Service in Hierarchical Viewer—**Opens the Topology Viewer and presents the unicast service in the Hierarchical Topology Viewer.
- **Display Graphical Service in Service Viewer—**Opens the Topology Viewer and presents the unicast service in the Service Viewer.

The selected tab opens in the Topology Viewer showing the flow of service-related data, represented by dashed arrows.

Display Graphical Unicast Service Path

To display a graphical unicast service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Unicast Services**.

The **Monitor** tab appears.

Step 2 Select a unicast service in the hierarchical menu.

Step 3 Right-click the service path you want to map in the Service Path section of the tab.

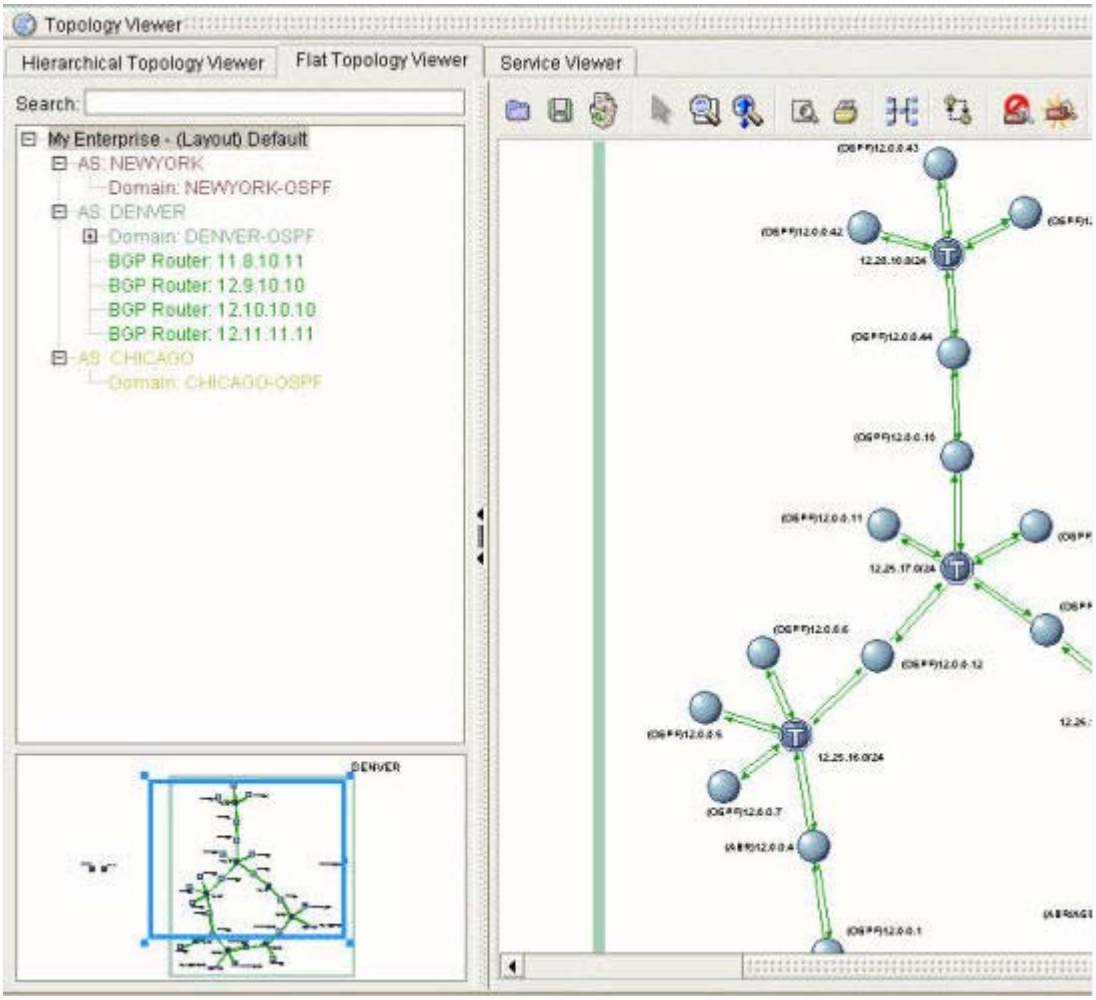
Step 4 Click **Display Graphical Service Path** and select one of the following options:

- **Display Flat Graphical Service Path—**Opens the Topology Viewer and presents the service path in the Flat Topology Viewer.
- **Display Hierarchical Graphical Service Path—**Opens the Topology Viewer and presents the service path in the Hierarchical Topology Viewer.

The selected tab opens in the Topology Viewer showing the flow of service-related data, represented by dashed arrows.

Figure 3-20 shows an available and conforming unicast service in the Hierarchical Topology Viewer. All service paths of the unicast service are available and conform to their configured baselines.

Figure 3-20 Available, Conforming Service



Remove a Graphical Unicast Service

To remove a graphical unicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Unicast Services**.

The **Monitor** tab appears.

Step 2 Right-click the name of the unicast service you want to remove from the map in the Services section of the tab, then click **Remove Graphical Service Display**.

Depending on which views you have opened, one or more of the following options is displayed:

- **Remove Flat Graphical Service Display**—Removes the graphical service from the Flat Topology Viewer.
- **Remove Hierarchical Service Display**—Removes the graphical service from the Hierarchical Topology Viewer.
- **Remove Monitored Service Display**—Removes the graphical service from the Service Viewer.

Step 3 Select one the options listed in Step 2.

The Topology Viewer remains open in the Management Console.

Remove a Graphical Service Path

To remove a graphical unicast service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Unicast Services**.

The **Monitor** tab appears.

Step 2 Right-click the name of the service path you want to remove from the map in the Service Path section of the tab, then click **Remove Graphical Service Path Display**.

Depending on which views you have opened, one or more of the following options is displayed:

- **Remove Flat Graphical Service Path Display**—Removes the graphical service path from the Flat Topology Viewer.
- **Remove Hierarchical Service Path Display**—Removes the graphical service path from the Hierarchical Topology Viewer.
- **Remove Monitored Service Path Display**—Removes the graphical service path from the Service Viewer.

The Topology Viewer remains open in the Management Console.

Note Removing a graphical service path will only remove the path from the Topology Viewer, not the Service Monitor.

Viewing the Root Cause of Unicast Service Path Issues

Misconfigurations, metric changes, and other routing issues can cause unicast services to become unavailable or to veer from set baselines. Identifying the root cause—the set of events that interrupt services—can be a time-consuming, labor-intensive process.

Service Monitor simplifies root cause identification by identifying the set of events that affect a service or service path on your network. The root cause is supplied in response to network events only, not to user actions that affect services, such as refreshing the baselines of a service path.

Note The root cause of a service-related issue is available for unicast services and service paths listed in Service Monitor and for unicast service and service path alarms triggered and displayed in Alarm Monitor.

View the Root Cause of a Change to a Unicast Service Path

To view the root cause of a change to a unicast service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the unicast service that contains the service path you want to view from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the unicast service path you want to view in the Service Paths section of the tab, then click **Display Root Cause**.

The Root Cause window opens in the Monitor tab and shows the events that caused the unicast service to change to its current state.

Note No **Display Root Cause** menu option will appear unless the service path has changed in some way.

Viewing Details of Unicast Services and Unicast Service Paths

Service Monitor provides data about unicast services, related service paths, and the branches of service paths.

View Details of a Unicast Service

To view the details of a unicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select a service to view the details of from the hierarchy of unicast services at the left of the Service Manager window.

Details of the unicast service are displayed in the Service Overview section of the Monitor tab.

View Details of a Service Path

To view the details of a unicast service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select a service path to view the details of from the hierarchy of unicast services at the left of the Service Manager window.

If the service path is not displayed automatically, expand the unicast service that contains it by clicking the plus (+) sign.

Details of the service path are displayed in the Service Path Details section of the Monitor tab.

All branches and sub-branches of the service path are displayed in the Service Path Branches section of the Monitor tab.

Step 3 Click the plus (+) sign at the top-level Service Path Branches hierarchy to expand the tree of branches that the service path contains.

Managing Baselines of Service Paths

You can set a baseline on any available service path. If you create a service path when intermediate routers or networks are unavailable, a baseline is not established for the service path or its related unicast service.

When the expected behavior of a service path does not conform to its baseline due to configuration changes in the network or any other changes in the network, you can reset the baseline.

You can also remove a baseline of a service path or service.

Resetting and Removing Baselines

The baseline of a service path can be reset or removed.

- Reset the Baseline of a Service Path, page 3-25
- Remove the Baseline of a Service Path, page 3-25

Reset the Baseline of a Service Path

To reset the baseline of a service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select the unicast service that contains the service path you want to change from the hierarchy of services at the left of the Service Manager window.

If the service path is not displayed automatically, click the plus (**+**) sign of the service that contains it.

Step 3 Right-click the service path you want to change (if available) by removing its baseline i n the Service Paths section of the Monitor tab.

Step 4 Select **Reset Baseline**.

The baseline of the selected service path is reset.

The following icon appears in the Conforms field of the service path to indicate that the baseline was reset: 

Remove the Baseline of a Service Path

To remove the baseline of a service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select the unicast service that contains the service path you want to change from the hierarchy of unicast services at the left of the Service Manager window. If the service path is not displayed automatically, click the plus (**+**) sign of the unicast service that contains it.

Step 3 Right-click the service path with the baseline you want to remove in the Service Paths section of the Monitor tab.

Step 4 Select **Remove Baseline**.

The baseline of the selected service path is removed.

The following icon appears in the Conforms field of the service path to indicate that the baseline was removed: 

Managing Unicast Services and Service Paths

Once service paths have been created, you can perform the following procedures:

- Remove a Single Unicast Service, page 3-26
- Remove Multiple Unicast Services, page 3-27
- Add Service Paths, page 3-27
- Reconfigure a Service Path, page 3-28
- Remove a Single Service Path, page 3-29
- Remove Multiple Service Paths, page 3-30

Remove a Single Unicast Service

To remove a single unicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 In the menu hierarchy, select the unicast service you want to remove.

Step 3 Click the **Configure** tab.

Step 4 Click **Remove Service** under Service Removal.

A message is displayed asking for confirmation to remove the unicast service.

Step 5 Click **Yes**.

The unicast service and all related service paths are removed.

or, to remove a single unicast service a different way:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select unicast service you want to remove from the hierarchy of unicast services in the left portion of the Service Monitor window.

Step 3 Select the **Monitor** tab.

Step 4 Right-click the name of the unicast service you want to remove in the Monitor tab.

Step 5 Select **Remove Service**.

A message is displayed asking for confirmation to remove the service.

Step 6 Click **Yes**.

The unicast service and all related service paths are removed.

Remove Multiple Unicast Services

To remove multiple unicast services:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Click **Unicast Services** in the menu hierarchy.

Step 3 Click the **Configuration** tab.

Step 4 Click **Remove Service(s)** under Services Removal.

The Services Removal Wizard appears.

Step 5 Select the services you want to remove.

Step 6 Click **Next**, then click **Finish**.

The unicast services and all related service paths are removed.

Add Service Paths

To add service paths to a service:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Click the unicast service you want to add a service path to from the hierarchy of unicast services at the left of the Service Manager window.

Step 3 In the Service Monitor window, select the **Configure** tab.

Step 4 Click **Create Service Paths** in the Service Paths Creation field.

The Service Path Creation wizard appears.

or

Step 1 Use the procedure to Start Service Monitor, page 3-37, and select **Unicast Services** from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the name of the unicast service you want to add a service path to in the Services section of the Monitor tab.

Step 4 Select **Add Service Paths**.

The Service Path Creation wizard appears. For information about completing the wizard, see Configure a Service Path, page 3-11.

Step 5 Complete the wizard to create a single, uni-directional service path.

For information about adding reverse service paths, see Configure a Reverse Service Path, page 3-12.

For information about adding more than one service path, see Add Service Paths to an Existing Unicast Service, page 3-14.

Reconfigure a Service Path

To reconfigure a service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select the service that contains the service path you want to change from the hierarchy of unicast services at the left of the Service Manager window.

If the service path is not displayed automatically, click the plus (**+**) sign of the service that contains it.

Step 3 Select the **Configure** tab in the Service Manager window.

Step 4 Click **Reconfigure Service Path** in the Service Path Configuration panel. The Service Path Reconfiguration wizard appears.

Step 5 Complete the Service Path Reconfiguration Wizard, and change any of the following attributes of the service path:

- In the Source IP Address field, enter the IP address of the service path source.
- In the Gateway Router ID field, enter the IP address of the primary gateway.
- From the Gateway AS or Domain field, select the autonomous system or routing domain of the source.
- In the Destination field, enter the IP address of the destination.

or

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select the unicast service that contains the service path you want to change from the hierarchy of unicast services at the left of the Service Manager window. If the service path is not displayed automatically, click the plus (**+**) sign of the unicast service that contains it.

Step 3 Select the **Monitor** tab.

Step 4 Right-click the name of the service path you want to change in the Service Paths section of the Monitor tab.

Step 5 Select **Reconfigure Service Path**.

The Service Path Reconfiguration Wizard appears.

Step 6 Complete the Service Path Reconfiguration Wizard, and change any of the following attributes of the service path:

- In the Source IP Address field, enter the IP address of the service path source.

- In the Gateway Router ID field, enter the IP address of the primary gateway.
- From the Gateway AS or Domain field, select the autonomous system or routing domain of the source.
- In the Destination field, enter the IP address of the destination.

Note You must change at least one field to reconfigure a service path.

Step 7 Click **Next**.

Step 8 Click **Finish**.

The service path is reconfigured with the new settings.

Remove a Single Service Path

To remove a single service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select the unicast service that contains the service path you want to remove from the hierarchy of unicast services at the left of the Service Manager window. If the service path is not displayed automatically, click the plus (**+**) sign of the service that contains it.

Step 3 Highlight the service path you wish to remove.

Step 4 Select the **Configure** tab in the Service Monitor window.

Step 5 Click **Remove Service Path** in the Service Path Removal section of the tab. A message is displayed asking for confirmation to remove the service path.

Step 6 Click **Yes**.

The service path and its branches are removed.

or

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the **Monitor** tab.

Step 2 Select the unicast service that contains the service path you want to remove from the hierarchy of services at the left of the Service Manager window.

If the service path is not displayed automatically, expand the unicast service that contains it by clicking the plus (**+**) sign.

Step 3 Right-click the service path you want to remove in the Service Paths section of the Monitor tab.

Step 4 Select **Remove Service Path**.

A message is displayed asking for confirmation to remove the service path.

Step 5 Click **Yes**.

The service path and its branches are removed. To remove more than one service path, see Remove Multiple Service Paths, page 3-30.

Remove Multiple Service Paths

To remove multiple service paths:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Click **Unicast Services** in the hierarchy of unicast services at the left of the Service Manager window.

Step 3 Select the **Monitor** tab.

Step 4 Right-click the unicast service name that contains the paths you wish to remove in the Services section of the Monitor tab.

Step 5 Select **Remove Service Paths** (see Figure 3-21).

The Service Paths Removal wizard appears.

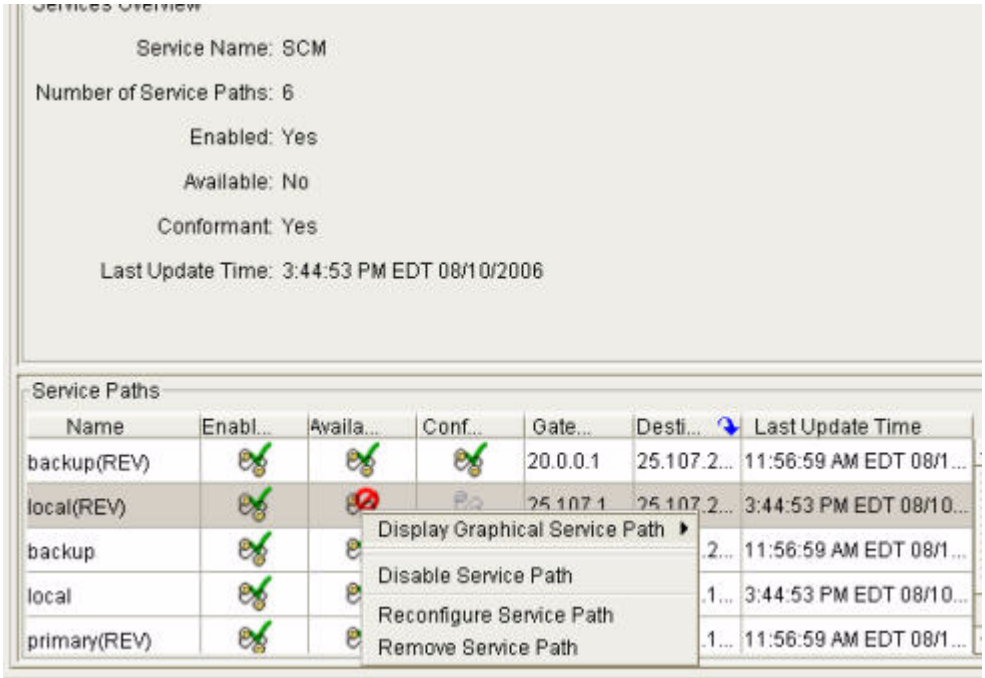
Step 6 From the Remove one or more Service Paths table, select all service paths you want to remove.

Step 7 Click **Next**.

Step 8 Click **Finish**.

All selected service paths are removed from the service. After the service paths are removed, they do not display in the Service Paths section of the Service Monitor window.

Figure 3-21 Pop-up Display for Managing Service Paths



Enabling and Disabling Unicast Services and Service Paths

Enabling a unicast service or service path in Service Monitor allows you to monitor its availability and conformity. In addition, setting alarms on a selected unicast service or service path in Alarm Monitor causes alarms to trigger when changes to the selected service or service path occur. Path Analyzer enables all unicast services and service paths by default when you create them.

You can disable a unicast service or service path—for example, to perform routine maintenance such as removing an intermediate router from your network. You can re-enable it when you completed maintenance activities.

Note After disabling a unicast service or service path, you have to re-enable it to continue monitoring it for availability and conformance. See Enable a Unicast Service, page 3-32 and Enable a Service Path, page 3-32 for information.

Disable a Unicast Service

To disable a unicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select **Unicast Services** in the menu hierarchy.

Step 3 Select the **Monitor** tab.

Step 4 Right-click the name of the unicast service you want to disable in the Service section of the tab.

Step 5 Click **Disable Service**.

The service is disabled, and the **Disabled** icon appears in the Status field of the service.

Disable a Service Path

To disable a service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select the unicast service name in the menu hierarchy that contains the service path you want to disable.

Step 3 Select the **Monitor** tab.

Step 4 Right-click the name of the service path you want to disable in the Service Path section of the tab.

Step 5 Click **Disable Service Path**.

The service path is disabled, and the **Disabled** icon appears in the Status field of the service path.

Enable a Unicast Service

To enable a unicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Unicast Services** in the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the name of the disabled unicast service you want to re-enable in the Service section of the tab.

Step 4 Click **Enable Service**.

The **Enabled** icon appears in the Status field of the unicast service, indicating that the service is enabled. The Availability and Conformity fields are updated immediately to reflect the current state of the system.

Enable a Service Path

To enable a service path:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the unicast service name in the menu hierarchy that contains the service path you want to enable.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the name of the disabled service path you want to re-enable in the Service Path section of the tab.

Step 4 Click **Enable Service Path**.

The **Enabled** icon appears in the Status field of the service path, indicating that the service path is enabled. The Availability and Conformity fields are updated immediately to reflect the current state of the system.

Setting Alarms on Unicast Services and Service Paths

In the Service Alarm Monitor, you can set alarms on unicast services and service paths to receive immediate, automatic notification of service changes, such as a service becoming unavailable or not conforming to a baseline. For more information, see Setting and Monitoring Alarms, page 8-1. When a unicast service or service path with an alarm is removed, the alarm is purged as well.

You can also export service alarms to a syslog host or an SNMP agent for notification through your network management system (NMS). For information, see Chapter 8, Exporting Alarm Triggers, in the *Cisco Service Path Analyzer System Administrator Guide*.

Replaying Historical Services

For information about replaying the changes to historical services and service paths, see Start a Module in a Historical Session, page 13-11 and Find Information about Historical Service Paths, page 13-13.

Related Forms

Details of a Unicast Service

From the Service details area of the Monitor tab, you can view unicast service details.

Table 3-2 describes unicast service details.

Table 3-2 Details of a Unicast Service

Field	Description
Service Details	Shows the following details of a unicast service: • Service Name • Enabled or Disabled • Available or Unavailable • Conformant or Non-Conformant • Last Update Time
Unicast Service Name	Identifies the name of the unicast service.
Enabled	Identifies if the unicast service is enabled or disabled.
Available	Identifies if the unicast service is available or unavailable.
Conformant	Identifies if the unicast service is conformant or deviant.
Last Update Time	Identifies the unicast service's last update time.

Details of a Unicast Service Path

From the Service Path details area of the Monitor tab, you can view service path details.

Table 3-3 describes the Service Path details.

Table 3-3 Details of a Unicast Service Path

Field	Description
Service Path Details	Shows the following details of service paths: • Service Path Name • Source IP Address • Gateway Shows • Gateway AS or Domain • Destination/IP Address • Enabled or Disabled • Available or Unavailable • Conformant or Non-Conformant • Path Loop • Last Update Time
Service Path Name	Identifies the name of a service path.
Source IP Address	Identifies the IP address of the service path source.
Gateway Shows	Identifies the gateway router.
Gateway AS or Domain	Identifies the autonomous system or routing domain in which the source is located.
Destination IP Address	Identifies the IP address of the destination router.
Enabled	Identifies if the service path is enabled or disabled.
Available	Identifies if the service path is available or unavailable.
Conformant	Identifies if the service path is conformant or deviant.
Path Loop	Identifies if a service path has a path loop.
Last Update Time	Identifies the service path's last update time.

Details of Service Path Branches Dialog Box

From the Service Path details area of the Monitor tab, you can view details of service path branches.

Table 3-4 describes the Details of Service Path Branches dialog box.

Table 3-4 Details of Service Path Branches

Field	Description
Service Path Branch	Provides detailed information about the nodes and links that a given path traverses through a network.
AS Sequence	Provides the ordered list of autonomous systems through which a path traverses through a network. It provides multiple ways which a path travels from a gateway to its destination.

Table 3-4 Details of Service Path Branches

Field	Description
AS	Provides the ordered listing of autonomous systems for the AS Sequence. It provides the starting point within an AS and ending point within an AS. It is the unique set of entry and exit points for an ordered AS.
Subbranch	Given two endpoints, it represents the unique traversal set of nodes and links.
Hop Number	Identifies each hop, each step from node-to-node, that the path makes from source to destination.
Hop Node	Shows the IP address or prefix of each hop between the source and destination.
Hop Area	Shows the area in which each hop resides.
Hop Interface	Shows the IP address of the router interface that the path traverses from source to destination.
The following fields are available for each selected hop. Expanding the router by clicking the plus sign (**+**) next to its entry causes the following fields to be displayed.	
Node Type	Provides some type of router or network.
Link Type	Provides some type of interface or router link.
Primary Route	Provides the information needed to determine why the service path made its routing decision (only on routers).
Secondary Route	Provides the information needed to determine why the service path made its routing decision (only on routers).
Destination Type	Shows the type of destination, for example, network or route outside the scope of Path Analyzer.

Monitoring Multicast Services

Multicast services have multiple subscribers who receive multicast information such as video or information services. Multicast services are supported by multicast routing, which enables the service to be automatically distributed to designated users or subscribers.

In multicast routing, the source sends data to a group of hosts represented by a multicast group address.This data is carried between endpoints across one or multiple Autonomous Systems (AS's) and routing domains.

The multicast router must determine which direction is upstream (toward the source) and what direction is downstream (toward the destinations). If there are multiple downstream paths, the router duplicates the packet and forwards the traffic down the right downstream paths. *Reverse path forwarding* (RPF) refers to the algorithm that each router employs to choose its upstream neighbor, based on its best unicast path to the source.

Path Analyzer delivers *static* multicast services, meaning the service branches, gateways, sources and destinations are defined when the service is created. When you create a new multicast service in Path Analyzer, you must define:

- Service redundancy type
- Domain

- Source router
- Gateway
- Destination router

Branches of a Multicast Service

When the flow of data in a multicast service splits for distribution to a leaf router, the service tree divides into branches that carry data toward the destination. Each branch represents one unique route from the Source Specific Multicasting (SSM) multicast service group to the leaf router or destination.

The Multicast Branches section of Service Monitor lists the branches of an SSM multicast service group, to help you track the cause of service-related issues. For example, a change in the branch count may indicate that an interface metric has changed, causing service data to be re-routed over an unintended path, thus interrupting load balancing.

Reverse path forwarding enables routers to forward multicast traffic down the distribution tree, using the existing routing table, in order to determine the upstream and downstream hops. A router forwards a multicast packet only if it is received on the upstream interface.

Visual, Real-time Traceroute on Multiple, Simultaneous Flows

In the Service Monitor, creating multicast services and SSM multicast service groups allows you to monitor where information travels, ensuring that multicast services are continuously available and received by those who need them.

Having an up-to-date picture of service deployment allows you to act on potential failures faster, with a clearer understanding of the location and cause of problems. For information about creating multicast services in Service Monitor, see Creating Multicast Services and Related SSM Multicast Service Groups, page 3-43.

Note Viewing the transmission of an SSM multicast service group and branches across your network is similar to having a visual, real-time display of the type of data you receive when you run the `traceroute` command. Viewing a multicast service in transit is equivalent to receiving a visual display of the results of multiple, simultaneous `traceroute` commands run on all SSM multicast service groups that make up a multicast service.

In addition to monitoring services from Service Monitor, you can select and view a multicast service and its corresponding SSM multicast service groups and branches in the Service Viewer. In the Service Viewer, you can also view the status of the routers and links across which service data traverses between endpoints. For information about using the Service Viewer, see Viewing Services in the Service Viewer on page 2-45.

Real-time and Historical Views of Multicast Services

You can view multicast services and SSM multicast service groups in two modes:

- **Real-time**—Presents the current and dynamic display of multicast services, SSM multicast service groups and branches across the multiple autonomous systems and routing domains of your network.

- **Historical**—Returns your network to a previous state, enabling you to review past conditions affecting multicast services, SSM multicast service groups and branches. For information about starting the Service Monitor while running a past sequence of events, see Start a Module in a Historical Session, page 13-11.

Service Monitor Tasks

- Starting Service Monitor, page 3-37
- Monitoring the Flow of Business Critical Data, page 3-38
- Creating Multicast Services and Related SSM Multicast Service Groups, page 3-43
- Interpreting Service Data on a Multicast Service, page 3-48
- View the List of Multicast Services and Related Distribution Trees, page 3-50
- Viewing Multicast Services Graphically, page 3-53
- Viewing the Root Cause of Multicast Services Issues, page 3-61
- Viewing Details of Multicast Services and SSM Multicast Service Groups, page 3-62
- Managing Baselines of Multicast Service and SSM Multicast Service Groups, page 3-63
- Managing Multicast Services and SSM Multicast Service Groups, page 3-64
- Reconfigure a SSM Multicast Service Group, page 3-68
- Enabling and Disabling Multicast Services and SSM Multicast Service Groups, page 3-70
- Setting Alarms on Multicast Services and SSM Multicast Service Groups, page 3-71
- Replaying Historical Services, page 3-72

Starting Service Monitor

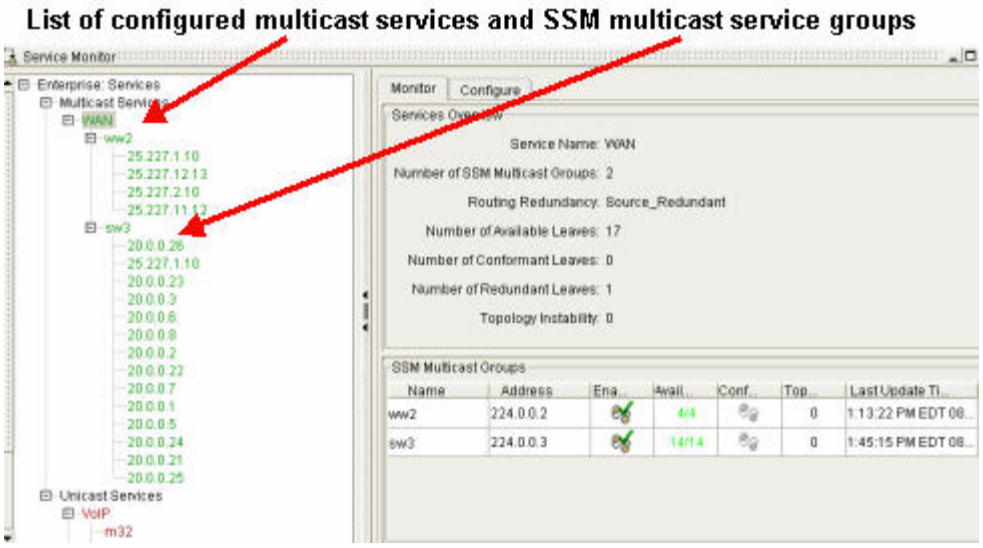
To configure multicast service paths and groups, you must first start Service Monitor.

Start Service Monitor

To start Service Monitor, from the Path Analyzer taskbar click **Start > Service Monitor**.

The Service Monitor opens in the Path Analyzer Management Console (see Figure 3-22).

Figure 3-22 Service Monitor in Path Analyzer



Monitoring the Flow of Business Critical Data

Your success depends upon your ability to maintain the applications and multicast services you provide to your customers. Path Analyzer monitors the endpoints and flow of your multicast services across routing domains and presents related information.

How Data is Displayed in Service Monitor

In Service Monitor, you create abstract, visual representations of multicast services—the multiple connections and devices that generate, transmit, and deliver data to your end users.

Figure 3-23 A Multicast Service Displayed in the Service Viewer and Service Monitor

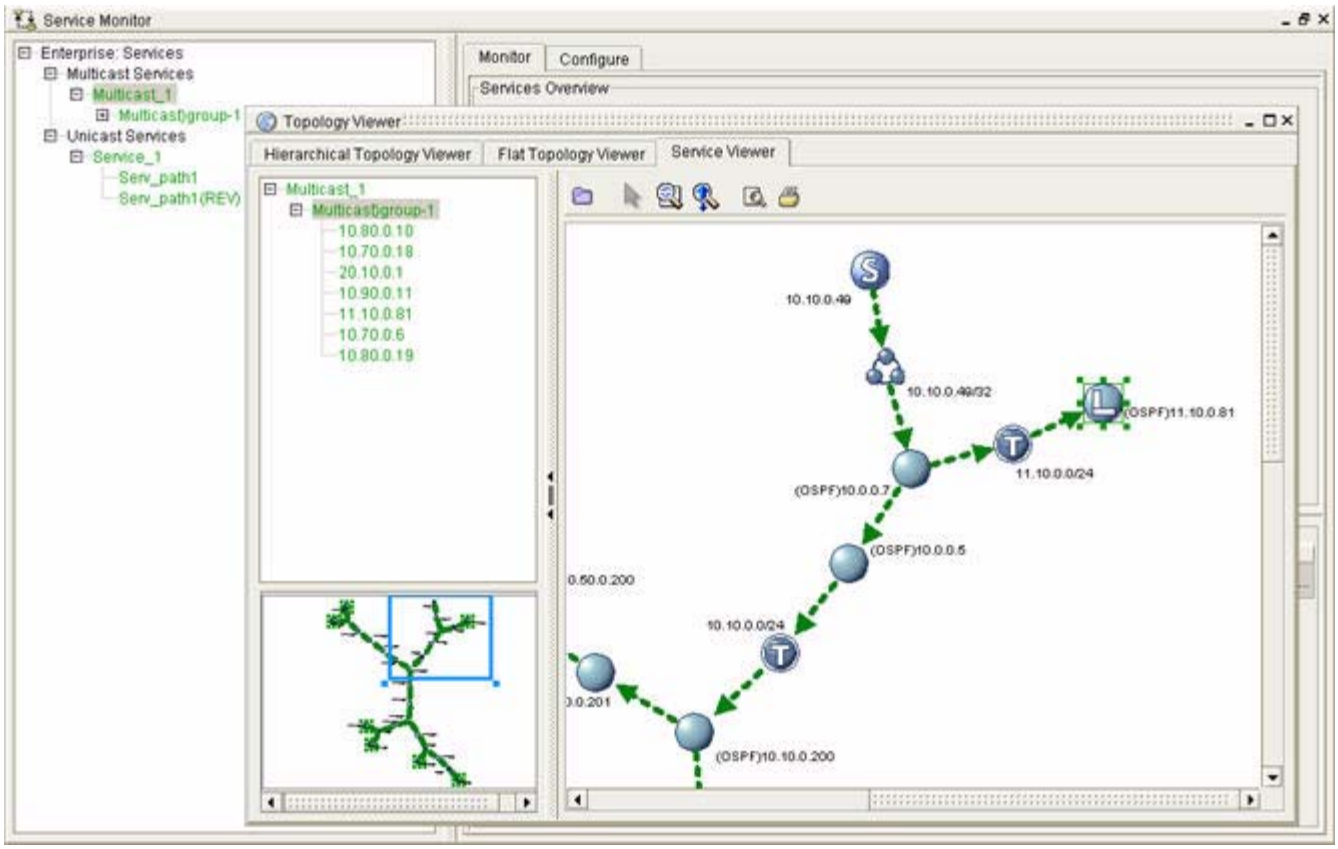


Figure 3-23 illustrates how a multicast service can be displayed using the Topology Viewer feature in Path Analyzer. Notice that the service is also listed hierarchically on the left side of the screen.

- **S** = Source
- **T** = Transit network
- **L** = Leaf router

SSM Multicast Service Groups: Multicast Distribution Trees

A multicast service uses a *Multicast Distribution Tree* to transport data from the source to the leaf routers. The Multicast Distribution Tree consists of:

- **Source**—the root of the Multicast Distribution Tree.
- **Primary Gateway—**the first router that receives service data from a host and passes it one hop toward the destination.
- **Destination**—the router that forwards the data to the destination host where the data is used.
- **Leaf routers**—which hang off the destination router and retrieve data for their designated SSM multicast group.

The availability and integrity of all these connections is vital to your business.

Figure 3-24 Unavailable Multicast Service

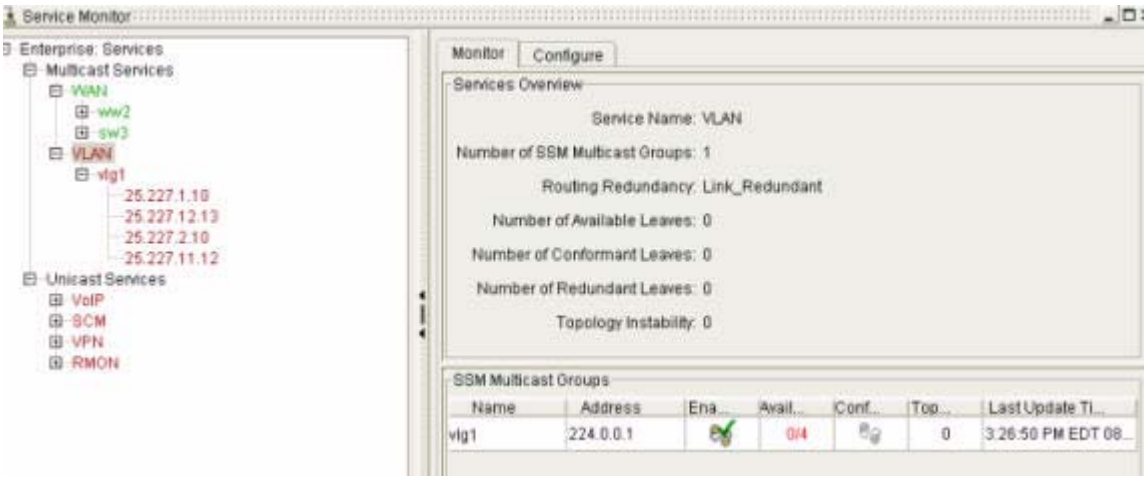


Figure 3-24 shows an unavailable multicast service in Service monitor.

Figure 3-25 Available Multicast Service

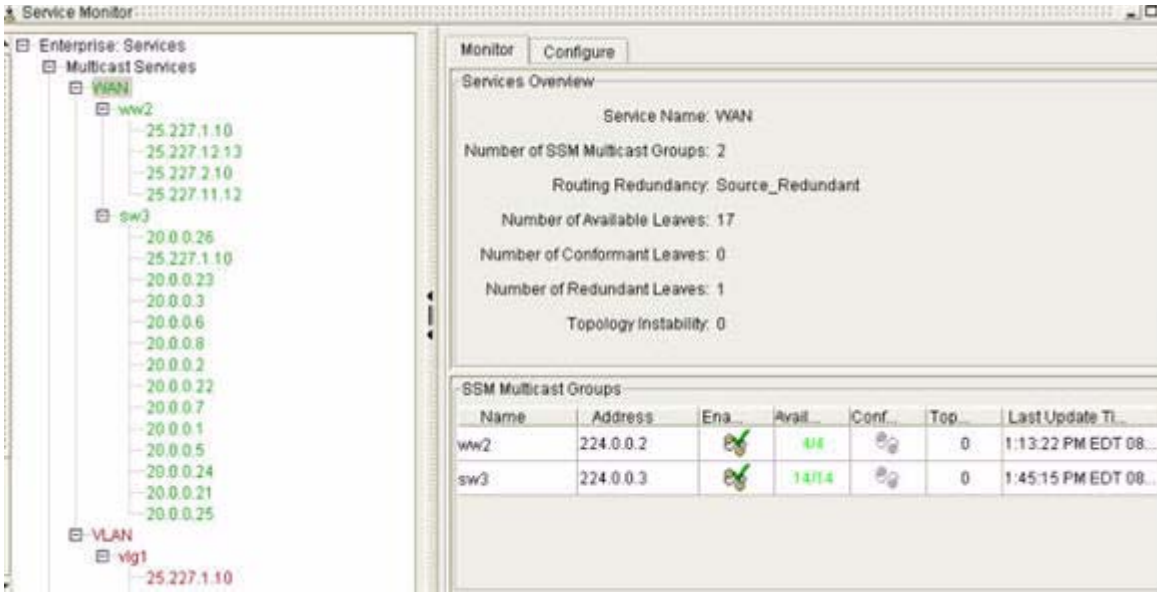
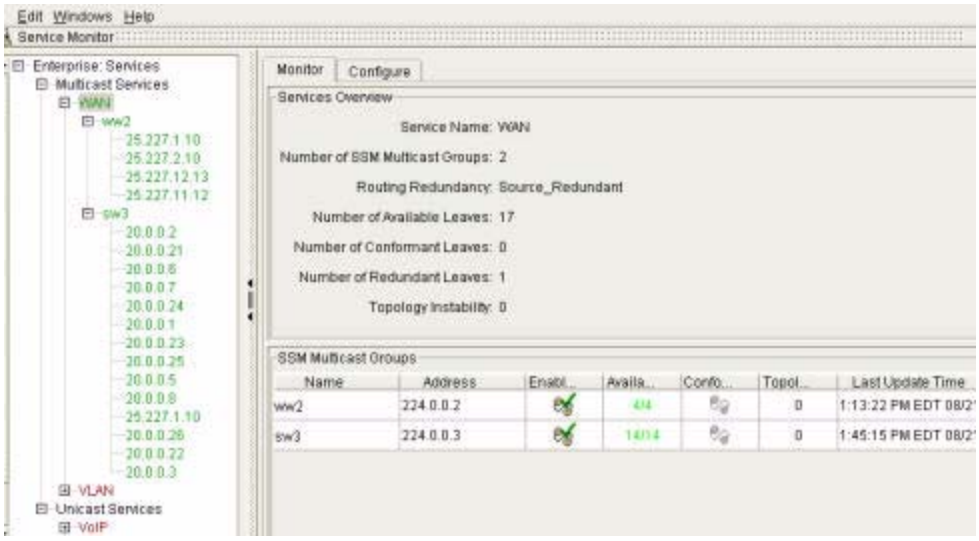


Figure 3-25 shows an available multicast service in Service monitor.

Viewing SSM Multicast Service Groups

Clicking a multicast service causes its related SSM multicast service groups to be displayed in the SSM Multicast Service Group section of the Service Monitor window (see Figure 3-26).

Figure 3-26 SSM Multicast Service Groups of a Selected Multicast Service



In Service Monitor, multicast services and related SSM multicast service groups are displayed with icons and text that indicate:

- Enabled or Disabled status
- Availability on the network
- Conformity to the path engineered for data between a source and destination
- Time stamp of the most recent updates
- Gateway and destination of the SSM multicast service group

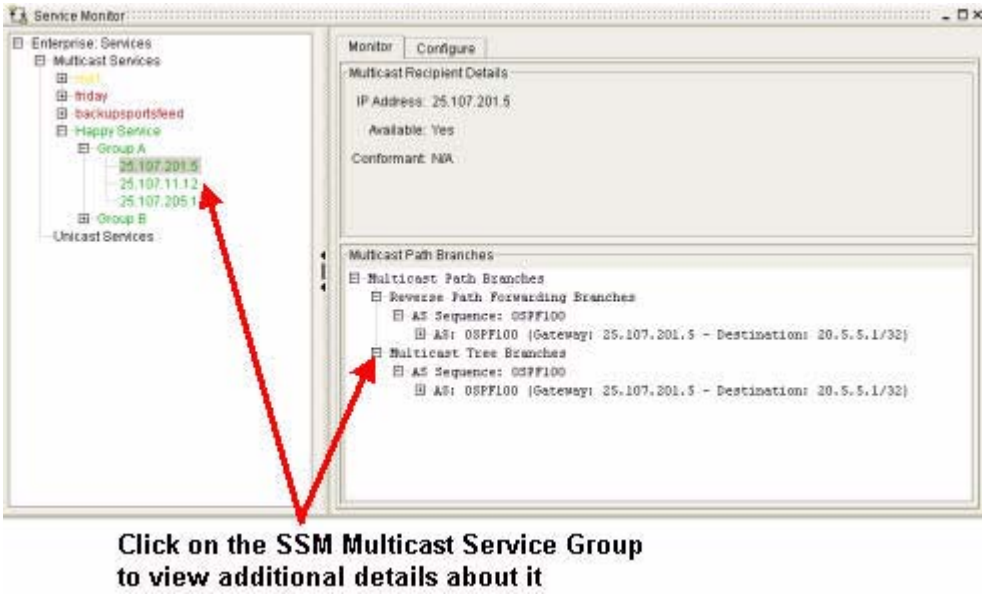
Viewing Details of Multicast Services and SSM Multicast Service Groups

After creating a multicast service and its related SSM multicast service groups in Service Monitor, you can:

- monitor the exact set of routers and interfaces that the multicast service relies on to deliver application traffic.
- identify when, where, and which multicast services are affected, in what way, and why.

For information, see Interpreting Service Data on a Multicast Service, page 3-48 and Figure 3-27.

Figure 3-27 Multicast Services and SSM Multicast Groups in Service Monitor

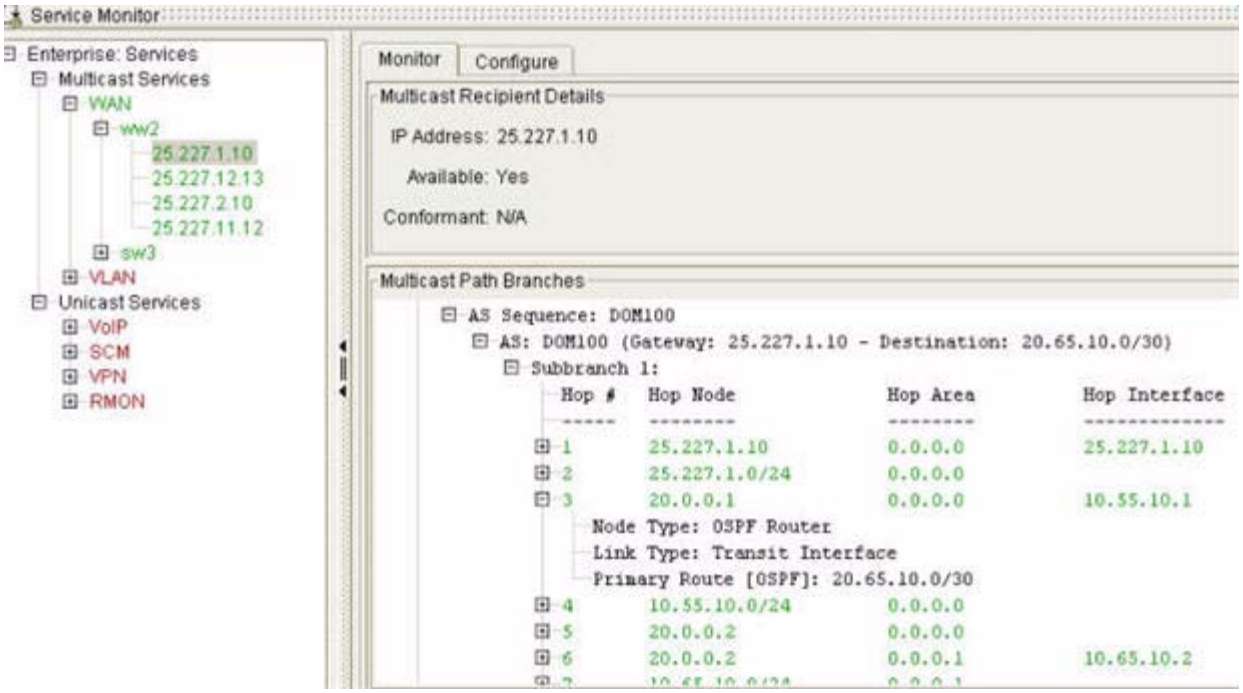


The source sends traffic to an SSM multicast group address, which represents a group of hosts. The multicast router must determine which direction to send data—upstream (toward the source) or downstream (toward the destination). If there are multiple downstream branches, the router replicates the packet and forwards it to the proper downstream branch.

Reverse Path Forwarding refers to forwarding traffic away from the source, instead of toward the receiver. Leaf routers tell the destination router or the source router they are interested in specific traffic. The routers go up the path looking for a leaf router in the tree that also subscribes to that service. If found, the leaf routers join the other leaf routers that already subscribe to the service as part of the corresponding multicast distribution tree. If the leaf routers cannot find another leaf router for the subscribed service, Path Analyzer creates another branch for the data to travel. This branch is built from the destination to the source router. The system designs a tree that connects the SSM multicast service group to the source.

Figure 3-28 shows hops to destination data in Service Monitor.

Figure 3-28 Hops to Destination in Service Monitor



Creating Multicast Services and Related SSM Multicast Service Groups

Use the Multicast Group Service Group Wizard to create multicast services and SSM multicast service groups. This enables Path Analyzer to monitor the routing patterns of multicast services within your network.

Required Information for Creating a Multicast Service or SSM Multicast Service Group

When you create a multicast service in the wizard, you must provide the following information for each multicast service and SSM multicast service group:

- Name that uniquely identifies the multicast service, or one that identifies the SSM multicast service group
- Redundancy type:
  - Not Redundant
  - Source Redundant
  - Link Redundant
- Router IDs for the multicast service or SSM multicast service groups:
  - Source Host IP address or Router ID
  - Recipient AS or Domain

- First Hop
- Available Recipients and Selected Recipients
- Address of Leaf Routers

Once these addresses are available for a SSM multicast group, Path Analyzer computes the Multicast Distribution Tree and monitors for any routing changes that will cause the tree to change. When Path Analyzer detects a change to the tree, it reports the change, identifying the root cause and the leaf routers affected.

Note Leaf routers use Internet Control Message Protocol (ICMP) to tell the source or another leaf router that they are interested in obtaining the service.

Start the SSM Multicast Group Creation Wizard

To start the SSM multicast group creation wizard:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

The Service Monitor window appears.

Step 2 Select **Multicast Services** from the menu hierarchy.

Step 3 Select the **Configuration** tab.

Step 4 Click **Create Service** in the Multicast Service Creation field.

Step 5 (Optional) Click the **Do not show this screen again** check box.

Step 6 In the initial wizard page, click **Next**.

The Create a Multicast Service screen appears (see Figure 3-29).

Figure 3-29 Configure a Multicast Service Screen in Service Creation Wizard

Provide a Name for the Multicast Service

To name the multicast service:

Step 1 Enter the name of the new multicast service in the Enter a Unique Service Name field.

Select a name that indicates the type of application, network service, location, or department that uses the service.

Examples:

- SecurityVirusScanner
- ERP_EastCoast
- Order Processing System

Step 2 Choose the Redundancy Type:

- **Not Redundant**
- **Source Redundant**
- **Link Redundant**

Step 3 By default, the **Check to Configure Multicast Service Group for your Multicast Service** box is selected.

a. Keep the default selection to configure a multicast service group for the service.

b. Click **Next** to continue to Configure an SSM Multicast Service Group, page 3-45.

or

a. Click the check box to deselect the option to configure a multicast service group.

b. Click **Finish**.

The new service is listed in the Services hierarchy at the left of the Service Monitor window. You can , page 3-48 at a later date.

Configure an SSM Multicast Service Group

To configure a multicast service group:

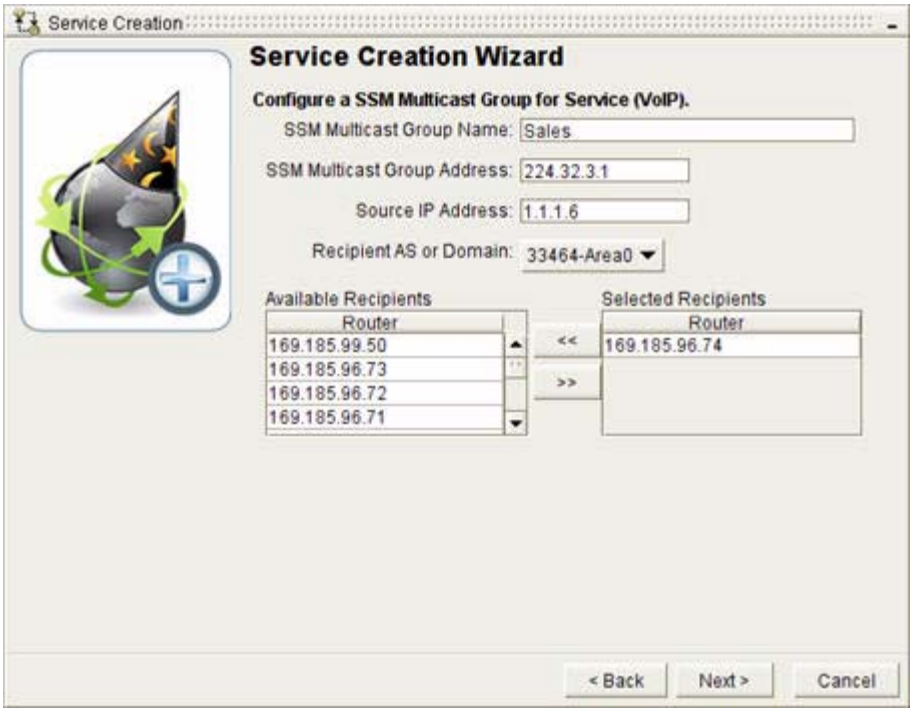
Step 1 Enter a name for the new SSM multicast service group in the Multicast Group Name field (see Figure 3-30).

Select a name that indicates the type of application, network service, location, or department that relies heavily on the SSM multicast service group or a number representing the multicast service.

Examples:

- **AcctPayable_CA-Office**
- **ERP_+NYCAdminGroup**
- **Order Processing Midwest_Distribution**

Figure 3-30 Configure a SSM Multicast Group for Service Screen in Service Creation Wizard



Step 2 Enter the IP address of the router that is the first hop from the source toward the destination (a value between 224.0.0.0 and 239.255.255.255) in the Multicast Group Address field.

Step 3 Enter the IP address of the source for the SSM multicast group source on the network in the Source IP Address field.

Step 4 Select the autonomous system (AS) or Open Shortest Path First (OSPF) routing domain in which the source of multicast group service resides in the Recipient AS or Domain field.

A list of available routers appears in the Available Recipients box.

Step 5 Select the router(s) you want to receive data by highlighting it in the box and clicking the bottom arrow to move it into the Selected Recipients box.

Step 6 Click **Next**.

A screen appears confirming that the SSM Multicast Service Group is added to your new multicast service (see Figure 3-31).

Figure 3-31 SSM Multicast Group(s) Added Screen in Service Creation Wizard

Step 7 The Check to Configure Additional SSM Multicast Service Groups field is automatically enabled. A check mark is displayed in the check box to indicate that the option is selected.

a. Keep the default selection and click **Next**.

The SSM Multicast Service Group is created, and the Configure a SSM Multicast Service Group Wizard screen appears, in which you can create another multicast service group.

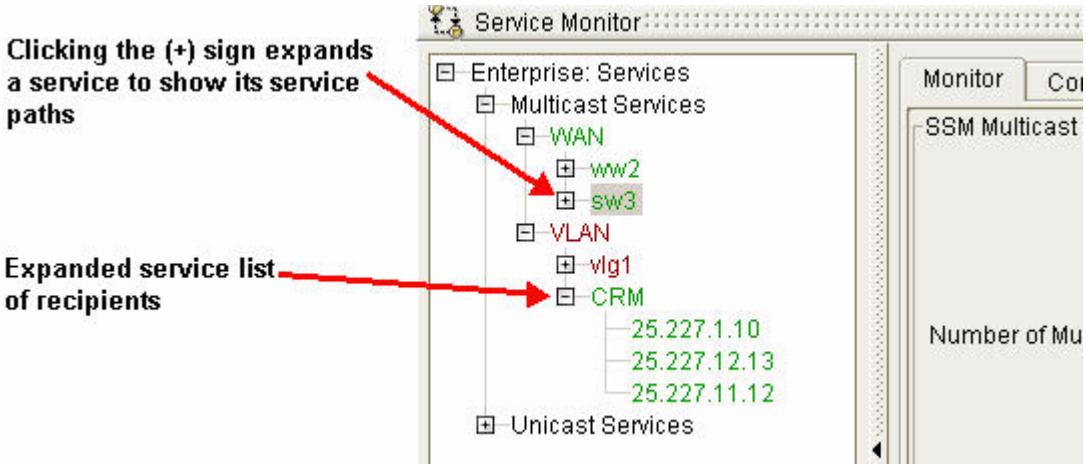
or

a. Click the **Check to Configure Additional Multicast Service Groups** check box to deselect the option.

b. Click **Finish**.

- After creating a multicast service, the multicast service is listed in the Service Monitor window, in the Services hierarchy of the enterprise.
- All SSM multicast service groups related to a multicast service are listed under the service to which they belong. To expand a multicast service and view its related SSM multicast service groups, click the plus sign (**+**) (see Figure 3-32).

Figure 3-32 Multicast Services Listed in Services Menu Hierarchy



Add Groups to an Existing Multicast Service

To add service groups to an existing SSM multicast service:

Step 1 Select the multicast service you want to add a SSM multicast service group to from the Services hierarchy.

Step 2 Select the **Configure** tab in the Service Monitor window.

Step 3 Click **Create SSM Multicast Group(s)**.

The Multicast Group Creation Wizard appears.

Step 4 Follow the steps for Configure an SSM Multicast Service Group, page 3-45.

Interpreting Service Data on a Multicast Service

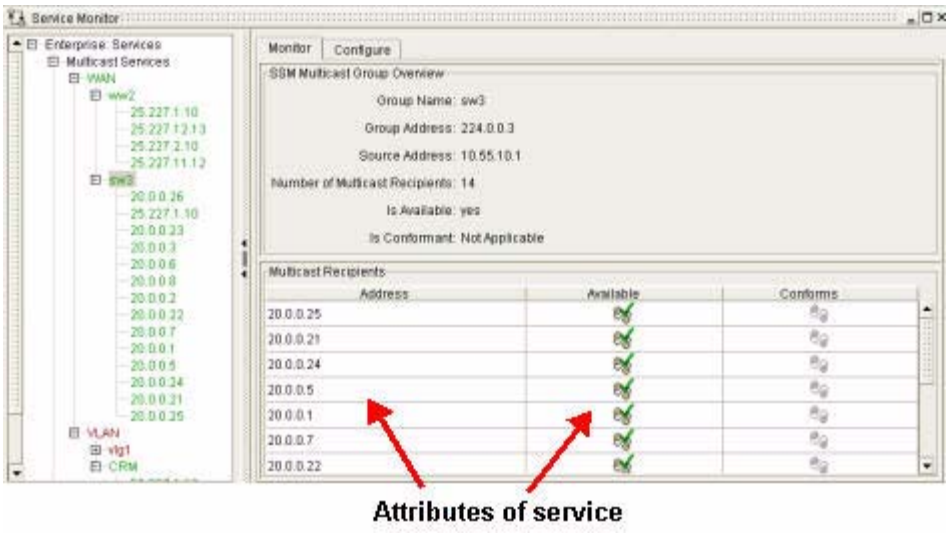
In the Enterprise Services tree, multicast services and SSM multicast service groups are listed hierarchically.

- Green multicast services and SSM multicast service groups are available on the network and conform to a baseline, which is the path you configured for data to take across the network.
- Red multicast services and multicast service groups are unavailable.
- Yellow multicast services and SSM multicast service groups deviate from the baseline you defined.
- Gray multicast services and multicast service groups are disabled.

Clicking the plus sign (**+**) in front of the Enterprise Services field in the network hierarchy causes information about a multicast service to be displayed in the Services section of the Monitor tab.

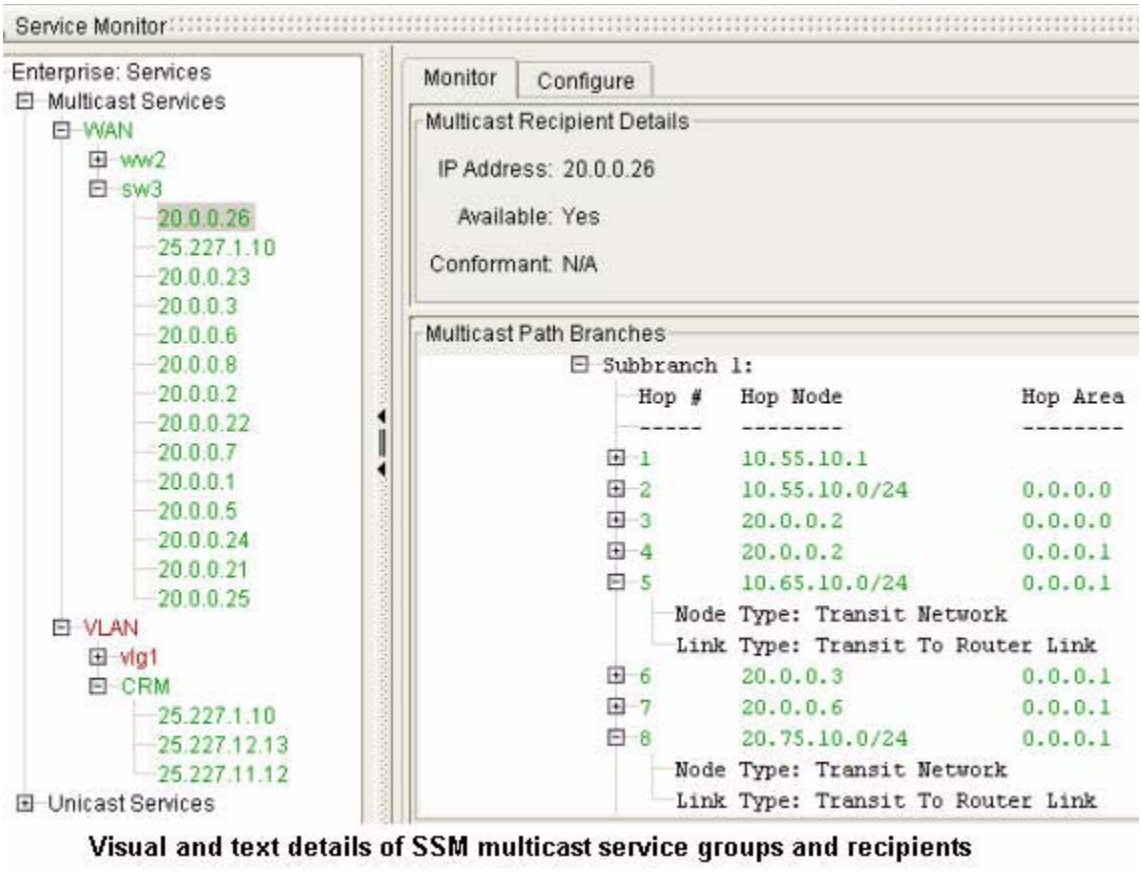
Clicking a multicast service causes information about its related SSM multicast service groups to be displayed in the Service Group section.

Figure 3-33 Service Data in Service Monitor



Selecting a multicast service from the hierarchy reveals its details in the **Monitor** tab (see Figure 3-33).

Figure 3-34 Details of a Multicast Service



Selecting an SSM multicast service group from the hierarchy also results in the details displaying in the Monitor tab (see Figure 3-34).

View the List of Multicast Services and Related Distribution Trees

The multicast services are listed in the Service Tree on the left side of the Service Monitor (see Figure 3-35).

Figure 3-35 Configuration Settings for an SSM Multicast Service Branch

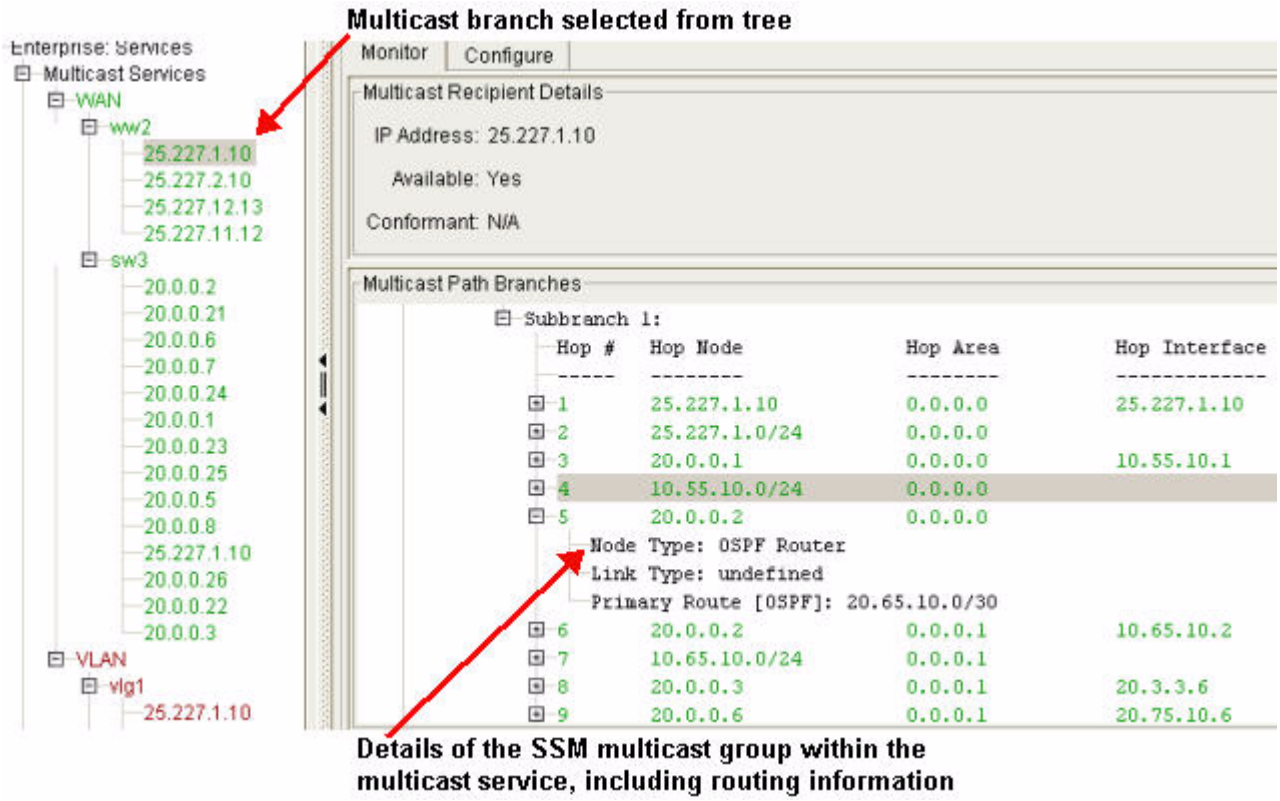


Table 3-5 explains the icons and terminology used to indicate the status of multicast services and SSM multicast service groups.

Table 3-5 Indicators of Status, Availability, and Conformity in Service Monitor

Icon for Entity	Displayed in Service Monitor Field	Description
Services		
	Enabled	Indicates that the multicast service is enabled and actively monitored in Service Monitor. A multicast service is enabled if any SSM multicast service groups are enabled. See Enabling and Disabling Multicast Services and SSM Multicast Service Groups, page 3-70 for detailed information about enabling and disabling services and related SSM multicast service groups.
	Available	Indicates that at least one segment exists for all service paths, allowing them to forward packets between the gateway and the destination. The multicast service is available on the network.
	Conforms	Indicates that all SSM multicast service groups of the service follow the set path of transmission that you established when you created the service (the baseline). Each SSM multicast service group has its own set baseline. See Viewing Multicast Services Graphically, page 3-53 for information about using the maps of the Topology Viewer to analyze the conformance of a multicast service.
	Enable	Indicates that the service is disabled in Service Monitor. The multicast service cannot be monitored until it is re-enabled on the network. All SSM multicast service groups are disabled if a multicast service is disabled.
	Available	Indicates that at least one of the SSM multicast service groups that make up the multicast service has become unavailable on the network.
	Conforms	Indicates that at least one SSM multicast service group of the multicast service does not conform to its set baseline. See Viewing the Root Cause of Multicast Services Issues, page 3-61 for information.
	Enable	Indicates that a multicast service has no SSM multicast service groups.

Table 3-5 Indicators of Status, Availability, and Conformity in Service Monitor

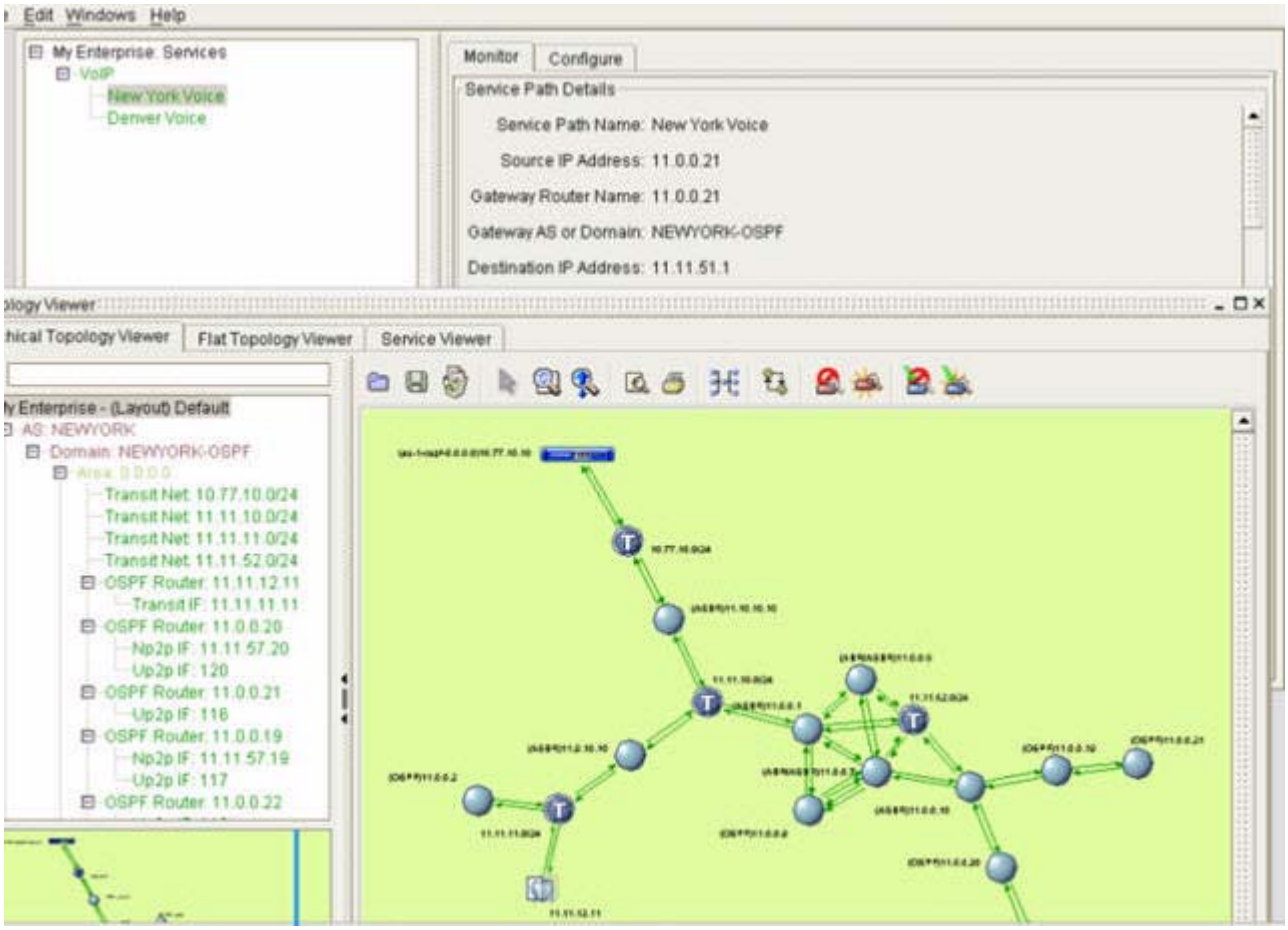
Icon for Entity	Displayed in Service Monitor Field	Description
	Available	Indicates that all related branches are disabled or that no SSM multicast service groups exist for a multicast service.
	Conforms	Indicates that baselines have not been established for any SSM multicast service of a multicast service. It can also indicate that there is no SSM multicast service or that all SSM multicast services are disabled.
Service Groups		
	Enable	Indicates that the SSM multicast service group is enabled and actively monitored.
	Available	Indicates that at least one branch of a SSM multicast service allows packet forwarding between the gateway and the destination. The SSM multicast service is available on the network.
	Conforms	Indicates that the service group conforms to its set baseline. See Display Graphical Multicast Tree, page 3-59 for information about using the maps of the Topology Viewer to analyze the conformance of an SSM multicast service group.
	Enable	Indicates that the SSM multicast service group is disabled. Monitoring is interrupted.
	Available	Indicates that all branches of an SSM multicast service group have become unavailable, interrupting packet forwarding between the gateway and the destination.
	Conforms	Indicates that the SSM multicast service group does not conform to its baseline.
	Conforms	Indicates that a baseline has not been established for the SSM multicast service group. An SSM multicast service group does not have a baseline if one or more intermediate routers or networks are unavailable when you create the SSM multicast service group, or if you remove it.

Viewing Multicast Services Graphically

You can view a multicast service or SSM multicast service group in the Flat Topology Viewer or the Hierarchical Topology Viewer. You can also use the Service Viewer to see a graphical representation of the entire multicast service and each of SSM multicast service groups and their branches— the direction over which data travels across the network between endpoints. The depiction of data branches in the Topology Viewer correlates with the Service Monitor icons that indicate the status, availability, and conformity of the multicast service and its SSM multicast service groups (see Figure 3-36).

For information about Service Monitor icons, see Interpreting Service Data on a Multicast Service, page 3-48.

Figure 3-36 Display of Multicast Service



The Flat Topology Viewer, Hierarchical Topology Viewer, and Service Viewer use the following colors to indicate service status, corresponding to the Enabled, Available, and Conforms status displayed in Service Monitor:

Table 3-6 Meaning of Multicast Service and SSM Multicast Service Group Colors

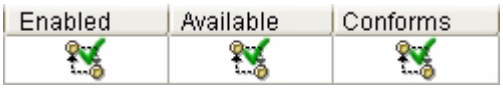
Color	Description
Green	Service and all of its SSM multicast service groups and branches are available on the network and conform to configured baselines. Example:  In the Monitor tab, the following icons are displayed for the corresponding multicast service, SSM multicast service group and all of its branches: 

Table 3-6 Meaning of Multicast Service and SSM Multicast Service Group Colors

Color	Description
Red	A multicast service is unavailable because at least one of its SSM multicast service group is unavailable. In the following example, the service group branch from a router in an external network is unavailable, possibly due to a hardware issue, flap on the router interface, or unavailability of the external network. Example:  In the Monitor tab, the following icons are displayed for the multicast service and at least one of its SSM multicast service groups: 

Table 3-6 Meaning of Multicast Service and SSM Multicast Service Group Colors

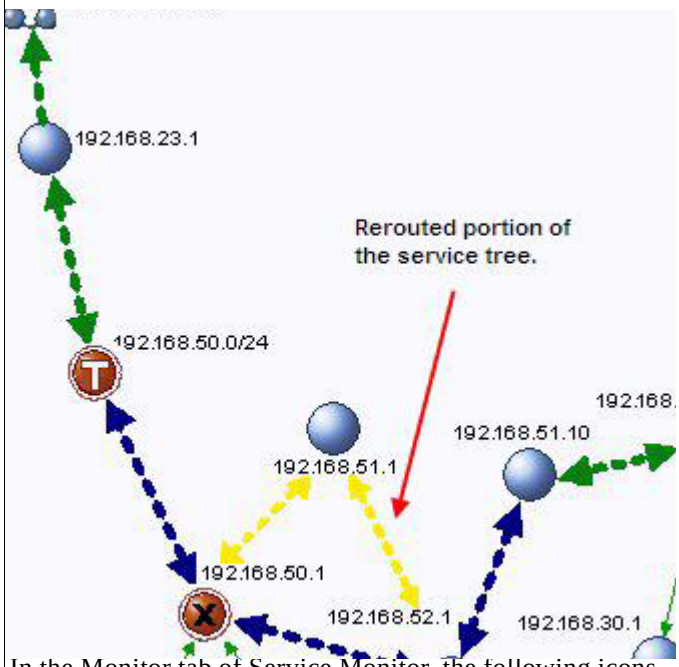
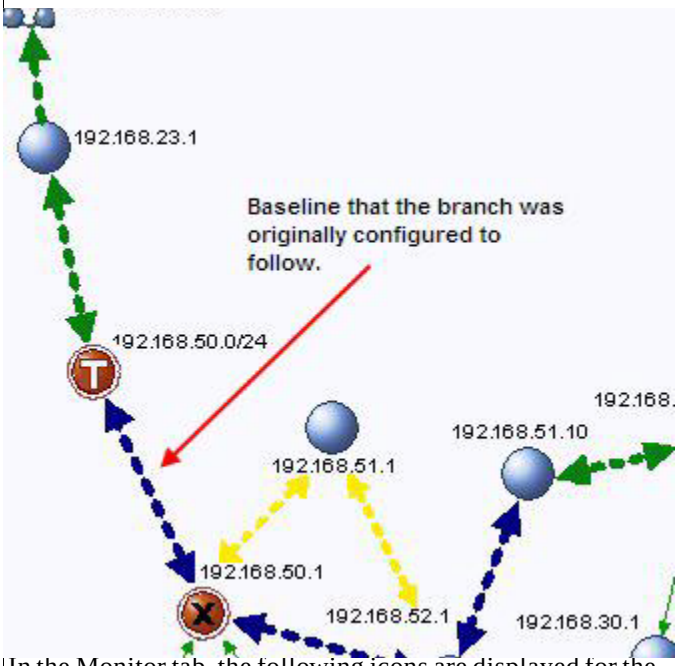
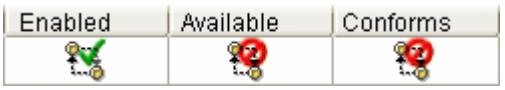
Color	Description
Yellow	Multicast service is available. However, at least one of the branches in the SSM multicast service group does not conform to its baseline. Where the SSM multicast service group is re-routed and follows a different branch, it is displayed as a yellow line in the Topology Viewer. Example:  In the Monitor tab of Service Monitor, the following icons are displayed for the service and the non-conformant service group:  An SSM multicast service in which at least one service group does not have a configured baseline also is displayed as a green line in the Topology Viewer.
	In the Monitor tab of Service Monitor, the following icons are displayed for the multicast service: 

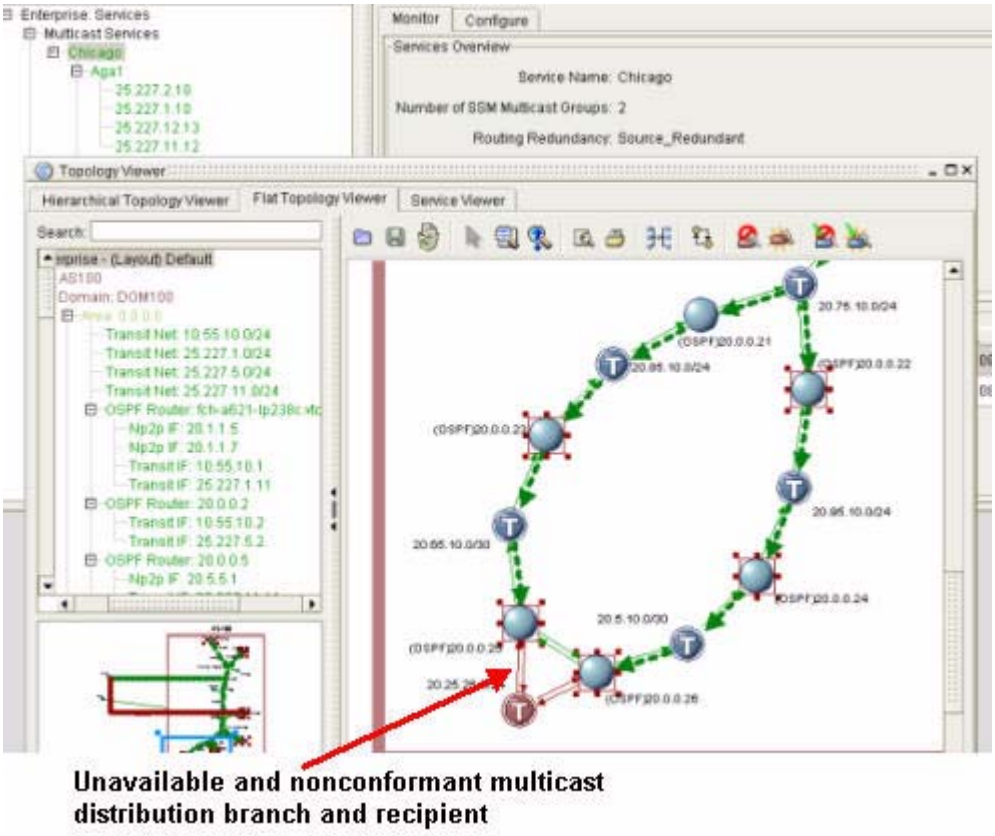
Table 3-6 Meaning of Multicast Service and SSM Multicast Service Group Colors

Color	Description
	and for its non-conformant SSM multicast service group: 
Blue	A multicast service is available to all recipients when all of its tree branches are available. However, in this example at least one branch does not conform to its baseline. The configured baseline is displayed as a blue line, indicating the direction that the non-conformant SSM multicast service branch is intended to follow although it traverses a different route. Example:  In the Monitor tab, the following icons are displayed for the multicast service and the non-conformant branch: 

- Figure 3-37 shows the data flow of an unavailable and non-conforming multicast service, shown graphically in the Topology Viewer. In Service Monitor, a multicast service is not available or conformant to all recipients because one of its distribution tree branches is unavailable.

- The graphic also shows a second set of icons you can display in the Topology Viewer and in individual element connections. For information about setting the display of icons and connections, see Select Topology Viewer Settings, page 1-25.

Figure 3-37 Graphical Service Path Showing an Unavailable Service



Both Service Monitor and the Topology Viewer can indicate when a multicast service becomes unavailable or deviates from its configured baseline.

For detailed information about how to interpret the visual display of multicast services and SSM multicast service groups in the maps of the Topology Viewer and Service Monitor, see Interpreting Service Data on a Multicast Service, page 3-48.

Display Graphical Multicast Service

To display a graphical multicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37, and select **Multicast Services** from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the name of the multicast service you want to map in the Services section of the tab.

Step 4 Select **Display Graphical Multicast Tree** and then select one of the following options:

- **Display Graphical Service in Flat Viewer—**Opens the Topology Viewer and presents the multicast service in the Flat Topology Viewer.
- **Display Graphical Service in Hierarchical Viewer—**Opens the Topology Viewer and presents the multicast service in the Hierarchical Topology Viewer.
- **Display Graphical Service in Service Viewer**—Opens the Topology Viewer and presents the multicast service in the Service Viewer.

The selected tab opens in the Topology Viewer showing the flow of service-related data, represented by dashed green arrows.

Display Graphical Multicast Tree

To display a graphical multicast tree:

Step 1 Use the procedure to Start Service Monitor, page 3-37, and select the name of a multicast service from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the name of the multicast service you want to map in the Services section of the tab.

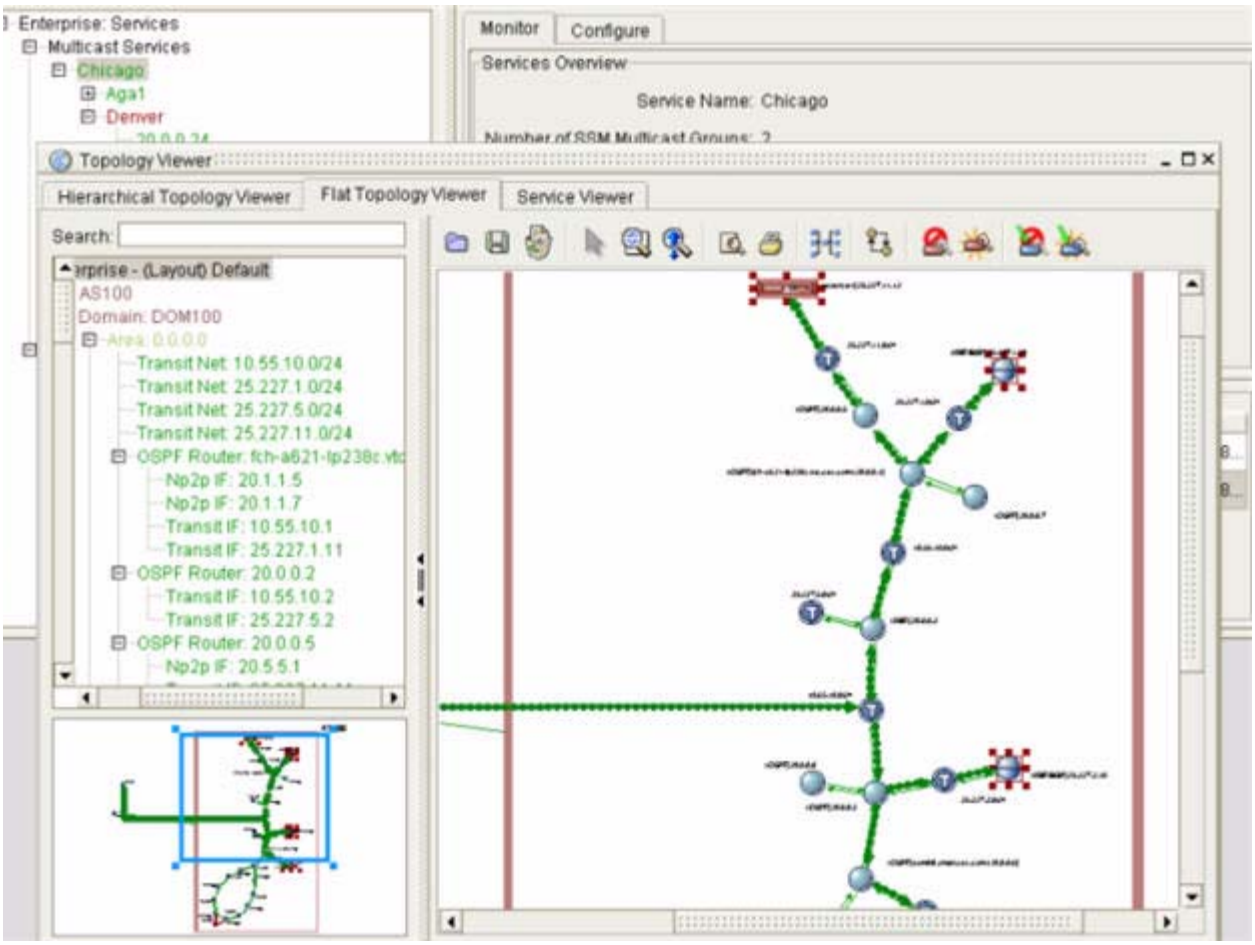
Step 4 Select **Display Graphical Multicast Tree** and then select one of the following options:

- **Display Flat Graphical Multicast Tree—**Opens the Topology Viewer and presents the multicast service in the Flat Topology Viewer.
- **Display Hierarchical Graphical Multicast Tree**—Opens the Topology Viewer and presents the multicast service in the Hierarchical Topology Viewer.

The selected tab opens in the Topology Viewer showing the flow of service-related data, represented by dashed green arrows.

Figure 3-38 shows an available and conforming multicast service in the Hierarchical Topology Viewer of the Topology Viewer. All SSM multicast service groups are available and conform to their configured baselines.

Figure 3-38 Available, Conforming Service



Remove a Graphical Multicast Service

To remove a graphical multicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Multicast Services** from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the name of the multicast service you want to map in the Services section of the tab.

Step 4 Select **Remove Graphical Multicast Tree Display** and then select one of the following options:

- **Remove Flat Graphical Service Display—**Removes the graphical service display from the Flat Topology Viewer.
- **Remove Hierarchical Service Display**—Removes the graphical service display from the Hierarchical Topology Viewer.
- **Remove Only Graphical Service Display**—Removes the graphical service display from the Service Viewer.

The Topology Viewer remains open in the Management Console.

Remove a Graphical Multicast Tree

To remove a graphical multicast tree:

Step 1 Use the procedure to Start Service Monitor, page 3-37, and select the name of a multicast service from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the name of the multicast service you want to map in the Services section of the tab.

Step 4 Select **Remove Graphical Multicast Tree Display** and then select one of the following options:

- **Remove Flat Graphical Multicast Tree Display—**Removes the graphical multicast tree from the Flat Topology Viewer.
- **Remove Hierarchical Graphical Multicast Tree Display**—Removes the graphical multicast tree from the Hierarchical Topology Viewer.

The Topology Viewer remains open in the Management Console.

Viewing the Root Cause of Multicast Services Issues

Misconfigurations, metric changes, and other routing issues can cause multicast services to become unavailable or to veer from their baselines. Identifying the root cause—the set of events that interrupt services—can be a time-consuming and labor-intensive process.

Service Monitor simplifies root cause diagnosis by identifying the set of events that affects a multicast service or SSM multicast service group. The root cause is supplied in response to network events only. (Network events do not include user actions that affect multicast services, such as refreshing the baselines of an SSM multicast service group.)

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the multicast service you want to view from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the multicast service you want to view in the Services section of the tab, and click **Display Root Cause**.

The Root Cause window opens in the Monitor tab and shows the events that caused the multicast service to change to its current state.

Note You will not see the Show Root Cause menu option displayed unless the multicast service has changed in some way.

Viewing Details of Multicast Services and SSM Multicast Service Groups

Service Monitor provides data about Multicast Services, SSM Multicast Service Groups, and Multicast Recipients.

To view the details of multicast services and SSM multicast service groups:

Step 1 Use the procedure to Start Service Monitor, page 3-37, and select **Multicast Services** from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Each multicast cast services is listed in the menu hierarchy under Multicast Services.

Step 3 Select a multicast service to view the details of from the hierarchy of services.

Each SSM multicast group is listed in the menu hierarchy under its multicast service name.

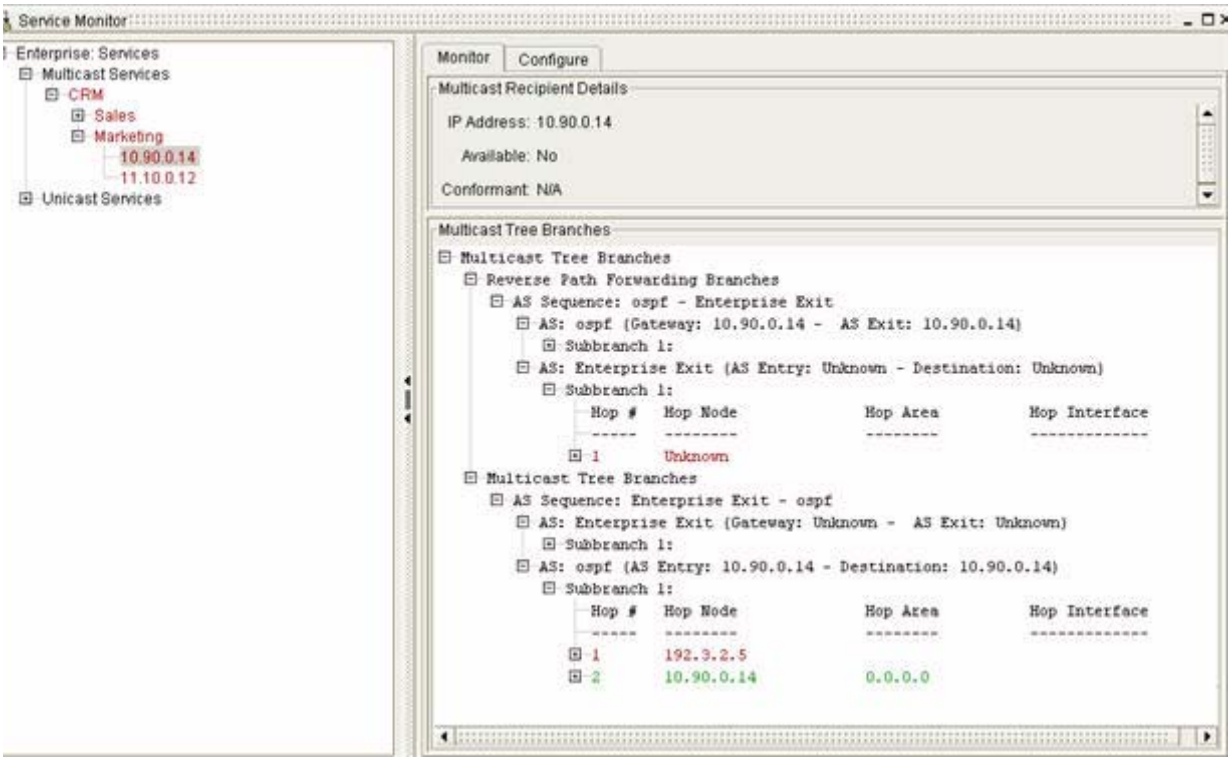
Step 4 Select an SSM multicast service group to display its recipients.

Each SSM multicast group recipient is listed in the menu hierarchy under its SSM multicast group. Each recipient and its current status is also shown in the Monitor tab under Multicast Recipients.

Step 5 Click on a recipient in the menu hierarchy.

The recipient's tree branches are displayed in the Monitor tab under Multicast Tree Branches. See Figure 3-39.

Figure 3-39 Multicast Service Tree Branches



Step 6 Click on the plus (+) signs to reveal the details of each branch and subbranch.

Managing Baselines of Multicast Service and SSM Multicast Service Groups

You can set a baseline on any available SSM multicast service group. If you create an SSM multicast service group when intermediate routers or networks are unavailable, a baseline is not established for the multicast service or its related SSM multicast service group.

When the expected behavior of an SSM multicast service group does not conform to its baseline due to configuration changes or any other changes in the network, you can reset the baseline. See Reset the Baseline of an SSM Multicast Service Group, page 3-64 for more information.

Reset the Baseline of a Selected SSM Multicast Service Group

To reset the baseline of an SSM multicast service group:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the name of a multicast service from the menu hierarchy that contains the SSM multicast service group you want to change.

Step 2 Select the **Monitor** tab.

Step 3 Select the multicast service that contains the SSM multicast service group you want to change in the Services section of the tab.

Step 4 Right-click the SSM multicast group in the SSM Multicast Group section of the tab.

Step 5 Click **Reset Baseline**.

The baseline of the selected SSM Multicast Group is refreshed.

Remove the Baseline of an SSM Multicast Service Group

To remove the baseline of an SSM multicast service group:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the **Monitor** tab.

Step 2 Select the multicast service that contains the SSM multicast service group you want to change from the hierarchy of multicast services at the left of the Service Manager window. If the SSM multicast service group is not displayed automatically, click the plus (**+**) sign of the multicast service that contains it.

Step 3 Right-click the SSM multicast group you want to remove baseline of in the SSM Multicast Group section of the Monitor tab.

Step 4 Select **Remove Baseline**.

The baseline of the selected SSM multicast group is removed.

The following icon appears in the Conforms field of the SSM multicast group to indicate that the baseline was removed. 

Reset the Baseline of an SSM Multicast Service Group

To reset the baseline of an SSM multicast service group:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the **Monitor** tab.

Step 2 Select the multicast service that contains the SSM multicast group you want to change from the hierarchy of services at the left of the Service Manager window. If the SSM multicast service group is not displayed automatically, click the plus (**+**) sign of the multicast service that contains it.

Step 3 Right-click the SSM multicast service group you want to change (if available) by removing its baseline in the SSM Multicast Service Group section of the Monitor tab.

Step 4 Select **Reset Baseline**.

The baseline of the selected SSM multicast service group is reset. The following icon appears in the **Enabled** field of the SSM multicast service group to indicate that the baseline was reset: 

Remove Baselines of an SSM Multicast Service Group

To remove the baselines of an SSM multicast service group:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the **Monitor** tab.

Step 2 Select the multicast service that contains the SSM multicast service group you want to change in the Services section of the tab.

Step 3 Right-click the SSM multicast service group in the SSM Multicast Service section of the tab.

Step 4 Click **Remove Baseline**.

The baseline of the selected SSM multicast service group is removed.

Managing Multicast Services and SSM Multicast Service Groups

Once you have configured service paths and groups, you can perform the following procedures:

- Remove a Single Multicast Service, page 3-65
- Remove Multiple Multicast Services, page 3-65
- Add SSM Multicast Service Groups, page 3-66
- Remove a Single SSM Multicast Service Group, page 3-67

- Remove Multiple SSM Multicast Service Groups, page 3-67
- Reconfigure a SSM Multicast Service Group, page 3-68

Remove a Single Multicast Service

To remove a single multicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the multicast service you want to remove from the menu hierarchy.

Step 2 Select the **Configure** tab.

Step 3 Click **Remove Service**.

A message is displayed asking for confirmation to remove the multicast service.

Step 4 Click **Yes**.

The multicast service and all related SSM Multicast Service groups are removed.

or

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Multicast Services** from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the multicast service you want to remove in the Monitor tab.

Step 4 Select **Remove Multicast Service**.

A message is displayed asking for confirmation to remove the multicast service.

Step 5 Click **Yes**.

The multicast service and all related SSM multicast service groups are removed.

Remove Multiple Multicast Services

To remove multiple multicast services:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Multicast Services** from the menu hierarchy.

Step 2 Select the **Configure** tab.

Step 3 Click **Remove Service(s)** in the Multicast Services Removal section of the tab.

The Services Removal Wizard appears (see Figure 3-40).

Figure 3-40 Service Removal Wizard

Step 4 Select the multicast services you want to remove and click **Next**.

Step 5 Click **Finish**.

The multicast services and all their associated SSM multicast groups are removed.

Add SSM Multicast Service Groups

To add SSM multicast service groups:

Step 1 Use the procedure to Start Service Monitor, page 3-37.

Step 2 Select the multicast service that to which you want to add an SSM multicast service group from the menu hierarchy.

Step 3 Select the **Configure** tab.

Step 4 Click **Create SSM Multicast Group(s)** in the SSM Multicast Groups Creation field.

The Multicast Group Creation wizard appears. See Configure an SSM Multicast Service Group, page 3-45.

or

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Multicast Services** from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the name of the multicast service you want to add an SSM multicast service group to in the Services section of the Monitor tab.

Step 4 Select **Add SSM Multicast Group**.

The SSM Multicast Service Creation wizard appears.

Step 5 Complete the wizard to create a SSM Multicast Service Group.

For information about completing the wizard, see Configure an SSM Multicast Service Group, page 3-45.

Remove a Single SSM Multicast Service Group

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select from the menu hierarchy the SSM multicast group that you want to remove.

Step 2 Select the **Configure** tab.

Step 3 Click **Remove SSM Multicast Group** in the SSM Multicast Group Removal section of the tab.

A message is displayed asking for confirmation to remove the SSM multicast service group.

Step 4 Click **Yes**.

The SSM multicast service group path and its branches are removed.

or

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select from the menu hierarchy the multicast service that contains the SSM multicast service group you want to remove.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the SSM multicast service group path you want to remove in the SSM Multicast Groups section of the Monitor tab.

Step 4 Select **Remove SSM Multicast Group**.

A message is displayed asking for confirmation to remove the SSM multicast service group.

Step 5 Click **Yes**.

The SSM multicast service group path and its branches are removed.

Remove Multiple SSM Multicast Service Groups

To remove multiple SSM multicast service groups:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select from the menu hierarchy the multicast service that contains the SSM multicast service group you want to remove.

Step 2 Select the **Monitor** tab.

Step 3 Click **Remove SSM Multicast Group**s in the SSM Multicast Groups Removal section of the tab.

The Multicast Groups Removal Wizard appears (see Figure 3-41).

Figure 3-41 Multicast Group Removal Wizard

Step 4 Select the SSM multicast groups you want to remove and press **Next**.

Step 5 Click **Finish**.

The SSM multicast service groups and their branches are removed.

Reconfigure a SSM Multicast Service Group

To reconfigure an SSM multicast service group:

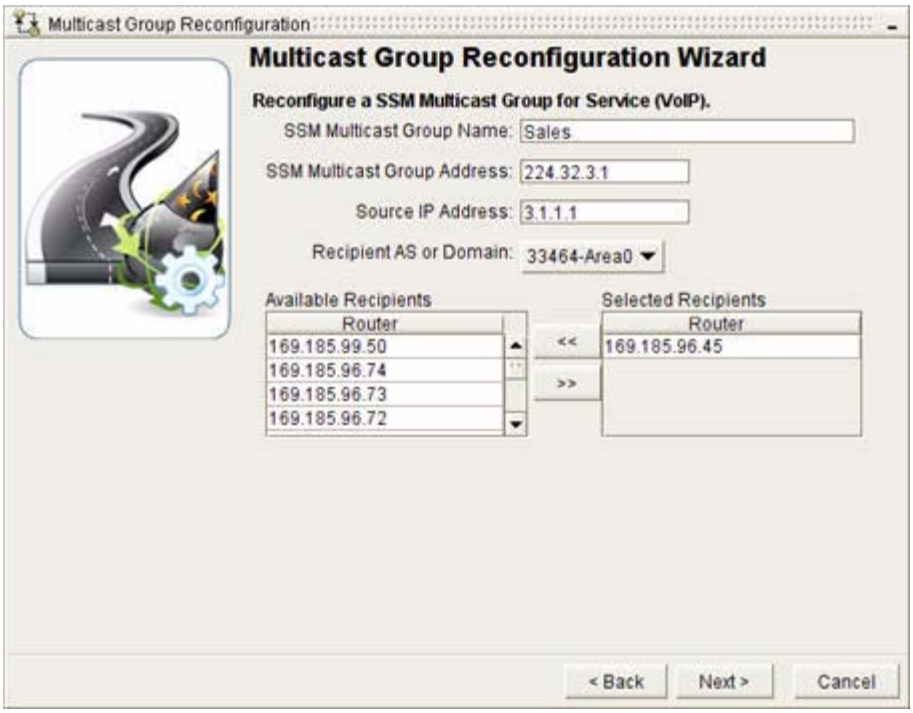
Step 1 Use the procedure to Start Service Monitor, page 3-37 and select the SSM multicast service group you want to reconfigure.

Step 2 Select the **Configure** tab in the Service Manager window.

Step 3 Click **Reconfigure SSM Multicast Group** in the SSM Multicast Group Configuration panel.

The Multicast Group Reconfiguration Wizard appears (see Figure 3-42).

Figure 3-42 Multicast Group Reconfiguration Wizard



Step 4 Make the necessary changes and click **Next**.

See Configure an SSM Multicast Service Group, page 3-45 for more information about completing this form.

Step 5 Click **Finish**.

or

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select from the menu hierarchy the multicast service that contains the SSM multicast service group you want to reconfigure.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the SSM multicast service group you want to change in the SSM Multicast Groups section of the Monitor tab.

Step 4 Select **Reconfigure SSM Multicast Group**.

The SSM Multicast Group Reconfiguration Wizard appears.

Step 5 Make the necessary changes and click **Next**.

See Configure an SSM Multicast Service Group, page 3-45 for more information about completing this form.

Step 6 Click **Finish**.

Enabling and Disabling Multicast Services and SSM Multicast Service Groups

Enabling a multicast service or SSM multicast service group in Service Monitor allows you to monitor its availability and conformity. In addition, setting alarms on a selected service or SSM multicast service group in Alarm Monitor causes alarms to trigger when to the selected multicast service or SSM multicast service group occur. Path Analyzer enables all multicast services and SSM multicast service group by default when you create them.

You can disable a multicast service or SSM multicast service group—for example, to perform routine maintenance such as removing an intermediate router from your network. You can re-enable it when you completed maintenance activities.

Note After disabling a multicast service or SSM multicast service group, you have to re-enable it to continue monitoring it for availability and conformance.

See Enable a Multicast Service, page 3-71 and Enable an SSM Multicast Service Group, page 3-71 for information.

Disable a Multicast Service

To disable a multicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Multicast Services** from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the name of the currently enabled multicast service you want to disable in the Services section of the tab.

Step 4 Click **Disable Service**.

The service is disabled. The **Disabled** icon  appears in the Status field of the service.

Disable an SSM Multicast Service Group

To disable an SSM multicast service group:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select from the menu hierarchy the multicast service that contains the SSM multicast service group you want to disable.

Step 2 Select the **Monitor** tab.

Step 3 Click the name of the service that contains the SSM multicast service group you want to disable in the SSM Multicast Group section of the tab.

Step 4 Click **Disable SSM Multicast Group**.

The SSM multicast service group is disabled. The **Disabled** icon appears in the Status field of the SSM multicast service group.

Enable a Multicast Service

To enable a multicast service:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select **Multicast Services** from the menu hierarchy.

Step 2 Select the **Monitor** tab.

Step 3 Right-click the disabled multicast service you want to re-enable in the Services section of the tab.

Step 4 Click **Enable Service**.

The **Enabled** icon appears in the Status field of the multicast service, indicating that the multicast service is enabled.

The Availability and Conformity fields are updated immediately to reflect the current state of the system.

Enable an SSM Multicast Service Group

To enable an SSM multicast service group:

Step 1 Use the procedure to Start Service Monitor, page 3-37 and select from the menu hierarchy the multicast service that contains the SSM multicast service group you want to disable.

Step 2 Select the **Monitor** tab.

Step 3 Click the name of the service that contains the SSM multicast service group you want to re-enable in the SSM Multicast Group section of the tab.

Step 4 Click **Enable SSM Multicast Group**.

The **Enabled** icon appears in the Status field of the SSM Multicast Group, indicating that the SSM multicast service group is enabled.

The Availability and Conformity fields are updated immediately to reflect the current state of the system.

Setting Alarms on Multicast Services and SSM Multicast Service Groups

In Service Alarm Monitor, you can set alarms on multicast services and SSM multicast service group to receive immediate, automatic notification of service changes, such as a multicast service becoming unavailable or not conforming to a baseline. For information, see Setting and Monitoring Alarms on page 8-1. When a multicast service or SSM multicast service group with an alarm is removed, the alarm is purged as well.

You can also export service alarms to a syslog host or an SNMP agent for notification through your network management system (NMS). For information, see Chapter 8, Exporting Alarm Triggers, in the *Cisco Service Path Analyzer System Administrator Guide*.

Replaying Historical Services

For information about replaying the changes to historical services and service paths, see Start a Module in a Historical Session, page 13-11 and Find Information about Historical Service Paths, page 13-13.

Related Forms

The following tables detail the graphical elements and dialog boxes of the Service Monitor.

Root Cause Dialog Box

In the Root Cause dialog box, you can View the Root Cause of a Change to a Multicast Service.

Table 3-7 describes the fields of the Root Cause dialog box.

Table 3-7 Root Cause

Field	Description
Event ID	Shows the Event ID of the root cause event.
Event Description	Shows a description of the root cause event.
Event Time	Shows the time and date when the event occurred, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32.

Details of a Multicast Service

From the Service details area of the Monitor tab, you can view service details.

Table 3-8 describes service details.

Table 3-8 Details of a Multicast Service

Field	Description
Service Details	Shows the following details of a multicast service: • Service Name • Enabled or Disabled • Available or Unavailable • Conformant or Non-Conformant • Last Update Time
Multicast Service Name	Identifies the name of the multicast service.

Table 3-8 Details of a Multicast Service

Field	Description
Enabled	Identifies if the multicast service is enabled or disabled.
Available	Identifies if the multicast service is available or unavailable.
Conformant	Identifies if the multicast service is conformant or deviant.
Last Update Time	Identifies the multicast service's last update time.

Details of a SSM Multicast Service Group

From the SSM Multicast Service Group details area of the Monitor tab, you can view SSM multicast service group details.

Table 3-9 describes the SSM Multicast Service Group details.

Table 3-9 Details of an SSM Multicast Service Group

Field	Description
SSM Multicast Service Group Details	Shows the following details of SSM multicast service group: • SSM Multicast Service Group Name • Source IP Address • Gateway Shows • Gateway AS or Domain • Destination/IP Address • Enabled or Disabled • Available or Unavailable • Conformant or Non-Conformant • Path Loop • Last Update Time
SSM Multicast Service Group Name	Identifies the name of an SSM multicast service group.
Source IP Address	Identifies the IP address of the SSM multicast service group.
Gateway Shows	Identifies the gateway router.
Gateway AS or Domain	Identifies the autonomous system or routing domain in which the source is located.
Destination IP Address	Identifies the IP address of the destination router.
Enabled	Identifies if the SSM multicast service group is enabled or disabled.
Available	Identifies if the SSM multicast service group is available or unavailable.

Table 3-9 Details of an SSM Multicast Service Group

Field	Description
Conformant	Identifies if SSM multicast service group is conformant or deviant.
Path Loop	Identifies if an SSM multicast service group has a path loop.
Last Update Time	Identifies the SSM multicast service group's last update time.

Details of SSM Multicast Service Group Branches Dialog Box.

From the SSM multicast service group details area of the Monitor tab, you can view details of SSM multicast service group branches.

Table 3-10 describes the Details of SSM Multicast Service Group Branches dialog box.

Table 3-10 Details of SSM Multicast Group Branches

Field	Description
SSM Multicast Service Group Branch	Provides detailed information about the nodes and links that a given branch traverses through a network.
AS Sequence	Provides the ordered list of autonomous systems through which a branch traverses through a network. It provides multiple ways which a path travels from a gateway to its destination.
AS	Provides the ordered listing of autonomous systems for the AS Sequence. It provides the starting point within an AS and ending point within an AS. It is the unique set of entry and exit points for an ordered AS.
Subbranch	Given two endpoints, it represents the unique traversal set of nodes and links.
Hop Number	Identifies each hop, each step from node-to-node, that the path makes from source to destination.
Hop Node	Shows the IP address or prefix of each hop between the source and destination.
Hop Area	Shows the area in which each hop resides.
Hop Interface	Shows the IP address of the router interface that the path traverses from source to destination.
The following fields are available for each selected hop. Expanding the router by clicking the plus sign (+) next to its entry causes the following fields to be displayed.	
Node Type	Provides some type of router or network.
Link Type	Provides some type of interface or router link.
Primary Route	Provides the information needed to determine why the service path made its routing decision (only on routers).

Table 3-10 Details of SSM Multicast Group Branches

Field	Description
Secondary Route	Provides the information needed to determine why the service path made its routing decision (only on routers).
Destination Type	Shows the type of destination, for example, network or route outside the scope of Path Analyzer.

CHAPTER 4

Monitoring Changes in Routing

Tracking Changes, Investigating Events

Depending on your Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) configuration, Listeners form adjacencies with routers and collect data about changes in routing patterns over the following combinations of Layer 3 routing protocols:

- **OSPF only**—Provides information about changes in routing within and between logical OSPF routing domains and describes destinations in external autonomous systems.
- **OSPF and BGP**—Provides information about routing patterns within and between multiple autonomous systems.

Both OSPF and BGP Listeners send collected information to the Path Analyzer Server, which receives, processes and persists data, and provides you with the visual, real-time or historical view of routing changes (*events*).

View of Real-time Events

The Path Analyzer Event Log enables you to view information about specific changes in routing patterns and find specific events by identifier or time of occurrence.

The Event Log shows:

- a high-level view of all real-time events occurring enterprise-wide in your network, and
- a low-level view of specific events related to a selected autonomous system or routing domain.

Use the high-level view of real-time events to identify the domain in which the events occur and to review these events before taking action.

Event Log Capabilities

The Event Log allows you to:

- view events.
- find specific events by ID or by time period.
- filter the full set of events that occur in your enterprise, or events within a selected autonomous system or routing domain.

Real-time Filtering and Investigative Querying

The Event Log provides real-time filtering and investigative querying for events in selected autonomous systems and routing domains. Using the information returned from filtering and querying, you can identify and fix routing problems, track the causes of past routing events, and ensure that your network remains available.

Historical Event Log

Event Log is available during a historical session, allowing you to replay events that occurred previously on your network. For information about starting Event Log in a historical session, see Start a Module in a Historical Session, page 13-11.

Event Log Tasks

- Starting the Event Log, page 4-2.
- Viewing Events, page 4-3.
- How Events Are Displayed in the Event Log, page 4-5.
- Working with Events, page 4-11.
- Finding Events, page 4-15.
- Filtering OSPF Events, page 4-16.
- Filtering BGP Events, page 4-20.
- Working with Filters, page 4-36.

Starting the Event Log

Start the Real-time Event Log to view the current, dynamic list of events. For information, see Start the Event Log, page 4-2.

Start Event Log in a historical session to view events that occurred during a selected period of time. For information, see Start a Module in a Historical Session, page 13-11.

Start the Event Log

To start the Event Log from the Path Analyzer taskbar, click **Start > Event Log**.

The Event Log window appears.

- A hierarchical menu of your enterprise occupies the left-hand side of the screen. It lists every autonomous system and domain in your enterprise and each category of event viewable in that AS or domain.
- The **AS/Domain Overview** section occupies the right-hand side of the window. It displays current Event ID's listed by the domain or autonomous system from which they originate.

Note Event identifiers are unique within a BGP-enabled autonomous system and OSPF routing domain. It is possible to find events that have the same identifier which have occurred in different autonomous systems.

Viewing Events

Path Analyzer generates events—notifications of routing changes within and between autonomous systems and routing domains in your network. These events inform you of real-time routing changes within your network.

Routers learn about changes via their routing protocols. Path Analyzer Listeners collect this routing information for the autonomous systems and routing domains in which they are instrumented.

- Listeners obtain information from adjacent routers about changes that occur *within* an autonomous system over Open Shortest Path First (OSPF) or internal Border Gateway protocol (iBGP).
- Listeners learn about changes *between* autonomous systems over external Border Gateway Protocol (eBGP).

Changes that Generate Events

Events provide information about the routers, routes, and interfaces in your network. These events indicate:

- Configuration Changes, page 4-3—including any addition, deletion, or change to a router interface as well as changes to the cost metric associated with a route.
- Network Changes, page 4-3—events that affect topology and routing patterns across your network such as the addition, removal, or change in state of a router.

Configuration Changes

Staying updated about configuration changes can assist in identifying misconfigurations that lead to routing issues, such as:

- Duplicate or incorrect IP address assigned to a router interface, which can lead to unexpected routing patterns.
- Incorrect cost metric assigned to a router interface, causing traffic to be sent over unexpected paths.
- Misconfigured interface-to-network connection, which can cause traffic to be routed to the wrong network.
- Flap on a router interface, which can result in the sporadic disruption of services. Flap can occur when a router is misconfigured.

Network Changes

Staying abreast of network changes can help you to monitor your network for issues such as:

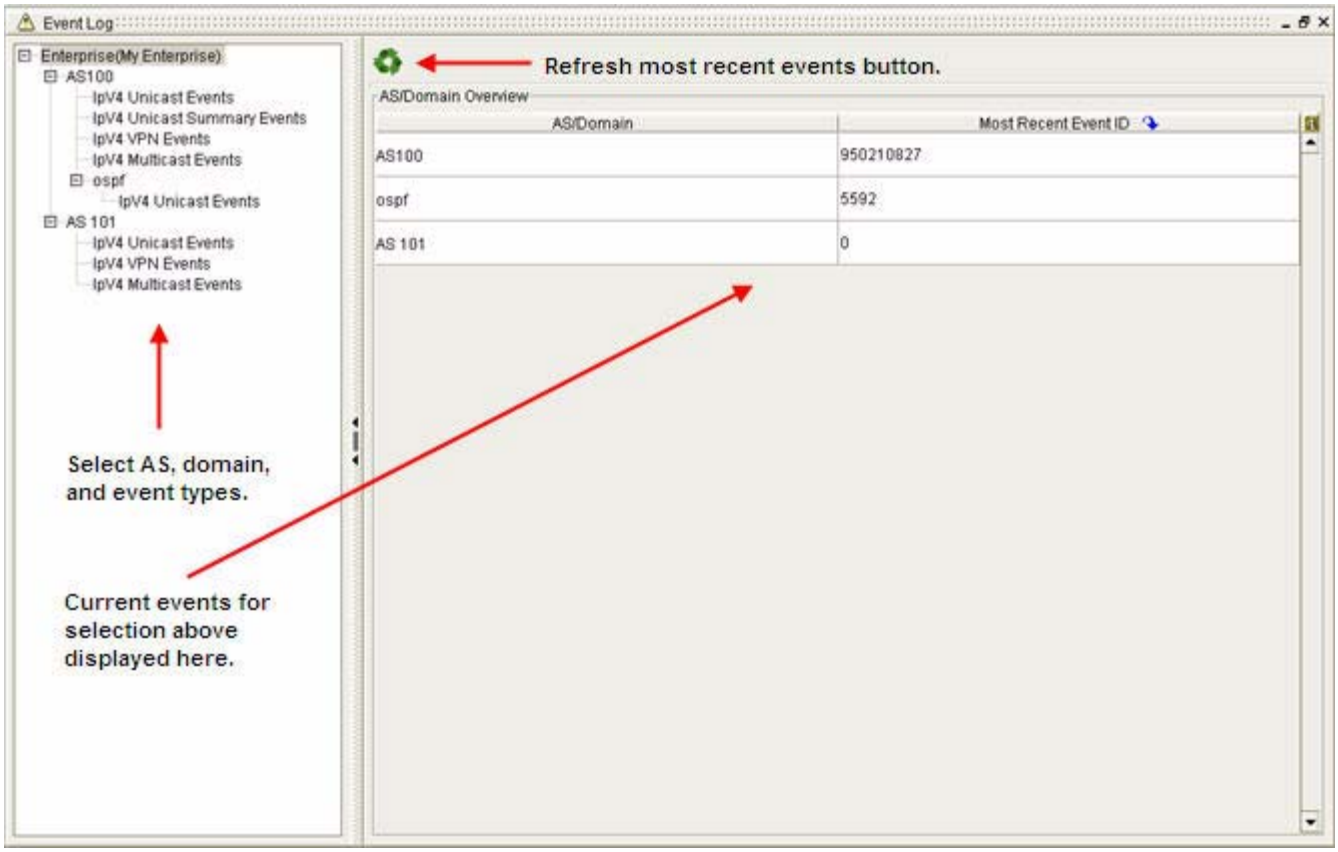
- Router overload, indicating the need for additional routers.
- Change in the number of areas an ABR supports. This can create a problem if an ABR changes state to a single-area router, and the affected area loses router support.

- Hardware issue affecting routing. For example, when a router or router interface becomes unavailable.
- Physical removal of a router from the network for maintenance or repair.

Enterprise Events

The Event Log provides an overview of event activity, per domain, and allows you to view the most recent routing events that have occurred in your network (see Figure 4-1).

Figure 4-1 Enterprise View in Event Log



Changes in Routing Between Autonomous Systems

Awareness of routing changes between autonomous systems provides immediate information about:

- Availability of routes across the autonomous systems of your network.
- Connectivity of routers that forward data across autonomous systems.
- Security of your data, ensuring that it reaches the destination you intended.

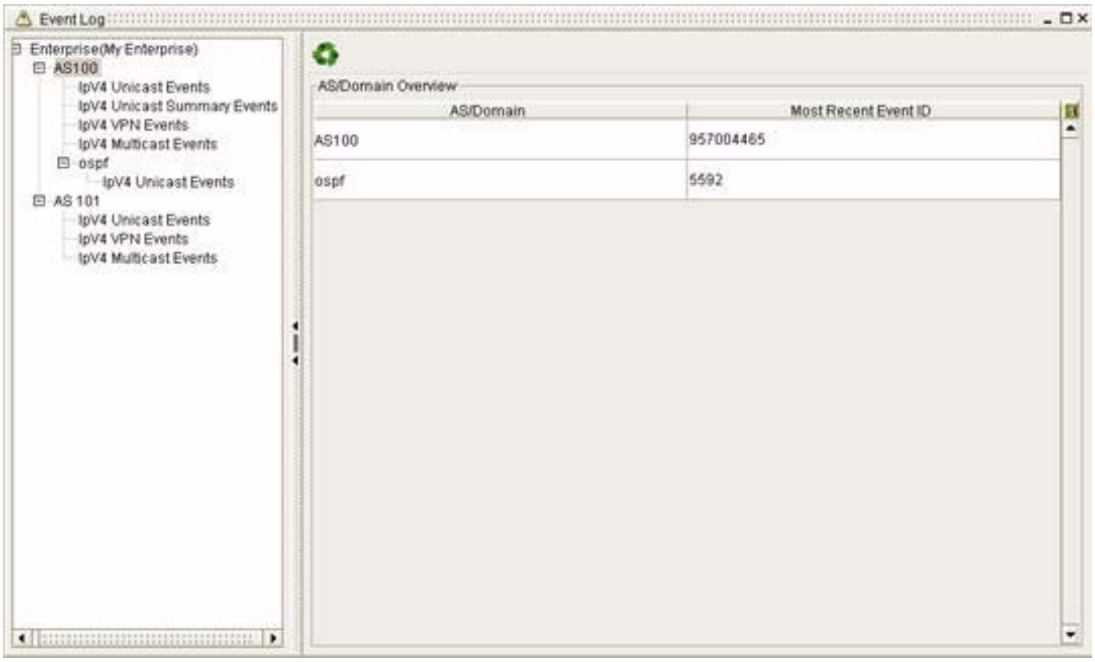
How Events Are Displayed in the Event Log

By default, an overview of your entire enterprise is displayed in the Event Log window when you first open it. You will see a listing of all the autonomous systems and domains and the most recent Event ID for each one.

Selecting an autonomous system from the network hierarchy in the left side of the Event Log window will reveal an overview for that AS (see Figure 4-2).

Selecting a domain from the network hierarchy in the left side of the Event Log window will reveal an overview for that domain.

Figure 4-2 Autonomous System View in Event Monitor



You can also select event types from the hierarchical menu, for either OSPF or BGP. The fields displayed on the event screen will vary, depending on the routing protocol and type of event you choose.

Displaying OSPF Events

The Event Log is used to display OSPF events.

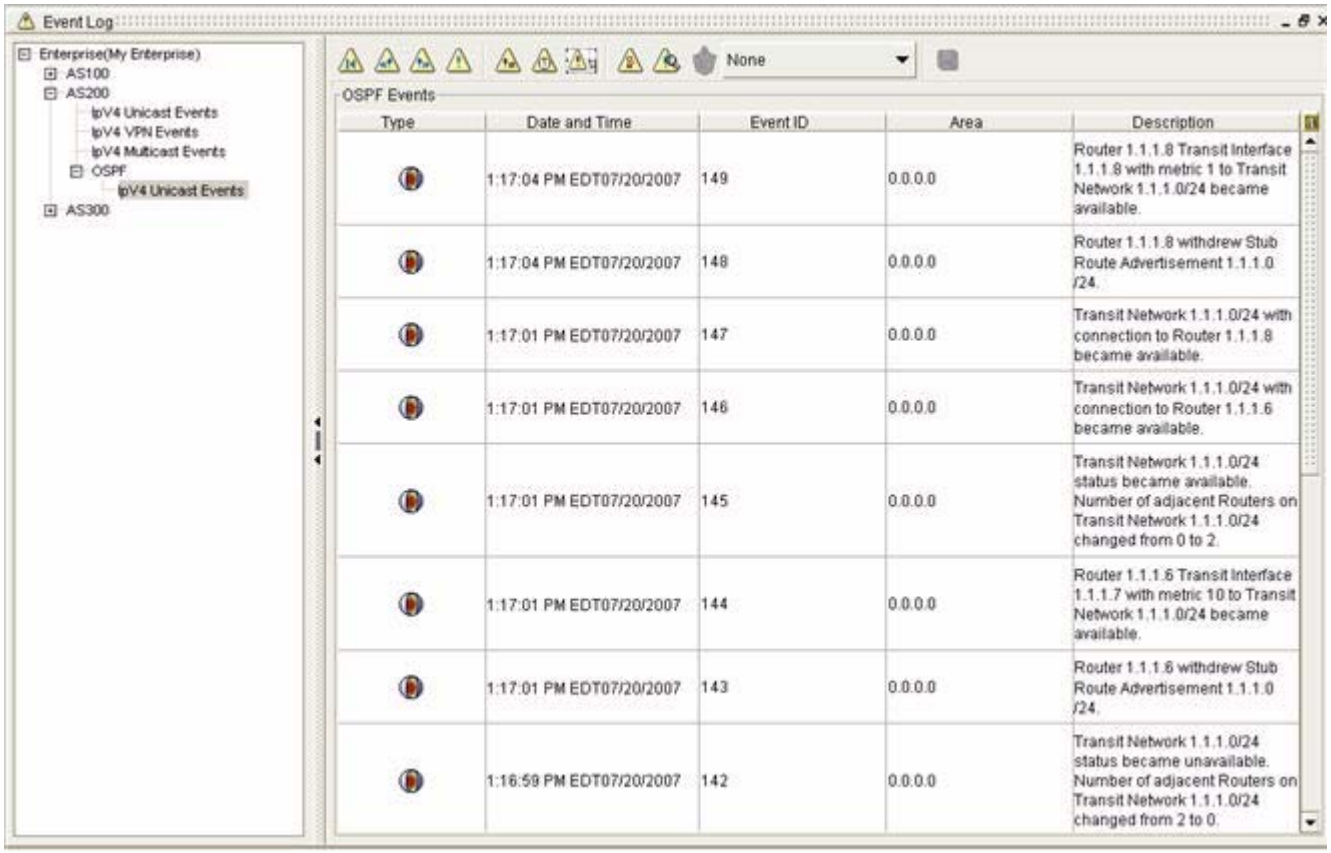
Displaying OSPF Events in the Event Log

In Path Analyzer, the Path Analyzer Server generates events about changes *within* an autonomous system from routing messages that Listeners collect from routers over the Open Shortest Path First (OSPF) Protocol.

Each routing message, called a Link State Advertisement (LSA), correlates to one or more events indicating changes to network entities, such as routers, interfaces, routes, and networks. Events that occur within or between OSPF areas are displayed in the Event Log and are persisted in the Path Analyzer database.

Selecting **IPV4 Unicast Events** within an OSPF domain will display the following information (see Figure 4-3).

Figure 4-3 Event Log Showing OSPF Events



Type—Shows the type of event, represented by an icon. See OSPF Event-Type Icons, page 4-6.

Date and Time—The time and date when the event occurred, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. If the date and time of an event are not displayed in the Date & Time field, refer to the date and time of the next event in the list for this information.

Event ID—The unique identifier of the event. Event IDs are unique per autonomous system or routing domain. It is possible for events in different routing domains to have the same Event ID.

Area—Provides the unique identifier of the OSPF routing domain, referred to as an area, in which the event occurred.

Description—Explains the nature of the event.

OSPF Event-Type Icons

The OSPF Event screen uses the icons in Figure 4-4 to indicate the event type:

Figure 4-4 Event Types

- **Core**—Changes to the entity affect routing within the configured area.
- **Propagation**—Changes to the entity affect routing in more than one area.
- **Peripheral**—Changes to the entity occur in more than one autonomous system (AS).

Displaying BGP Events

The Event Log is used to display BGP events:

- Displaying BGP Events in the Event Log, page 4-7
- Displaying BGP IPV4 Unicast Events, page 4-7
- BGP Event Detail Dialog Box, page 4-8
- Displaying BGP IPV4 Unicast Summary Events, page 4-9
- Displaying BGP IPV4 VPN Events, page 4-10
- View a Specific VPN Event, page 4-11
- Displaying BGP IPv4 Multicast Events, page 4-11

Displaying BGP Events in the Event Log

At the edges of autonomous systems, routers exchange data about destinations in other autonomous systems over external gateway protocols, such as external Border Gateway Protocol (eBGP).

Path Analyzer Listeners form adjacencies with BGP routers, called BGP speakers, to obtain routing data. Listeners move this information to the Path Analyzer Server, which then generates and sends event identifiers, descriptions, and other related information to the Event Log.

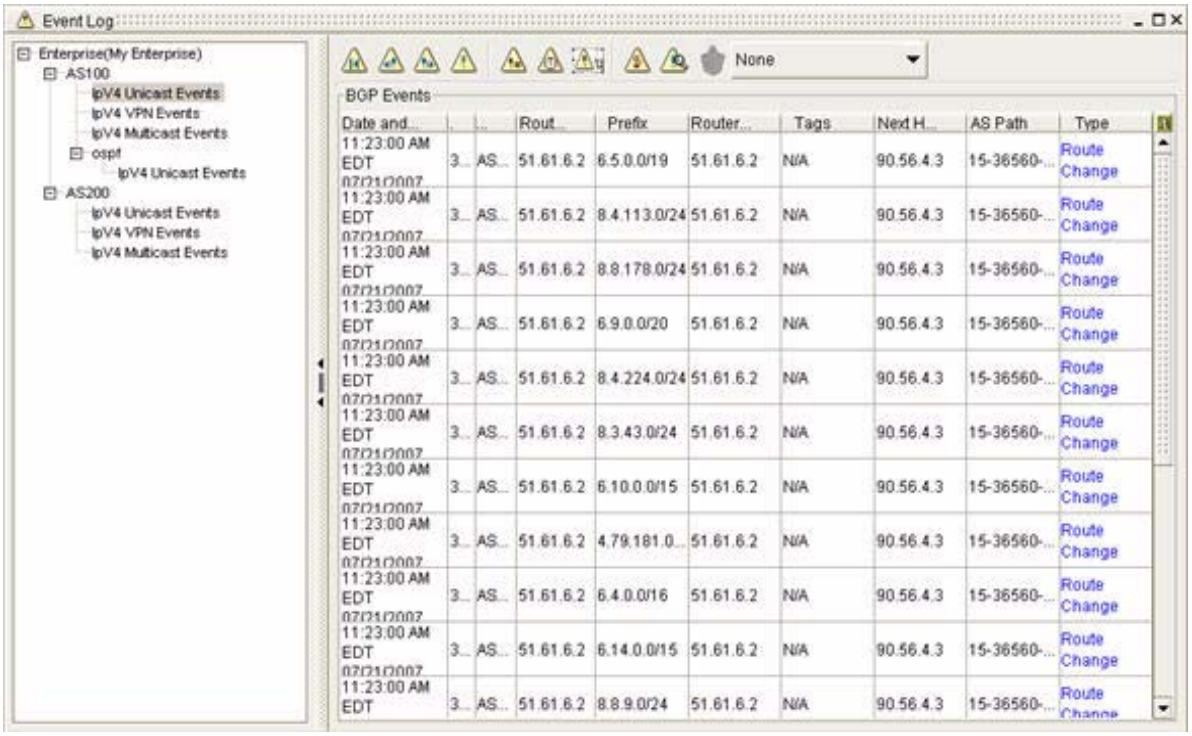
You can choose the following kinds of BGP events to display:

- IPV4 Unicast Events
- IPV4 Unicast Summary Events (Route summarization must be activated to see this menu selection)
- IPV4 VPN Events
- IPV4 Multicast Events

Displaying BGP IPV4 Unicast Events

Selecting IPV4 Unicast Events within an AS will display the following information (see Figure 4-5).

Figure 4-5 Event Log for BGP IPV4 Unicast Events



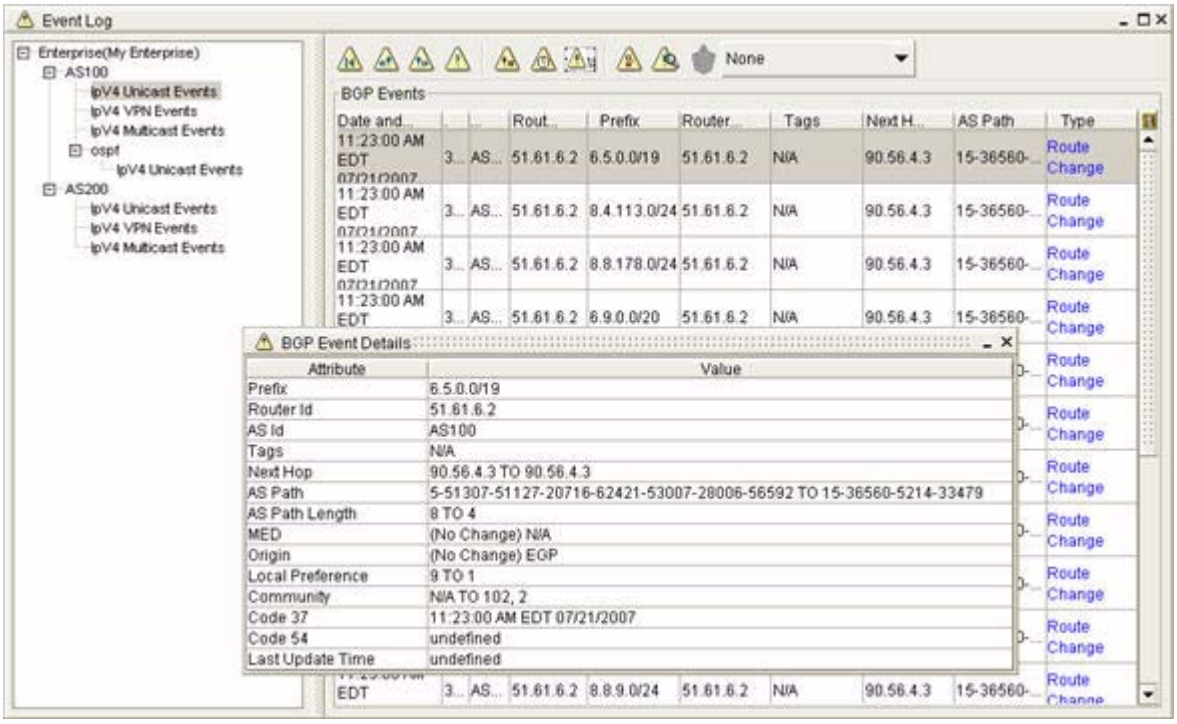
- **Date and Time**—Date and time stamp indicating when the Path Analyzer Server received the BGP message from which the event was derived.
- **Event ID**—A numeric value the Path Analyzer Server generates to uniquely identify a BGP event in an autonomous system. Because each event is unique within its routing domain or autonomous system, you may discover events that occurred in different and separate routing domains, which have the same Event ID.
- **AS Name**—Name of the autonomous system in which the event was advertised.
- **Router Name—**BGP speaker that advertised the event.
- **Prefix**—The prefix of the BGP route in the format `1.1.1.1/24`.
- **Router ID**—The IP address of BGP router that advertised the event.
- **Tags**—Any BGP tags associated with the event. For more information see Chapter 6, BGP Tagging.
- **Next Hop**—The router ID of the BGP speaker from which the advertising router receives routing updates.
- **AS Path**—The AS Path value, used to prevent routing loops.
- **Type**—Description of the event. Clicking the **Type** link causes the BGP Event Detail dialog box to open, showing specific details of the event (see Figure 4-6).

BGP Event Detail Dialog Box

The content of the BGP Event Details dialog box will vary, depending on:

- the event category (unicast, multicast, multicast summary, VPN).
- the type of event (new, change, etc.).

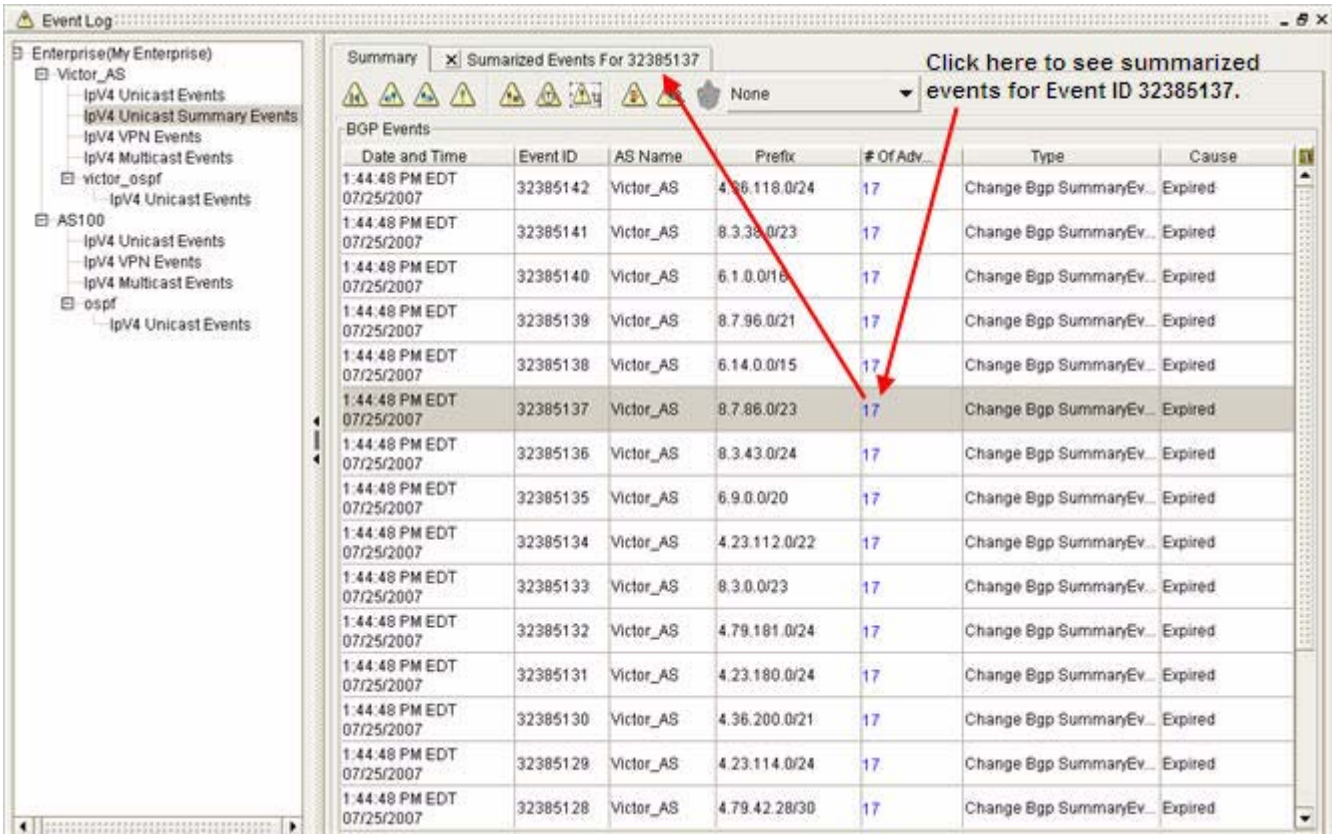
Figure 4-6 BGP Event Detail Dialog Box in Event Log



Displaying BGP IPV4 Unicast Summary Events

Selecting **IPV4 Unicast Summary Events** within an AS will display the following information (see Figure 4-7).

Figure 4-7 IPV4 Summary Events Screen in Event Log



To view summarized events for a specific Event ID:

Step 1 Click in the corresponding # of Adv. column.

A tab with the Event ID appears at the top of the screen.

Step 2 Click on the **Summarized Event** tab to open it.

The summary events for that particular Event ID appears.

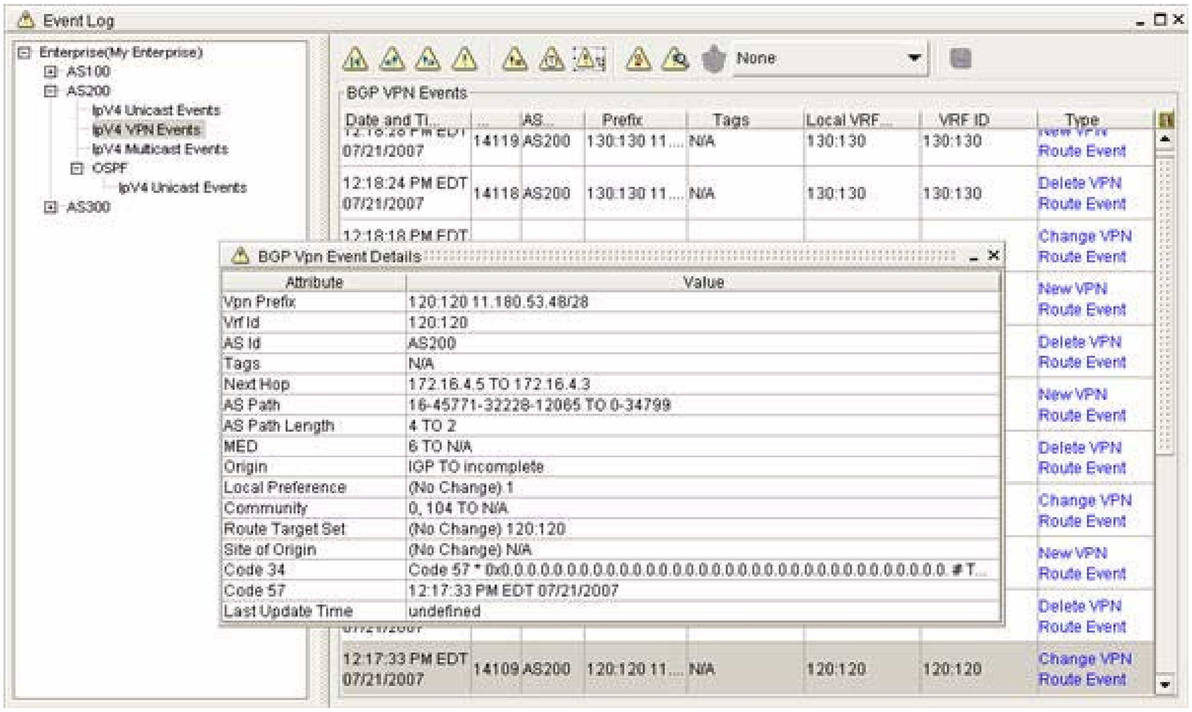
Step 3 Click on an associated entry in the Type column to view details for a specific event.

The BGP Event Details dialog box appears. Content of this box will vary depending on the type of event (new, change, delete).

Displaying BGP IPV4 VPN Events

Selecting **IPV4 VPN Events** within an AS will display the following information (see Figure 4-8).

Figure 4-8 Event Log and BGP VPN Event Details Screen for BGP IPV4 VPN Events



View a Specific VPN Event

Clicking the Type link causes the BGP Event Detail dialog box to open, showing specific details of the event.

The content of the Event Details dialog box will vary, depending on the type of event you have selected to view (New VPN route, Delete VPN route, etc.).

Displaying BGP IPv4 Multicast Events

To display BGP IPv4 events:

Step 1 Select **IPV4 Multicast Events** from the hierarchical menu.

Step 2 Click a link in the Type column.

The BGP Event Detail dialog box appears, showing specific details of the multicast event.

Working with Events

In the Event Log, you can perform the following tasks:

- View Enterprise Events, page 4-12
- View BGP Events, page 4-12

- View OSPF Events, page 4-12
- Scroll through Events, page 4-13
- Browse Backward through Events, page 4-13
- Browse Forward through Events, page 4-13
- Refresh the Event Log, page 4-14
- View the Beginning of the Event Log, page 4-14
- Change the Number of Events Displayed, page 4-14

View Enterprise Events

To view enterprise events:

Step 1 Use the procedure to Start the Event Log, page 4-2.

The Overview section shows the date and time of the most recent event per autonomous system or routing domain.

Step 2 Click the **Refresh Most Recent Events** button in the Most Recent Events section of the Event Log.

A list of the most recent events appears.

View BGP Events

To view BGP events:

Step 1 Use the procedure to Start the Event Log, page 4-2.

Step 2 Select an autonomous system from the network hierarchy, and then click one of the following event types to view its events.

- **IPV4 Unicast Events**
- **IPV4 Unicast Summary Events** (Route summarization must be activated to see this menu selection)
- **IPV4 VPN Events**
- **IPV4 Multicast Events**

The BGP events advertised within the selected autonomous system are displayed in the Event Log.

View OSPF Events

To view OSPF events:

Step 1 Use the procedure to Start the Event Log, page 4-2.

Step 2 Select an OSPF routing domain from the network hierarchy, and then click **IPV4 Unicast Events** to view its events.

The OSPF events advertised within the selected OSPF routing domain are displayed in the Event Log.

Scroll through Events

Drag the scroll box of the vertical scroll bar to scroll through the list.

See Change the Number of Events Displayed, page 4-14 for information about changing the number of events that can fit into the Event Log at the same time. See Event Log Toolbar, page 4-38.

Browse Backward through Events

Browsing backward through the list of events interrupts the dynamic updating capabilities of the Event Log, and allows you to browse backward through the static list of events.

To browse backward through events from the Event Log toolbar:

Step 1 Click the **Step Back** button.

The previous set of events are displayed.

Step 2 Continue to click **Step Back** to move backward through the list of events.

See Change the Number of Events Displayed, page 4-14 for information about changing the number of events to display in the Event Log window.

For example, if you set the number of events to display to `10`, you can scroll backward at the rate of ten events per click.

Step 3 Click the **Show Current** button to restore dynamic updating.

For information about browsing forward through the event list, see Browse Forward through Events, page 4-13, and Event Log Toolbar, page 4-38.

Browse Forward through Events

Browsing backward or forward through the event list interrupts the dynamic updating capabilities of the Event Log, and allows you to browse through the static list of events.

To browse forward through events from the Event Log toolbar:

Step 1 Click the **Step Forward** button.

The next set of events appears.

Step 2 Continue to click **Step Forward** to move forward through the list of events.

See Change the Number of Events Displayed, page 4-14 for information about changing the number of events to display at the same time.

For example, if you set the number of events to display to `10`, you can scroll forward at the rate of ten events per click

Step 3 Click **Show Current** to restore dynamic updating.

See Refresh the Event Log, page 4-14.

Refresh the Event Log

From the Event Log toolbar, click the **Show Current** button.

.

The Event Log dynamically updates the list of events. For information about browsing backward through the event list, see Browse Backward through Events, page 4-13, and Event Log Toolbar, page 4-38.

The Event Log dynamically updates the list of events to ensure that you always have a current view of routing events in your network.

Browsing backward or forward through the list of events interrupts dynamic updating, allowing you to browse backward or forward through the static list of events. See Browse Forward through Events, page 4-13 and Browse Backward through Events, page 4-13.

Clicking the **Show Current** button restores dynamic updating in Current Mode, and updates the event list with the most recent list of events.

View the Beginning of the Event Log

From the Event Log toolbar, click the **Show Oldest** button.

:

The list of events is redisplayed in the Event Log starting with the beginning of the list.

Change the Number of Events Displayed

To change the number of events displayed in the Event Log:

Step 1 Click the **Enter Number of Events to Display** button in the Event Log toolbar.

:

The Enter Number of Events to Display dialog box appears.

Step 2 Enter the number of events to be displayed into the Enter Number of Events to Display field when you click **Show Current**, **Step Back**, or **Step Forward**.

By default, you can display from 1 to 100 events at one time.

Step 3 Click **Set**.

The Number of Events setting is changed to the value you entered.

Finding Events

The Event Log provides two ways to find events:

- By unique identifier—Allows you to retrieve a specific event by entering its unique identifier.
- By timeframe—Allows you to retrieve a set of events that occurred on or before a selected date and time.

Find Events by ID

To find events by ID:

Step 1 Use the procedure to Start the Event Log, page 4-2.

Step 2 Click the **Find Events By ID** button in the Event Log toolbar.

:

The Enter Event ID dialog box appears.

Step 3 Enter the unique identifier of the event in the Enter Event ID field.

Step 4 Click **OK**.

The event is retrieved and is displayed in the Event Log.

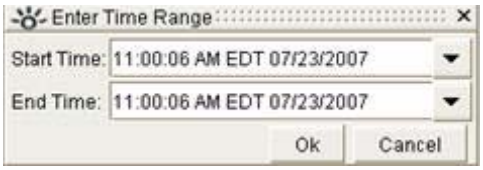
Find Events that Occurred in a Selected Timeframe

To find events that occurred in a selected timeframe:

Step 1 Use the procedure to Start the Event Log, page 4-2.

Step 2 Click the **Find Events By Time** button in the Event Log toolbar.

The Enter Time Range dialog box appears.



Step 3 Use the first drop-down menu to set the start date for the event timeframe. Select the month, day, and year.

Step 4 Use the second drop-down menu to set the end date for the event timeframe. Select the month, day, and year.

Step 5 Click **OK**.

The Event Log retrieves the set of events that occurred in the selected timeframe.

Filtering OSPF Events

You can refine the Event Log view to Filter OSPF events:

- Starting the Filter Wizard, page 4-16
- Choosing a Predefined Filter, page 4-18
- Customizing Filters, page 4-19
- Changing the Filter Name, page 4-19
- Saving the Filter, page 4-20
- OSPF Filtering Example, page 4-20

Starting the Filter Wizard

To start the filter wizard:

Step 1 Click the **Event Filter** icon in the Event Log Toolbar, page 4-38.

The Filter Events wizard appears (see Figure 4-9).

Figure 4-9 Enter Time and Router/Route Id Screen in OSPF Query Events Wizard

Step 2 In the Enter Time and Router/Route Id Constraints screen:

a. Select the radio button for the Type of OSPF events you want to query, either **Router Id** or **Route Id**.

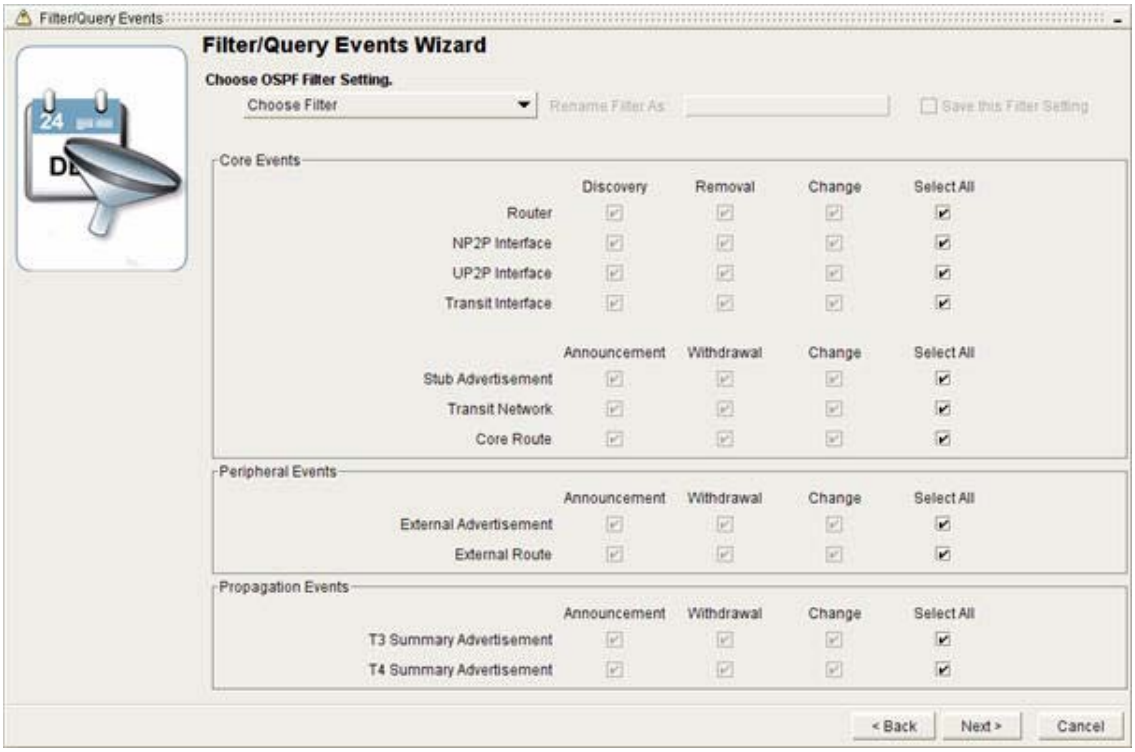
b. In the Router/Route Id field, enter the router or route ID you want to query.

c. If you want to filter in a specific period of time, check the **Please select to enter Time Constraints** checkbox, and enter a Start Time and End Time.

d. Click **Next**.

Step 3 Use the Filter Events wizard to filter the complete set of events, and select a specific set of events to display in the Event Log.

Figure 4-10 OSPF Filter Wizard



Choosing a Predefined Filter

To choose a predefined filter in the Choose Filter screen (see Figure 4-10):

Step 1 You can:

a. select a predefined filter by clicking the **Choose Filter** drop-down menu (See Figure 4-11),

or

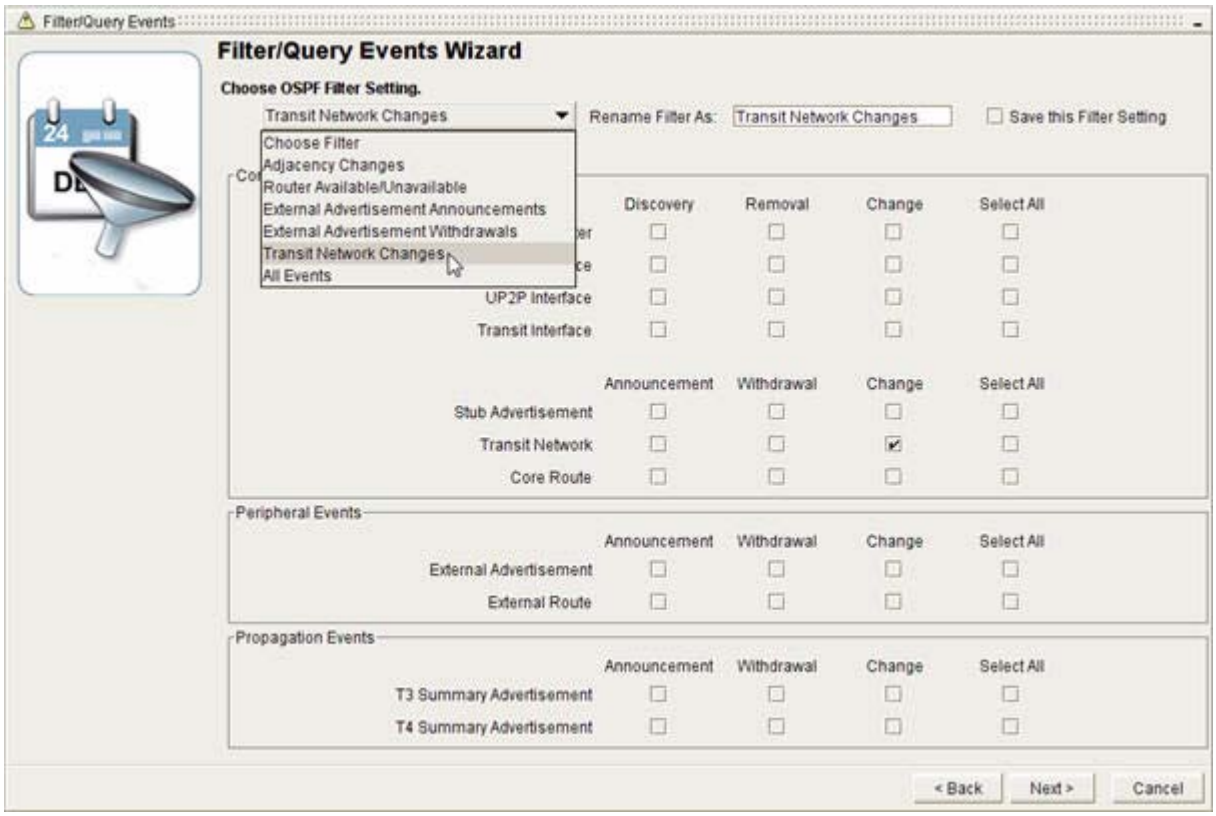
a. customize and save a filter to reuse it later. (See Customizing Filters, page 4-19.)

The predefined options are:

- **Adjacency Changes**—Returns events that describe the withdrawal of transit-to-router links, Numbered Point-to-Point (NP2P) interfaces, and Unnumbered Point-to-Point (UP2P) interfaces from your network.
- **Router Available/Unavailable**—Returns events that describe new router advertisements in and router withdrawals from your network.
- **External Advertisement Announcements**—Returns events that describe external route advertisements.
- **External Advertisement Withdrawals**—Returns events that describe withdrawals of external routes.
- **Transit Network Changes**—Returns events that describe changes to Transit networks.

– **All Events—**Returns all events for the current day.

Figure 4-11 OSPF Event Filter with Choose Filter Menu



Customizing Filters

OSPF Events are organized by type—Core, Propagation, Peripheral. For definitions of OSPF event types, see OSPF Event-Type Icons, page 4-6.

By default, all options in the dialog box are selected. A check mark is displayed in each corresponding check box to indicate the selection.

Once you select a filter, only the appropriate boxes for that filter will display a check mark.

You can customize your filter by deselecting options, such as advertisements, withdrawals, or changes that you do not want to display in the Event Log. Leave options checked for events you want to view.

For a particular network element, you can also select the **Select All** option to display all Advertisement, Withdrawal, or Change Events related to the selected router, route, or interface type.

Changing the Filter Name

The Rename File As box will display the filter name you have chosen. You can enter a new name if you wish, but it will overwrite the existing name in the **Choose OSPF Filter Setting** drop-down menu.

Saving the Filter

To save a customized Event Log filter:

Step 1 Click the **Save This Filter Setting** check box.

Step 2 Once you have finished selecting your filtering criteria, click **Next**.

Step 3 Click **Finish**.

The Event Log retrieves the set of events you have specified in the filter.

If you have elected to save a customized filter, its name will appear in the **Choose OSPF Filter Setting** drop-down menu for later reuse.

OSPF Filtering Example

To filter for all router events for the current day using a customized filter:

Step 1 Use the procedure to View OSPF Events, page 4-12.

Step 2 Click the **Event Filter** icon in the Event Log Toolbar, page 4-38.

The Filter/Query Events Wizard appears.

Step 3 Using the Choose OSPF Filter Settings drop-down menu, select **All Events Today**.

All the Core Events, Peripheral Events, and Propagation Events are selected by default.

Step 4 Filter out all events except Router Events, by clicking on **Select All** for all the other categories of event.

Check boxes are empty of check marks to indicate that they are deselected.

Step 5 Click **Next**.

Step 6 Click **Finish**.

All the router events for the day are displayed.

Filtering BGP Events

You can use the Event Filter to search for the following BGP events:

- IPV4 Unicast Events
- IPV4 Unicast Summary Events
- IPV4 VPN Events
- IPV4 Multicast Events

Select BGP Events to Filter

To select BGP events to filter:

Step 1 Use the procedure to Start the Event Log, page 4-2.

Step 2 Identify the AS you want to filter from the menu hierarchy, and select the category of events (unicast, unicast summary, VPN, or multicast).

BGP Filtering Example 1: IPv4 Unicast Events

This section shows a filtering example, using BGP IPv4 unicast events.

Starting the Filter Wizard

To start the filter wizard:

Step 1 Click the **Event Filter** icon in the Event Log Toolbar, page 4-38.

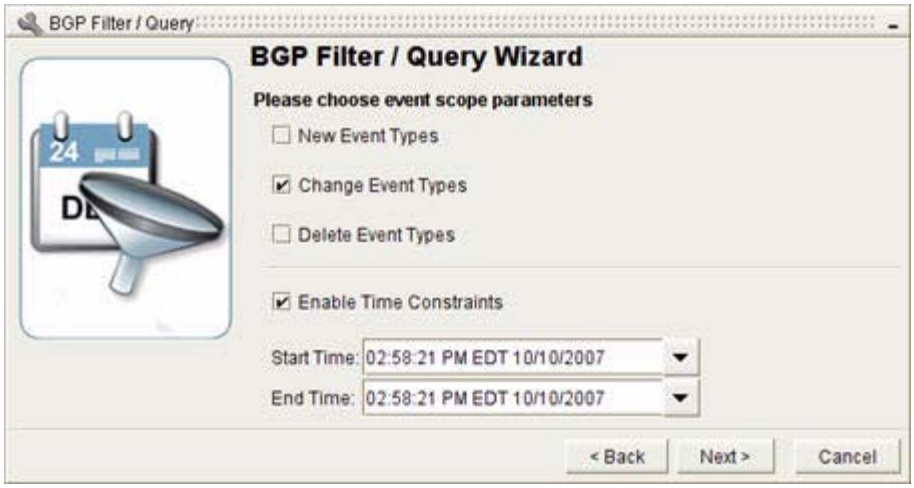
The Filter Events wizard opens and displays the Please Select a Domain and Name the Filter screen (see Figure 4-12).

Figure 4-12 Select a Domain and Name the Filter Screen in BGP Event Filter

Step 2 Enter the Filter Name and click **Next**. (The Select Your Domain field is completed automatically based on your selection from the menu hierarchy.)

The Please Choose Event Scope Parameters screen appears (see Figure 4-13).

Figure 4-13 Event Scope and Parameters Screen in BGP Event Filter



Choose Event Scope Parameters

To choose event scope parameters for your Event Log filter:

Step 1 Click the check box next to the event type(s) you want to filter.

Event types appear in the **Type** column of any BGP Events screen. They vary with the type of event you are filtering (unicast, unicast Summary, VPN, multicast).

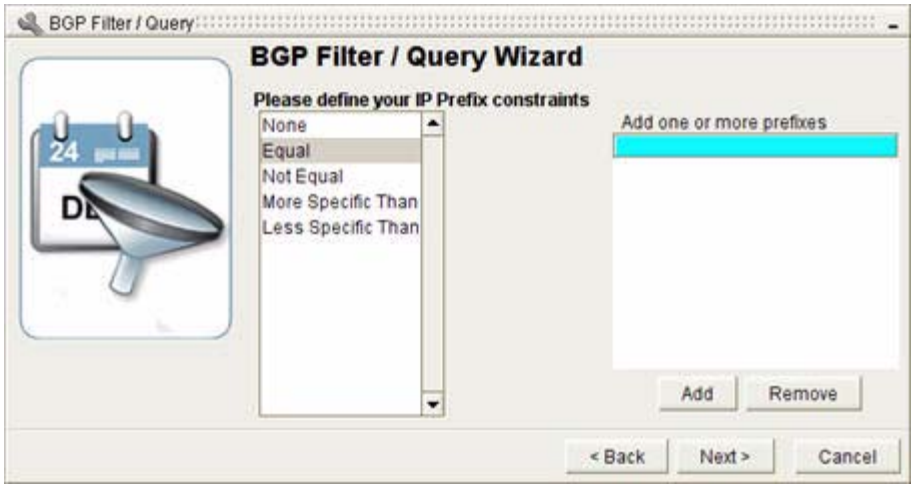
a. If you wish to search events within a specific time period, click the **Enable Time Constraints** check box and select the **Start Time** and **End Time** times and dates using the drop-down menu calendars.

b. If you wish to search the entire database, leave the **Enable Time Constraints** box unchecked.

Step 2 Click **Next**.

The Define Your IP Prefix Constraints screen appears (see Figure 4-14).

Figure 4-14 IP Prefix Constraints Screen in BGP Event Filter



Define IP Prefix Constraints

To define IP prefix constraints for your Event Log filter:

Step 1 Select one of the following options:

a. If you don't wish to filter by IP Prefix, select **None**.

or

a. If you wish to filter by IP Prefix you have the following choices:

- **Equal—**Will return all entries that contain the specified IP prefix(es).
- **Not Equal—**Will return all entries that do not contain the specified IP prefix(es).
- **More Specific Than—**Will return all entries that are more specific than the specified range.

  Example: If you enter 10:10 192.168.0.0/24, the filter might return values between 10:10 192.168.0.1 and 10:10 192.168.0.254, or any subnets of 10:10 192.168.0.0/ in the range /25 to /32).
- **Less Specific Than—**Will return all entries that are less specific than the specified range.

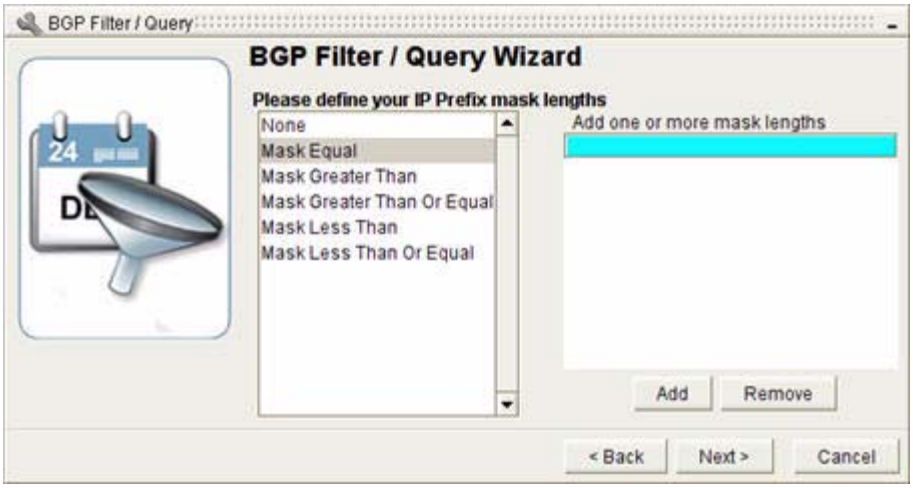
b. Select one of the listed options, enter one or more IP prefix(es), and click **Add**.

Note If you wish to remove a constraint you have entered in the BGP Event Filter, highlight the entry and click the **Remove** button.

Step 2 Click **Next**.

The Define Your IP Prefix Mask Lengths screen appears (see Figure 4-15).

Figure 4-15 IP Prefix Mask Lengths Screen in BGP Event Filter



Define IP Prefix Mask Lengths

To define IP prefix mask lengths for your Event Log filter:

Step 1 Select one of the following options:

a. If you don't wish to filter by Prefix Mask Length, select **None**.

or

a. If you wish to filter by Prefix Mask Length you have the following choices:

- **Mask Equal—**Will return all entries that contain the specified Prefix Mask Length(s).
- **Mask Greater Than—**Will return all entries that contain a value greater than the specified Prefix Mask Length(s).
- **Mask Greater Than/Equal—**Will return all entries that contain a value greater than or equal to the specified Prefix Mask Length(s).
- **Mask Less Than—**Will return all entries that contain a value less than the specified Prefix Mask Length(s).
- **Mask Less Than/Equal—**Will return all entries that contain a value less than or equal to the specified Prefix Mask Length(s).

b. Select one of these options, enter one or more Prefix Mask Length(s), and click **Add**.

Step 2 Click **Next**.

The Enter Router Constraints screen appears (see Figure 4-16).

Figure 4-16 Enter Router Constraints Screen in BGP Event Filter

Enter Router Constraints

To define router constraints for your Event Log filter:

Step 1 Select one of the following options:

a. If you don't wish to filter by Router ID, select **None**.

or

a. If you wish to filter by Router ID you have the following choices:

- **Equal—**Will return all entries that contain the specified Router ID(s).
- **Not Equal—**Will return all entries that do not contain the specified Router ID(s).

b. Select one of these options, enter one or more Router ID(s) or a range of Router IDs, and click **Add**.

Step 2 Click **Next**.

The Select Path Change Mask Constraints screen appears (see Figure 4-17).

Figure 4-17 Select Path Change Mask Constraints Screen in BGP Event Filter

Select Path Change Mask Constraints

To select path change mask constraints for your Event Log filter:

Step 1 If you want to filter for changes to any of the following, select the associated check box(es):

- AS Path
- Community
- Local Preference
- Multi-Exit Discriminator (MED)
- Next Hop
- Opaque
- Origin
- Route Target (RT)
- Site of Origin (SOO)
  - If you decided to filter only **Delete Event Types** on the Choose Event Scope and Parameters Screen, don't complete this screen.
  - If you decided to filter only **Change Event Types** on the Choose Event Scope and Parameters Screen, you can specify which types of change events on this screen. If you don't complete this screen, all types are filtered.
  - If you decided to filter only **New Event Types** on the Choose Event Scope and Parameters Screen, don't complete this screen.

Step 2 Click **Next**.

The Please Enter Tag Constraints screen appears (see Figure 4-18).

Figure 4-18 Enter Tag Constraints Screen in BGP Event Filter

Enter Tag Constraints

To enter tag constraints for your Event Log filter:

Step 1 Select one of the following options:

a. Select the BGP tag(s) you want to use in your search by clicking on it.Hold down the Control key to make multiple selections.

BGP tags will only appear in this screen if they have been imported previously. For more information, see , BGP Tagging, on page 6-1.

or

a. Don't enter any BGP tags.

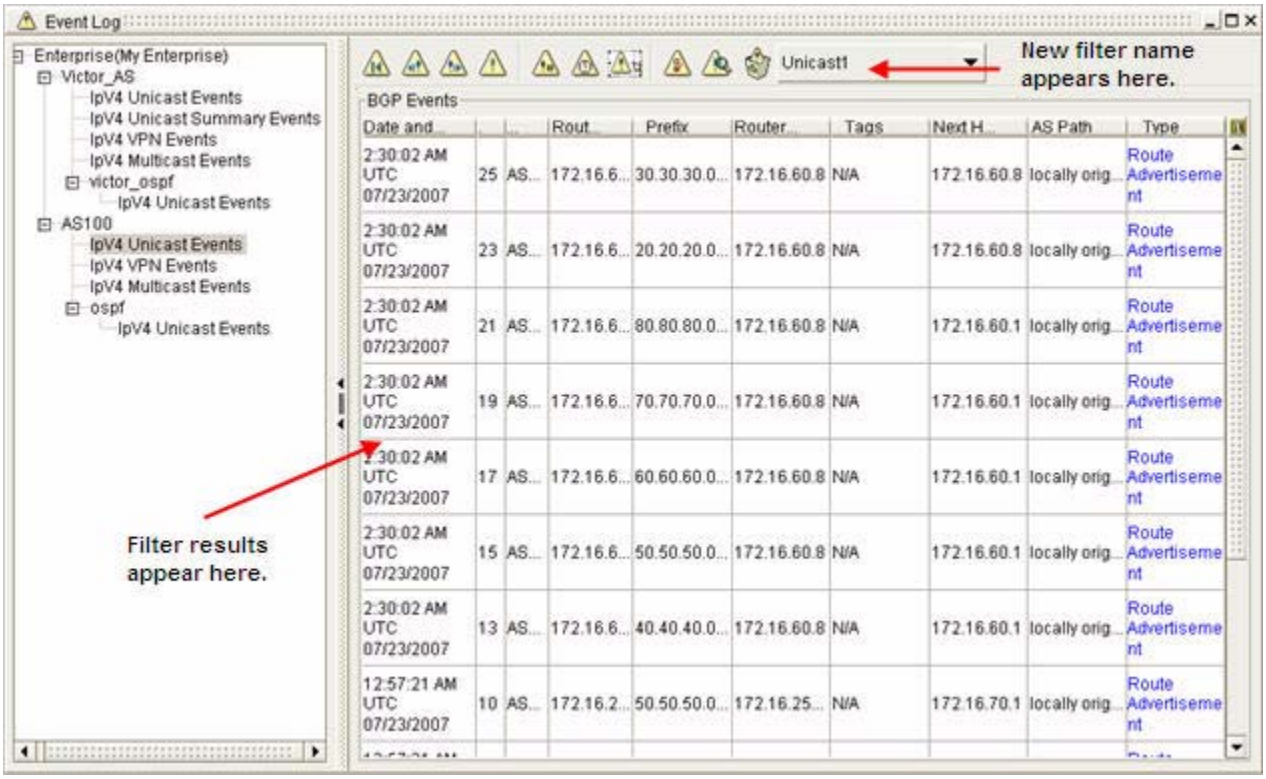
Step 2 Click **Next**.

Step 3 Click **Finish**.

The filter results are displayed and the new filter name is placed in the drop-down menu, so it can be used again when needed (see Figure 4-19).

If no results are found, you will receive a message: "There are no matching events for the applied filter."

Figure 4-19 Filter Results Page for BGP IPV4 Unicast Events



BGP Filtering Example 2: IPV4 VPN Events

A second example will show how the BGP filtering process works with VPNs.

Starting the Filter Wizard

To start the Event Log filter wizard:

Step 1 Click the **Event Filter** icon in the Event Log Toolbar, page 4-38.

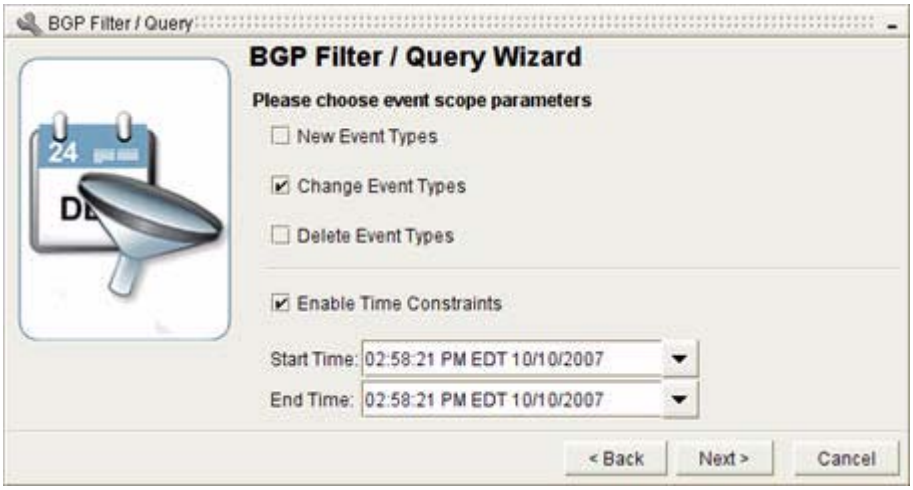
The Filter Events wizard opens and displays the Please Select a Domain and Name the Filter screen (see Figure 4-20).

Figure 4-20 Select a Domain and Name the Filter Screen in Event Filter

Step 2 Enter the Filter Name and click **Next**. (The Select Your Domain field is completed automatically based on your selection from the menu hierarchy.)

The Please Choose Event Scope Parameters screen appears (see Figure 4-21).

Figure 4-21 Choose Event Scope and Parameters Screen in Event Filter



Choose Event Scope Parameters

To choose event scope parameters for the Event Log filter wizard:

Step 1 Click the check box next to the event type(s) you want to filter. Event types appear in the **Type** column of any BGP Events screen. They vary with the type of event you are filtering (Unicast, Unicast Summary, VPN, Multicast)

a. If you wish to search events within a specific time period, click the **Enable Time Constraints** check box and select the **Start Time** and **End Time** times and dates using the drop-down menu calendars.

b. If you wish to search the entire database, leave the **Enable Time Constraints** box unchecked.

Step 2 Click **Next**.

The Please Enter VPN IP Prefix Constraints screen appears (see Figure 4-22).

Figure 4-22 VPN IP Constraints Screen in BGP Event Filter

Enter VPN IP Prefix Constraints

To enter VPN IP prefix constraints for the Event Log filter wizard:

Step 1 Select one of the following options:

a. If you don't wish to filter by VPN IP Prefix, select **None**.

or

a. If you wish to filter by VPN IP Prefix you have the following choices:

- **Equal—**Will return all entries that contain the specified VPN IP prefix(es).
- **Not Equal—**Will return all entries that do not contain the specified VPN IP prefix(es).
- **More Specific Than—**Will return all entries that are more specific than the specified range.

  Example: If you enter 10:10 192.168.0.0/24, the filter might return values between 10:10 192.168.0.1 and 10:10 192.168.0.254, or any subnets of 10:10 192.168.0.0/ in the range /25 to /32).
- **Less Specific Than—**Will return all entries that are less specific than the specified range.

b. Select one of these options, enter one or more VPN IP prefix(es), and click **Add**.

Step 2 Click **Next**.

The Enter VPN Prefix Mask Length Constraint screen appears (see Figure 4-23).

Enter VPN Prefix Mask Length Constraint

Figure 4-23 VPN Prefix Mask Length Constraint Screen in BGP Event Filter

To enter VPN prefix mask length constraints for the Event Log filter wizard:

Step 1 Select one of the following options:

a. If you don't wish to filter by VPN Prefix Mask Length, select **None**.

or

a. If you wish to filter by VPN Prefix Mask Length you have the following choices:
   - **Mask Equal—**Will return all entries that contain the specified VPN Prefix Mask Length(s).
   - **Mask Greater Than—**Will return all entries that contain a value greater than the specified VPN Prefix Mask Length(s).
   - **Mask Greater Than/Equal—**Will return all entries that contain a value greater than or equal to the specified VPN Prefix Mask Length(s).
   - **Mask Less Than—**Will return all entries that contain a value less than the specified VPN Prefix Mask Length(s).
   - **Mask Less Than/Equal—**Will return all entries that contain a value less than or equal to the specified VPN Prefix Mask Length(s).

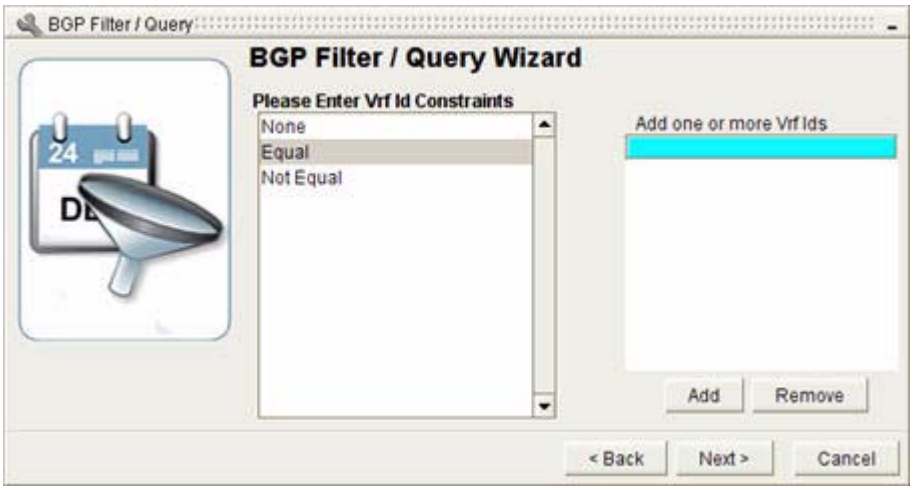
b. Select one of these options, enter one or more VPN Prefix Mask Length(s), and click **Add**.

Step 2 Click **Next**.

The Enter Vrf Id Constraints screen appears (see Figure 4-24).

Enter VRF ID Constraints

Figure 4-24 Enter Vrf Id Constraints Screen in BGP Event Filter



To enter VRF ID constraints for the Event Log filter wizard:

Step 1 Select one of the following options:

a. If you don't wish to filter by VRF ID, select **None**.

or

a. If you wish to filter by VRF ID you have the following choices:

- **Equal—**Will return all entries that contain the specified VRF ID(s).
- **Not Equal—**Will return all entries that do not contain the specified VRF ID(s).

b. Select one of these options, enter one or more VRF ID(s), and click **Add**.

Step 2 Click **Next**.

The Enter Local Vrf Id Constraints screen appears (see Figure 4-25).

Enter VRF ID Constraints

Figure 4-25 Local Vrf Id Constraints Screen in BGP Event Filter

To enter VRF ID constraints for the Event Log filter wizard:

Step 1 Select one of the following options:

a. If you don't wish to filter by Local VRF ID, select **None**.

or

a. If you wish to filter by Local VRF ID you have the following choices:

- **Equal—**Will return all entries that contain the specified VRF ID(s).
- **Not Equal—**Will return all entries that do not contain the specified VRF ID(s).

b. Select one of these options, enter one or more Local VRF ID(s), and click **Add**.

Step 2 Click **Next**.

The Select Path Change Mask Constraints screen appears (see Figure 4-26).

Select Path Change Mask Constraints

Figure 4-26 Select Path Change Mask Constraints Screen in BGP Event Filter

To enter path change mask constraints for the Event Log filter wizard:

Step 1 If you want to filter for changes to any of the following, select the associated check box(es):

- AS Path
- Community
- Local Preference
- Multi-Exit Discriminator (MED)
- Next Hop
- Opaque
- Origin
- Route Target (RT)
- Site of Origin (SOO)
  - If you decided to filter only Delete Event Types on the Choose Event Scope and Parameters Screen, don't complete this screen.
  - If you decided to filter only Change Event Types on the Choose Event Scope and Parameters Screen, you can specify which types of change events on this screen. If you don't complete this screen, all types are then filtered.
  - If you decided to filter only New Event Types on the Choose Event Scope and Parameters Screen, don't complete this screen.

Step 2 Click **Next**.

The Please Enter Tag Constraints screen appears (see Figure 4-27).

Enter Tag Constraints

Figure 4-27 Enter Tag Constraints Screen in BGP Event Filter

To enter tag constraints for the Event Log filter wizard:

Step 1 Select one of the following options:

a. Select the BGP tag(s) you want to use in your search by clicking on it.Hold down the Control key to make multiple selections.

BGP tags will only appear in this screen if they have been imported previously. For more information, see Working with BGP Tags, page 6-9.

or

a. Don't enter any BGP tags.

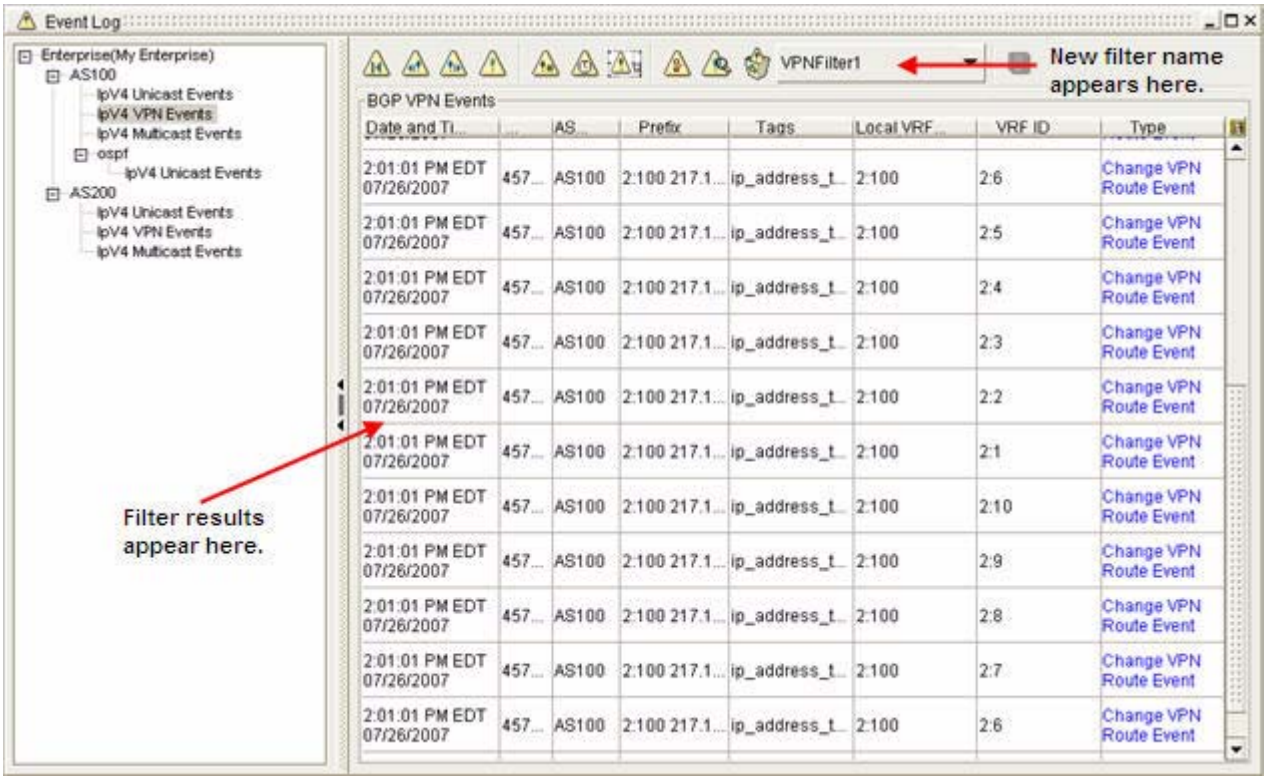
Step 2 Click **Next**.

Step 3 Click **Finish**.

The filter results appear and the new filter name is placed in the drop-down menu, so it can be used again when needed (see Figure 4-28).

If no results are found, you will receive a message: "There are no matching events for the applied filter."

Figure 4-28 BGP Event Filter Results Page



Working with Filters

Once you have created a filter, you can perform the following tasks:

- Apply a Filter, page 4-36
- Edit a Filter, page 4-37
- Remove a Filter, page 4-37

Apply a Filter

To apply a filter to the Event Log:

Step 1 Use the procedure to Start the Event Log, page 4-2.

Step 2 Identify the AS from the menu hierarchy, and select the category of events you want to filter.

Step 3 Select the filter you wish to apply from the drop-down menu in the Event Log toolbar.

The filter results appear.

Edit a Filter

To edit a filter for the Event Log:

Step 1 Use the procedure to Start the Event Log, page 4-2.

Step 2 Identify the AS from the menu hierarchy, and select the category of events you want to filter.

Step 3 Select the filter you wish to edit from the drop-down menu in the Event Log toolbar.

The filter results appear.

Step 4 Click the **Edit Current Event Filter** button in the Event Log toolbar.

The Filter Wizard opens for the filter you have selected.

Step 5 Change the name of the filter so that you can save it once you have made changes.

Step 6 Use the **Next** button to navigate through the pages of the wizard making changes where you wish.

Step 7 Click **Finish** when you are done.

The filter results appear and the new filter name is placed in the drop-down menu, so it can be used again when needed.

If no results are found, you will receive a message: “There are no matching events for the applied filter.”

Remove a Filter

To remove a filter from the Event Log:

Step 1 Use the procedure to Start the Event Log, page 4-2.

Step 2 Identify the AS from the menu hierarchy, and select the category of events you want to filter.

Step 3 Select the filter you wish to remove from the drop-down menu in the Event Log toolbar.

Step 4 Click the **Delete the Current Event Filter** button in the Event Log toolbar.

The filter is deleted.

Related Forms

The following tables detail the graphical elements and dialog boxes of the Event Log.

Event Log Toolbar

Table 4-1 describes buttons available on the toolbar in the Real-time Event Logs.

Table 4-1 Event Log Toolbar

Button	Name	Description
	Show Oldest	Returns the Event Log to the beginning of the event list. See View the Beginning of the Event Log, page 4-14.
	Step Back	Interrupts dynamic updating and sets the Event Log to Browse Mode, allowing you to browse backward through the list of events. See Browse Backward through Events, page 4-13.
	Step Forward	Interrupts dynamic updating and sets the Event Log to Browse Mode, allowing you to browse forward through the list of events. See Browse Forward through Events, page 4-13.
	Show Current	Interrupts Browse Mode and restores dynamic updating. Updates the list of events to show the most recent events. **Note:** The Event Log dynamically receives updates as events happen. See Refresh the Event Log, page 4-14.
	Find Events By ID	Opens the Enter ID dialog box, in which you can query for events by event number. See Find Events by ID, page 4-15.
	Find Events By Time	Opens the Enter Time dialog box, in which you can query for events that occurred before a selected start and end time. See Find Events that Occurred in a Selected Timeframe, page 4-15.
	Enter Number of Events to Display	Opens the Enter Number of Events dialog box, in which you can change the size of the viewing area for events. See Change the Number of Events Displayed, page 4-14.

Table 4-1 Event Log Toolbar (continued)

Button	Name	Description
	Filter Events Using Wizard	Starts the Filter Events Wizard, in which you can filter OSPF or BGP events using a predefined or customized set of filters. See Filtering OSPF Events, page 4-16 and Filtering BGP Events, page 4-20.
	Edit an Existing Event Filter	Opens an existing filter so you can edit and save it under another name. See Edit a Filter, page 4-37.
	Delete the Current Event Filter	Deletes a selected filter from the Filter Name drop-down Menu. See Remove a Filter, page 4-37.
 Filter drop-down Menu		Lists all of your saved filters.

CHAPTER 5

Monitoring Network Activity

Viewing Network Activity and Projecting Trends

The Event Monitor provides a view of network activity compared to a mean average amount of activity over a selected period of time.

- Monitoring network activity within a selected timeframe allows you to locate periods of frequent, unexpected activity.
- Monitoring activity over an extended period assists in predicting network behavior and projecting future trends.

  For example, you can leave Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) running overnight, then start the Event Monitor in the morning to view network activity; or run the Event Monitor at intervals to obtain an ongoing view of activity.

Spikes in activity indicate routing changes that occurred in your network during the selected period of time. You can view this information as normalized data, use the T-Score setting to view deviations, or view a Gaussian or Poisson distribution of the data.

View Most Active Routers

Event Monitor shows the most active routers in your network, which can help you to pinpoint issues that result in performance degradation or failure. Identifying routers that experience unexpected amounts of activity can help you to correct problems and optimize network performance.

Use Event Monitor with Event Log

Determine the date and time of a period of high activity by analyzing spikes in network activity with Event Monitor. You can right-click a graph of network activity and pivot directly to an OSPF or BGP Event Log, which displays related events. For information about the Event Log, see Chapter 4, “Monitoring Changes in Routing”.

Event Monitor Tasks

- Start the Event Monitor, page 5-2.
- Viewing Network Activity, page 5-2.

- Graph Network Activity, page 5-12.
- View Most Active Routers, page 5-1.

Viewing OSPF Convergence Activity

The OSPF Event Log is a Web-based tool that provides real-time and historical views of LSAs between Path Analyzer Listeners.

OSPF Convergence Log Tasks

- Open the OSPF Convergence Log, page 5-14.
- OSPF Convergence Analysis Screen, page 5-15.
- LSA Activity Screen, page 5-16.

Start the Event Monitor

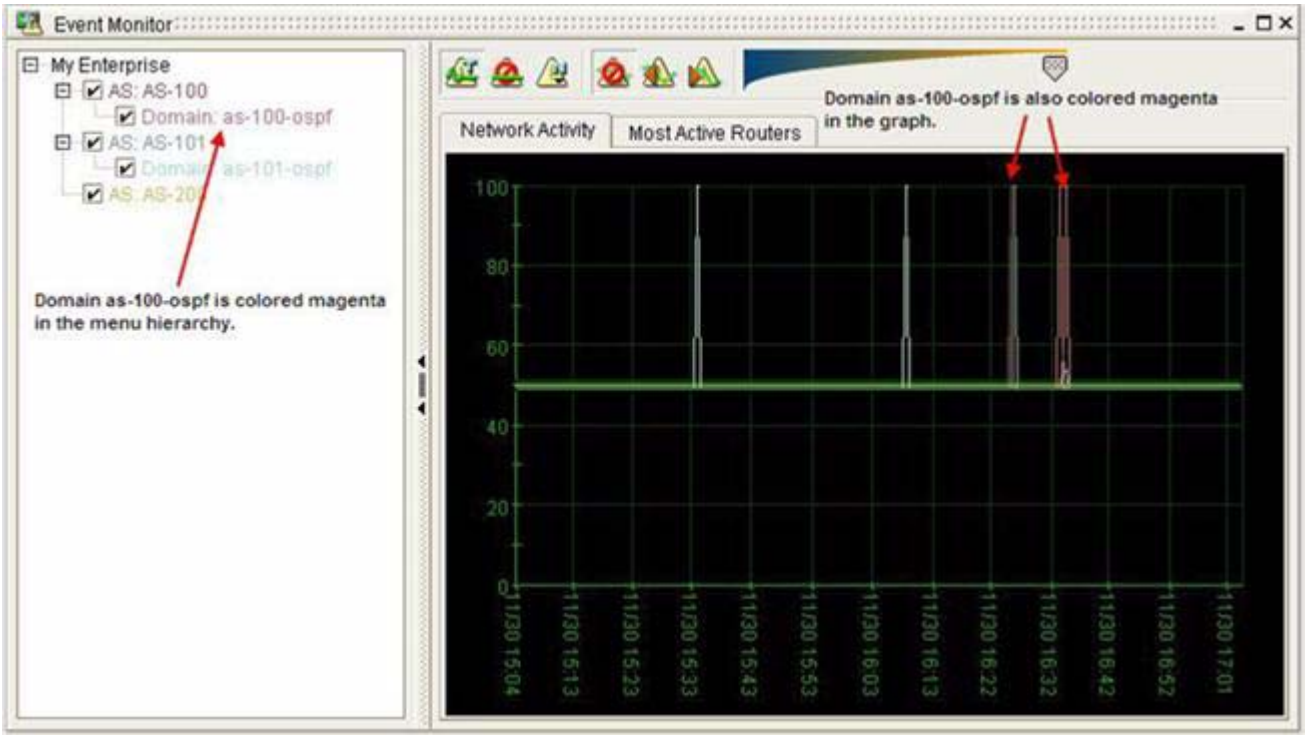
To start the Event Monitor from the Path Analyzer taskbar, click **Start > Event Monitor**.

The Event Monitor window appears. From the Event Monitor toolbar, you can control the display of data. For information about the toolbar, see The OSPF Convergence Log, page 5-14.

Viewing Network Activity

The Event Monitor shows the level of activity that occurs on your network in autonomous systems instrumented with Path Analyzer. Each color-coded autonomous system, listed hierarchically at the left side of the Event Monitor window, corresponds to the line of the same color depicted in the graph at the right side of the window (see Figure 5-1).

Figure 5-1 Activity of an Area, Shown in Event Monitor



Set Data Normalization

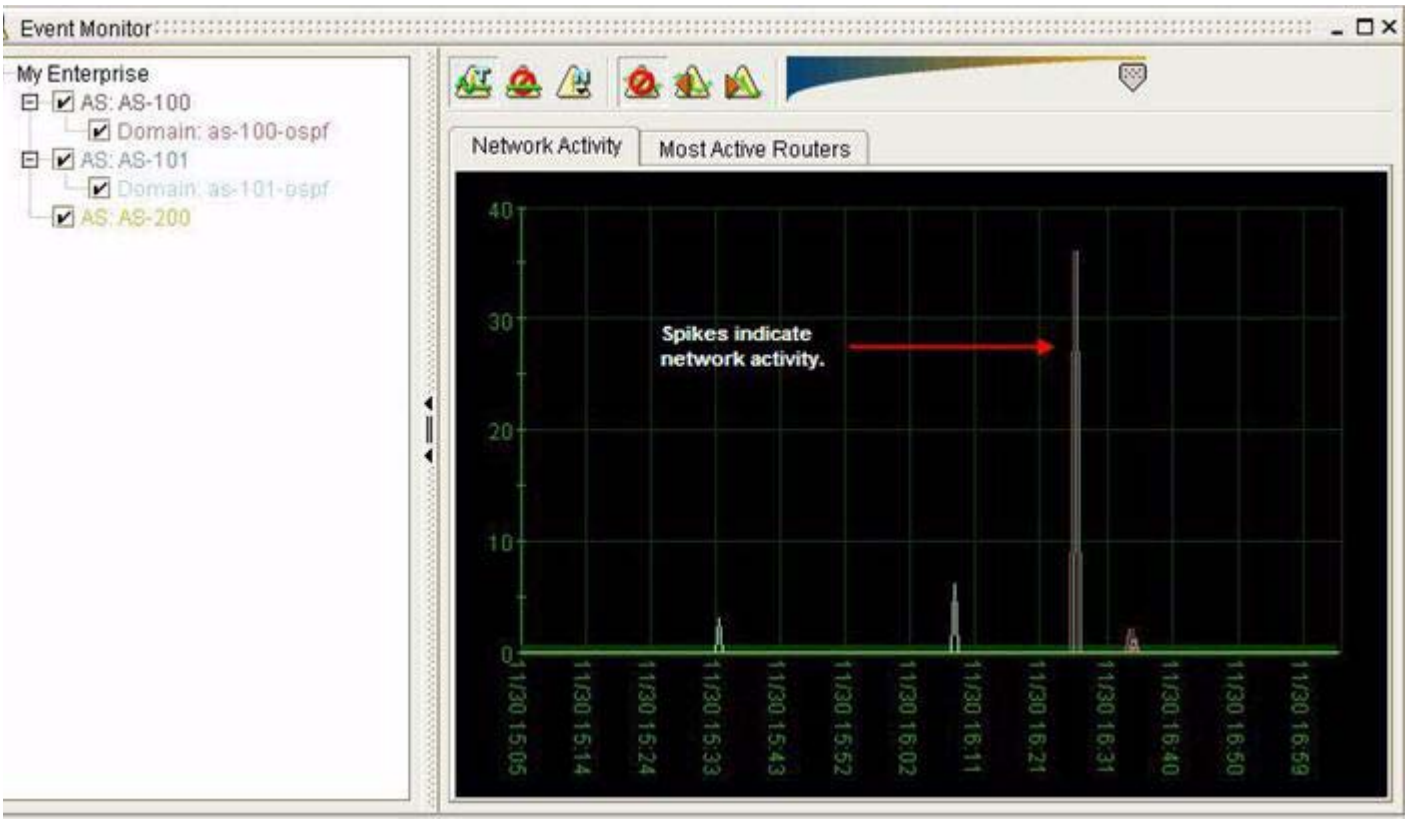
Event Monitor supports the following types of data normalization:

- Raw Data Without Normalization, page 5-3.
- T-Score Normalization, page 5-4.
- Binomial Distributions, page 5-6.
  - Gaussian Distribution, page 5-6.
  - Poisson Distribution, page 5-7.

Raw Data Without Normalization

In a graph of raw data without applied normalization or smoothing, the X-axis shows divisions in the selected period of time. The Y-axis shows the actual measure of activity that occurred in the selected period of time. No mean values are presented (see Figure 5-2).

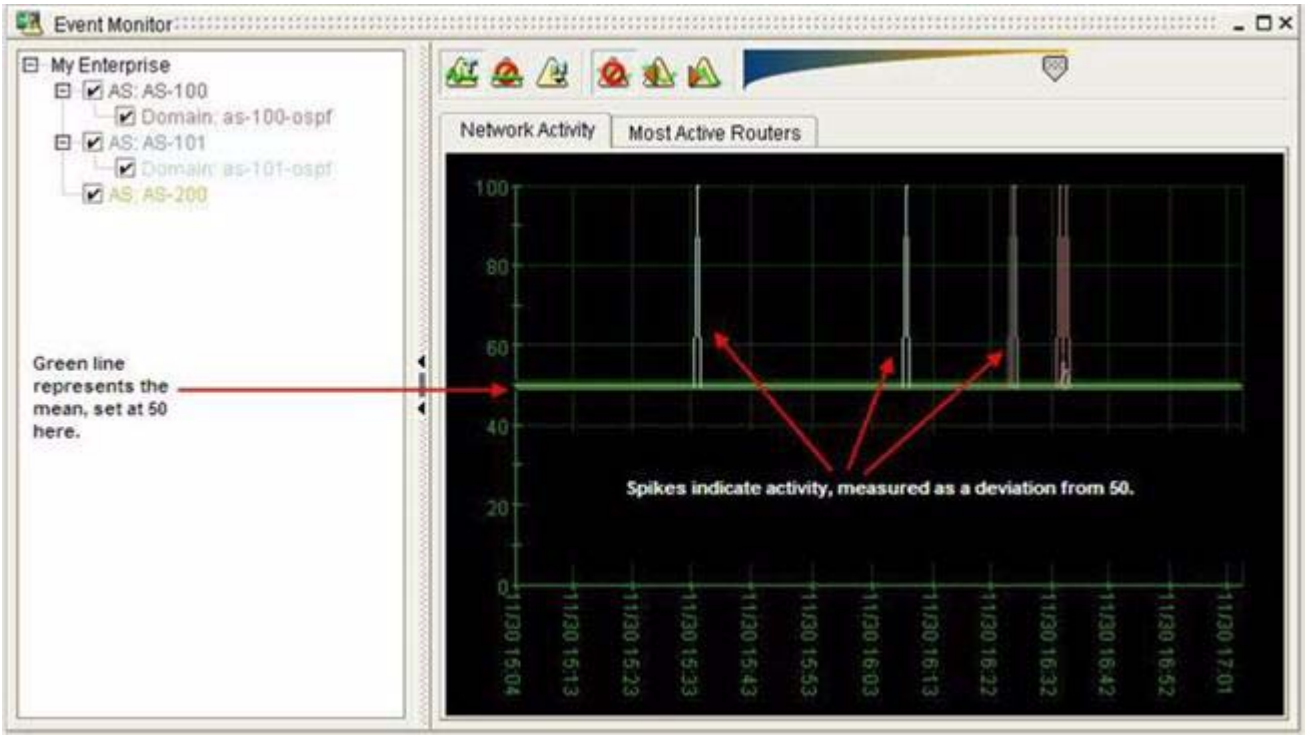
Figure 5-2 Activity in Raw Data



T-Score Normalization

The T-Score graph shows the number of standard deviations above or below the mean value of network activity. The Y-axis is set between 0 and 100 with the thick, green line centered at the mean, 50. Spikes of network activity measured against the Y-axis show the number of standard deviations above or below the norm value (see Figure 5-3).

Figure 5-3 Mean Activity in Graph Showing T-Score



T-Score

T-Score is calculated using the following formula, which shows the range of deviation from the mean in a sample of data:

$T\_1 = 50 + 10(x\_1 - x\_mean) / x\_var$

where

x_1 = the number of time delimiters, or buckets into which your data is divided; for example, you can have 2 days of data divided into 576 bins of 5 minutes each, resulting in a range from *x_1* to *x_576* in which *x_1* is the oldest sample.

x_mean = the average of all components in the sample.

x_var = the variance of the sample from the average.

Consequently, a T-Score of 50 is the average—represented as the thick, green line at the 50 point in the graph—and every 10 points above or below the line is a standard deviation away from the average value.

A simplified way to interpret data presented as T-Scores is:

- **0-39—**Little activity is occurring on your network. What could cause a cessation of network activity? Did a network device become unavailable?
- **40-59—**Average network activity.
- **60-79—**More activity than normal occurs on the network, possibly requiring investigation.
- **80+**—Much more activity than normal occurs on the network, requiring investigation.

Binomial Distributions

The Event Monitor generates graphs of data based on binomial distribution functions, equations that specify the number of times an event can occur in a set of independent trials, from 1 to infinity, measured against the probability of an event occurring in a single, independent trial.

The Event Monitor supports two types of binomial distributions for modeling data:

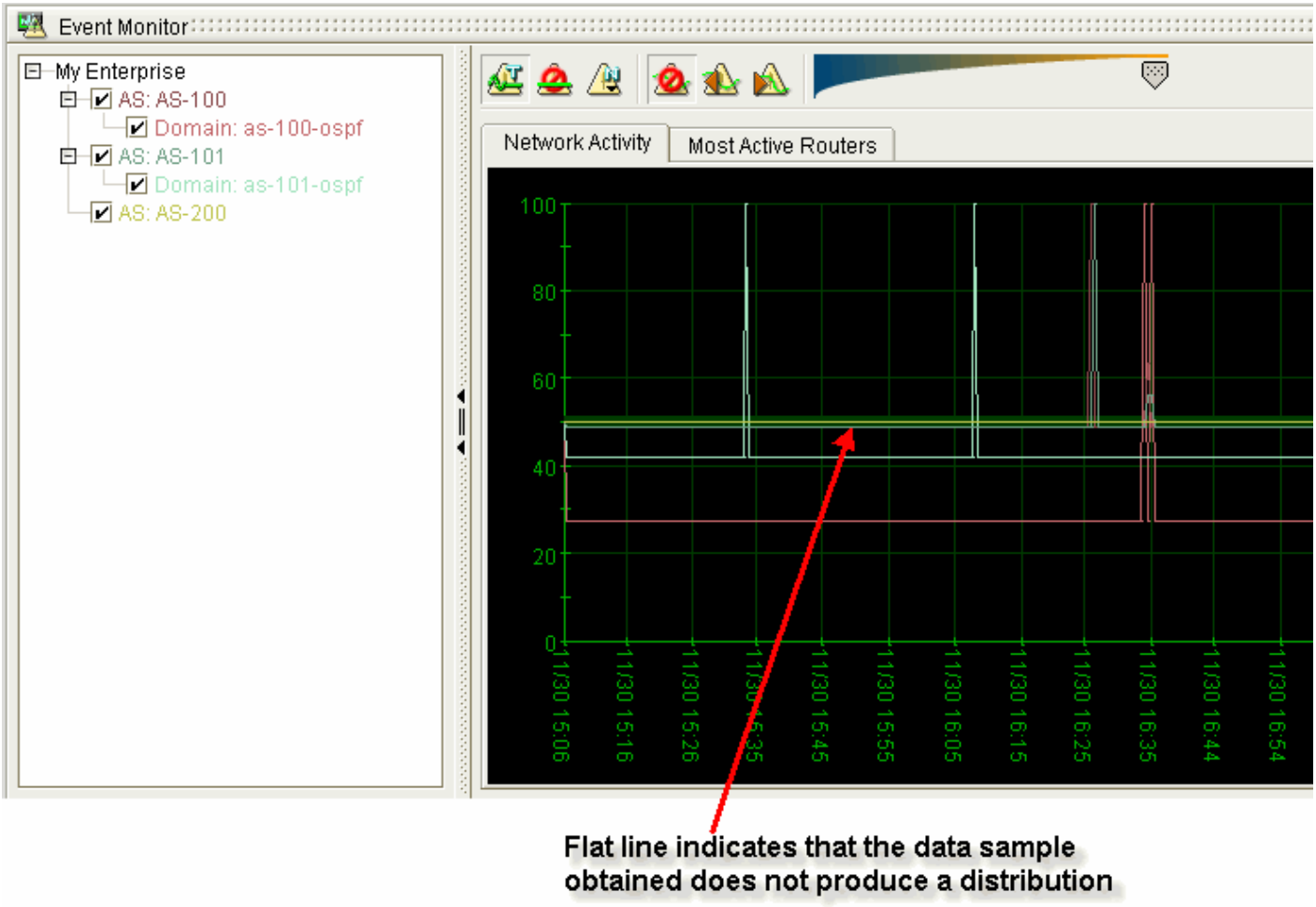
- Gaussian Distribution, page 5-6—Used to model data in instances where the number of events that occur is very large.
- Poisson Distribution, page 5-7—Used to model data in instances where the probability that an event will occur during the designated period of time is very small.

Gaussian Distribution

The Gaussian distribution, also referred to as the normal distribution or the bell-shaped curve, is used to model systems in which a very large number of events occur.

For a large routing domain, in which tens of thousands of events can occur every 30 seconds, use the Gaussian distribution to model data (see Figure 5-4).

Figure 5-4 Gaussian Distribution, Normalized Data



Poisson Distribution

The Poisson distribution is generally used to model systems in which the probability that an event will occur is low, but where the number of opportunities for the event to occur is high. (See the Poisson Distribution Graph on page 5-8.)

For example, use the Poisson distribution to model data for a highly redundant network that carries data over a finite set of same-cost paths (for example, three main paths that all have the same cost). In this case, the probability of a failover on one of the links in a 30 second period is very low within the number of opportunities for the event to occur.

Modeling data with the Poisson distribution is appropriate when:

- Data points are total counts of events.
- Each event has a binary set of attributes. (For example, a router can be available or unavailable; a service path can conform to an engineered baseline or can deviate from its baseline.)

  and

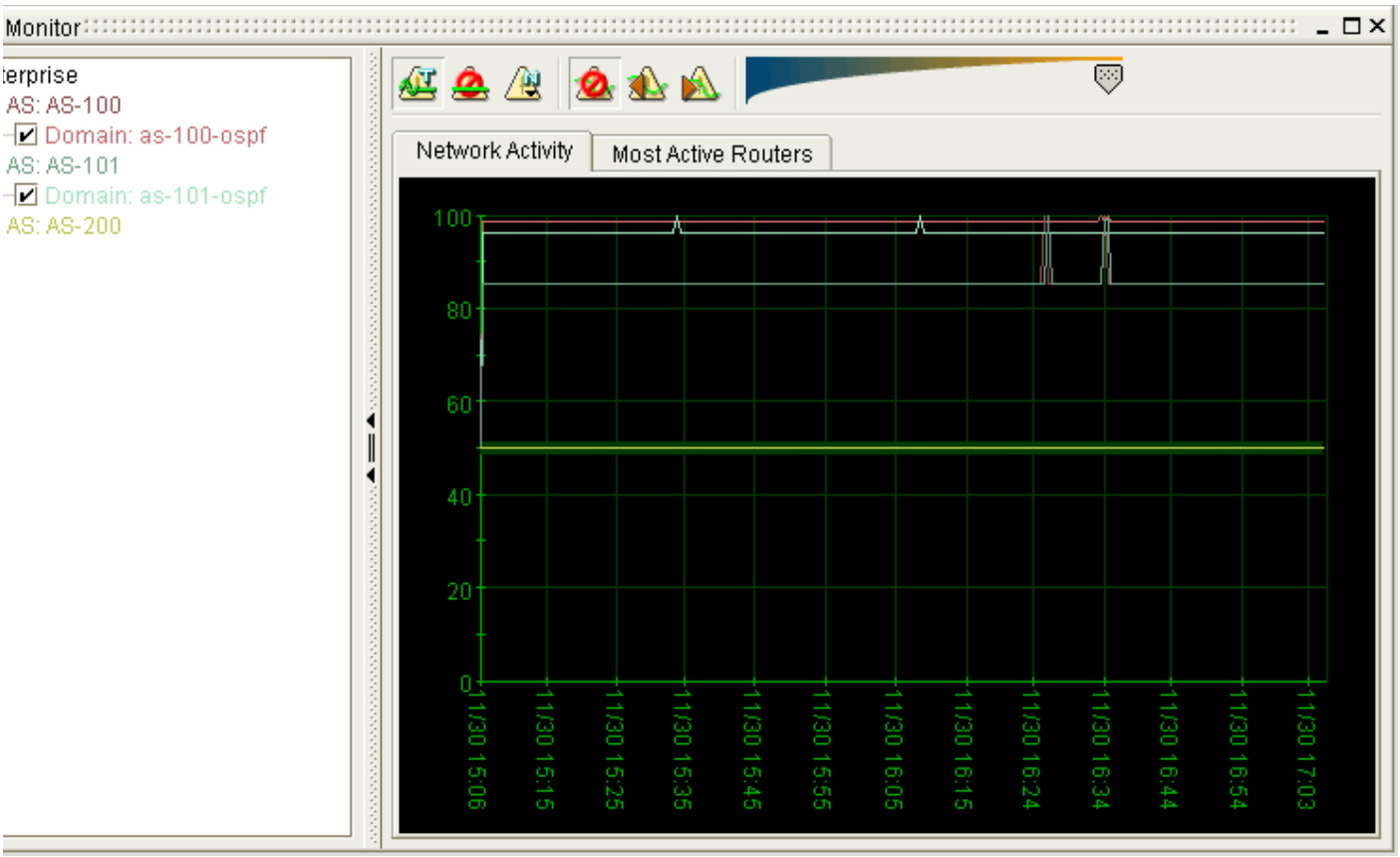
  One attribute is less likely to occur than the other. (For example, a router interface is more likely to be available—correctly configured—than unavailable—misconfigured.)
- Variance = mean.
- Sampling occurs randomly.
- Events are distributed randomly.

In Event Monitor, the Poisson graph shows the distribution of the number of times a rare event occurs on your network (see Figure 5-5).

For example, in a small network with one or two routers, the probability that routing will be interrupted due to a misconfigured cost metric on a router interface is logarithmically less likely than in a large, enterprise network. A small network has minimal probability but many opportunities for misconfigurations.

As a network grows in size and the number of routers increase, the probability of misconfigurations grows exponentially. Network size correlates directly with the number of probable misconfigurations.

Figure 5-5 Poisson Distribution Graph



Exponential Smoothing of Data

Exponential smoothing assists in making accurate predictions of future activity. Applying exponential smoothing to your normalized, T-Score, or Poisson activity graphs allows you to view your data with a preference for current or past events.

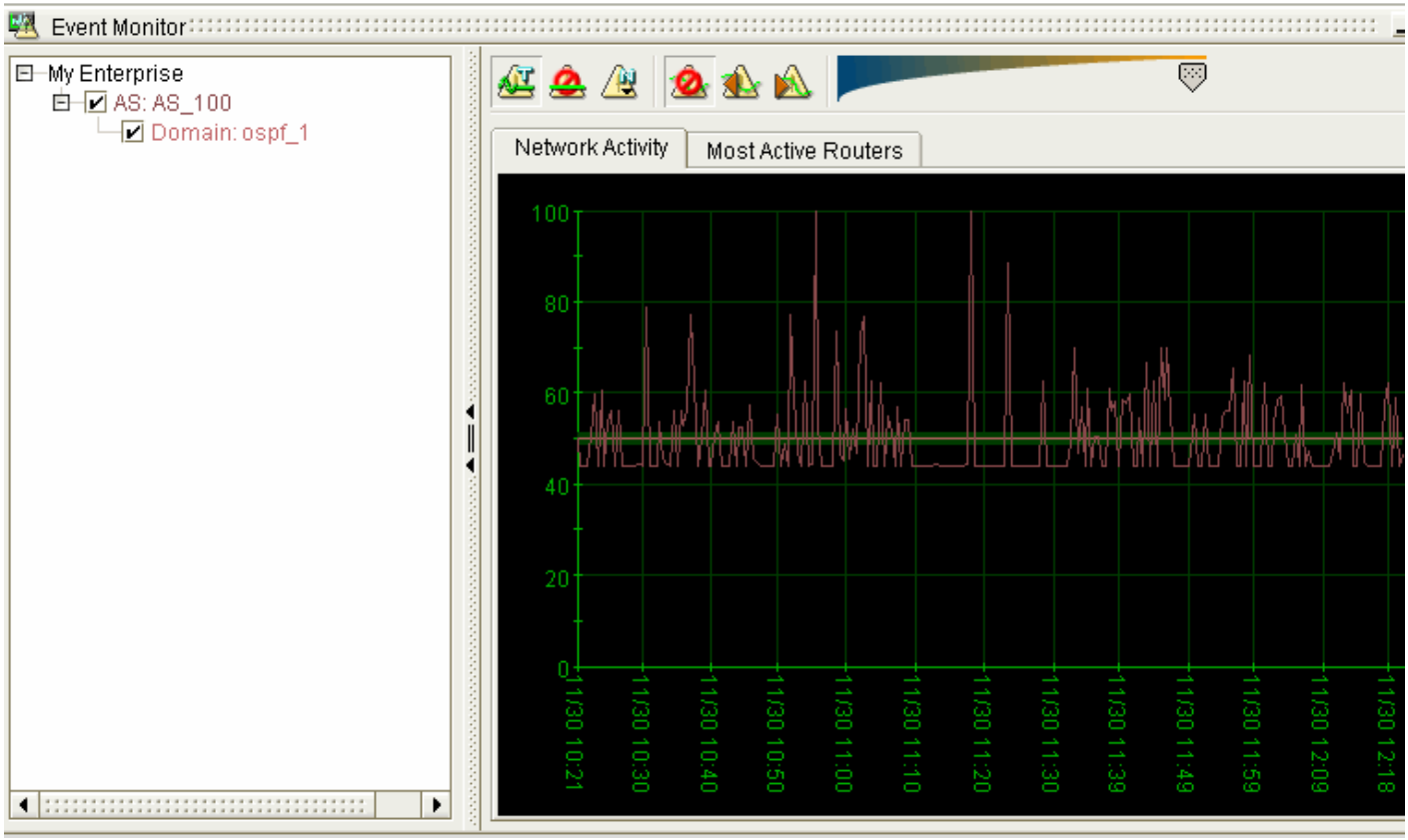
Path Analyzer supports the following options for exponential smoothing:

- No Smoothing, page 5-8.
- Exponential Smoothing to Present, page 5-9.
- Exponential Smoothing to Past, page 5-10.

No Smoothing

Without data smoothing, equal weight is given to present and past events. The time and date that an event occurs has no effect on the presentation of the data (see Figure 5-6).

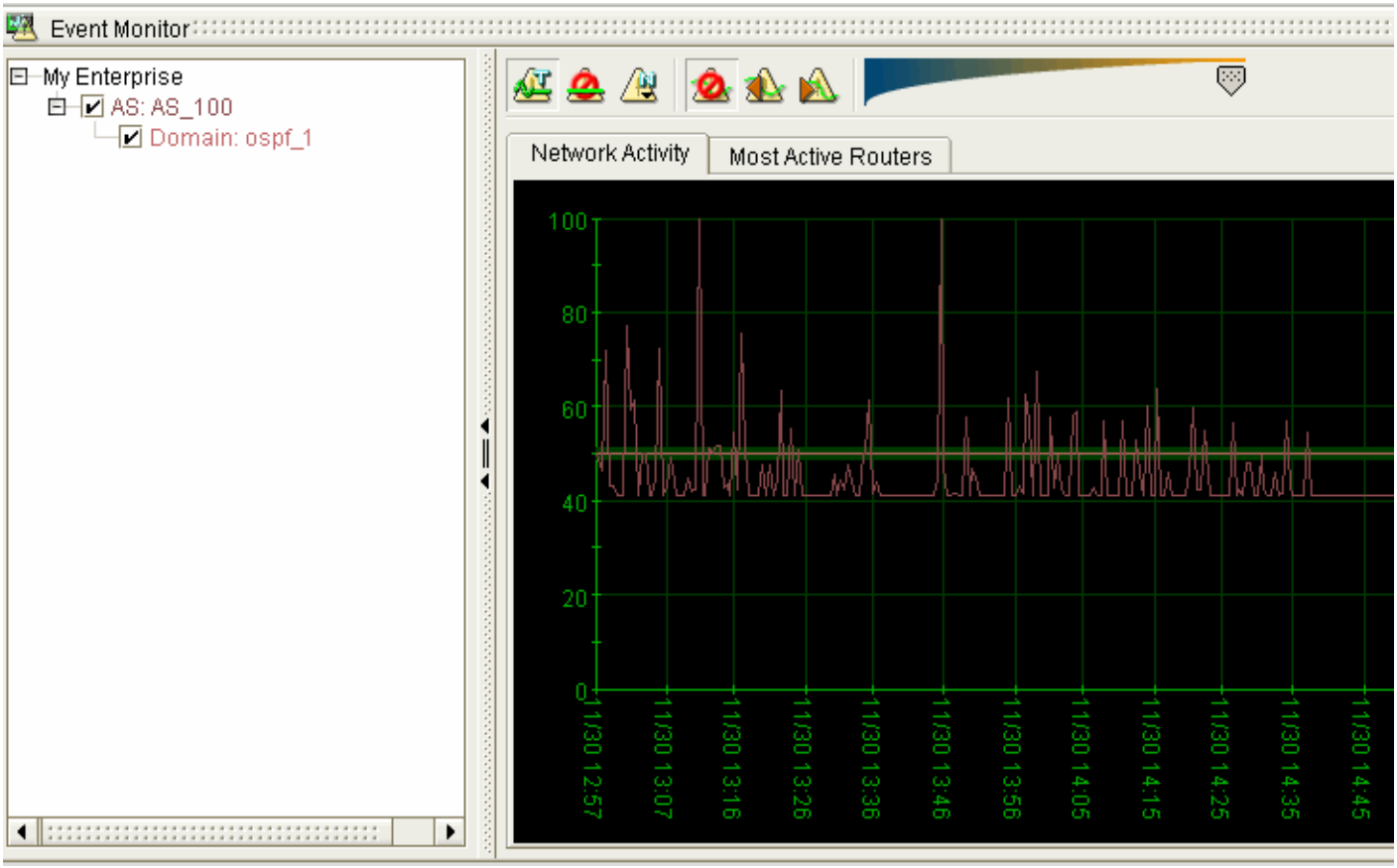
Figure 5-6 T-Score Graph Without Data Smoothing



Exponential Smoothing to Present

Figure 5-7 shows a T-Score graph with Exponential Smoothing to Present. The most recent set of events has greater weight in determining future levels of network activity.

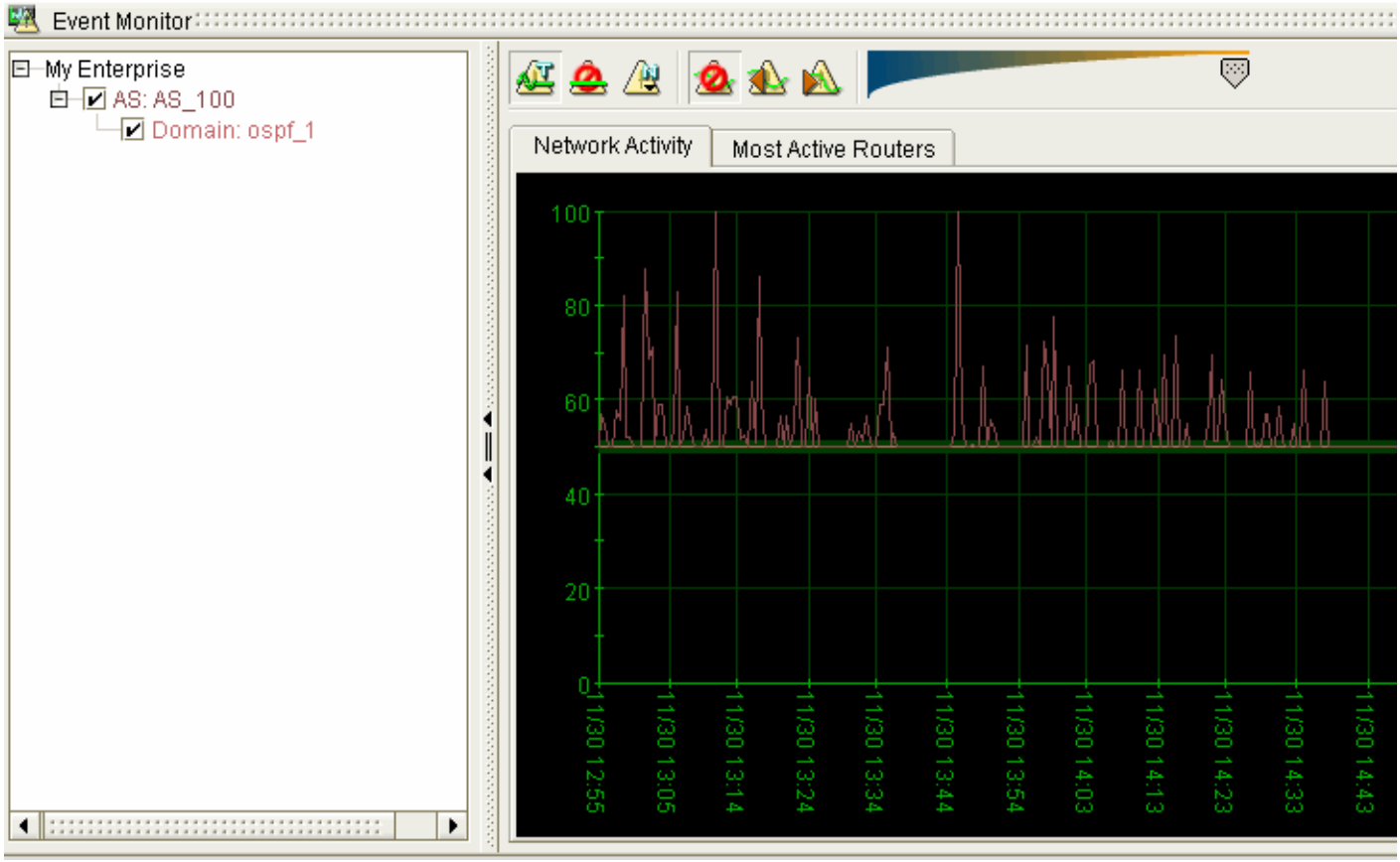
Figure 5-7 T-Score Graph, Exponential Smoothing to Present



Exponential Smoothing to Past

Figure 5-8 shows the same T-score graph with Exponential Smoothing to Past. Historical events have greater weight in determining future levels of network activity.

Figure 5-8 T-Score Graph, Exponential Smoothing to Past



Event Monitor Toolbar

Table 5-1 describes buttons available on the toolbar in the Event Monitor.

Table 5-1 Event Monitor Toolbar

Button	Name	Description
	T-Score Normalization	Plots network activity as a T-Score, showing network activity as the number of standard deviations from the norm, which is set at 50.
	No Normalization	Plots network activity as raw data, enabling you to identify the mean amount of network activity and actual values.

Table 5-1 Event Monitor Toolbar (continued)

Button	Name	Description
	Other Normalization	Plots network activity as one of the following binomial distributions: **Poisson**—Plots network activity as a Poisson distribution. **Gaussian**—Plots network activity as a Gaussian distribution.
	No Smoothing	Plots data with an equal emphasis on all events in the time period.
	Exponential to Present Smoothing	Plots data with a preference for most recent events.
	Exponential to Past Smoothing	Plots data with a preference for least recent events.
	Time Increment Slider	Changes the span and granularity of the time increments displayed on the X-axis. Ranges from 6 1/2 hour increments (left) to 6 1/2 minute increments (right), approximately.

Graph Network Activity

To graph network activity in the Event Monitor:

Step 1 Use the procedure to Start the Event Monitor, page 5-2.

Step 2 Select one of the following options for data normalization from the Event Monitor toolbar:

- **T-Score**—Plots network activity as a T-Score, showing the number of standard deviations of network activity from the norm.
- **None**—Plots network activity as raw data, enabling you to identify the mean amount of network activity and actual values.
- **Other—**Lists options for binomial distributions. Select one of the following:
  - **Poisson**—Plots network activity as a Poisson distribution.
  - **Gaussian—**Plots network activity as a Gaussian distribution.

Step 3 Select one of the following options for exponential smoothing from the Event Monitor toolbar:

- **No Smoothing—**Plots data with an equal emphasis on all events in the timeframe.
- **Exponential Smoothing to Past—**Plots data with a preference for least recent events.
- **Exponential Smoothing to Present—**Plots data with a preference for most recent events.

Step 4 Drag the slider in the Event Monitor toolbar to select the measure of activity to be displayed in the graph. As you drag the slider to the right, the increments of data on the X-axis increase.

The data is plotted on the graph according to your selections.

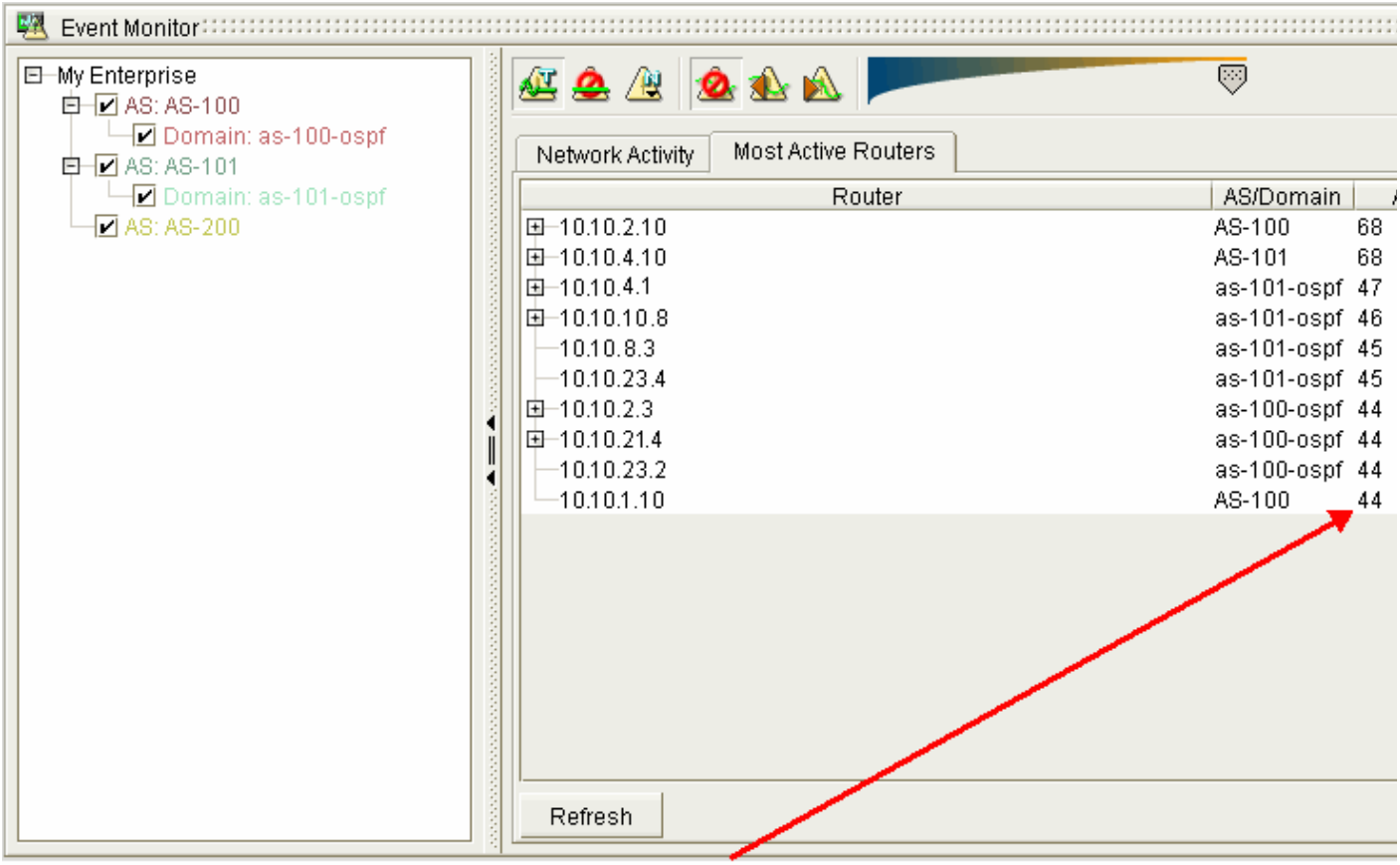
View the Most Active Routers in a Domain

To view the most active routers in a domain:

Step 1 Use the procedure to Start the Event Monitor, page 5-2.

Step 2 Select the **Most Active Routers** tab (see Figure 5-9).

Figure 5-9 Most Active Routers Tab



Step 3 Click the **Refresh** button to update the display for a real-time view of the most active routers.

The OSPF Convergence Log

The OSPF Convergence Log enables you to see how efficiently routing information is being propagated throughout your network. The OSPF Convergence Log presents the time it take for LSAs to propagate from one Listener to another within a given area. Slow propagation times may indicate delayed OSPF Convergence. Convergence is required before OSPF can properly route packets.

In order to view OSPF convergence activity, you must first administer the feature. See Reconfiguring a Path Analyzer Server in Chapter 3: Configuring the Path Analyzer Server in the *Cisco Service Path Analyzer Administration Guide.*

Open the OSPF Convergence Log

To open the OSPF Convergence Log:

Step 1 Open your Web browser and enter the IP address of your Path Analyzer server.

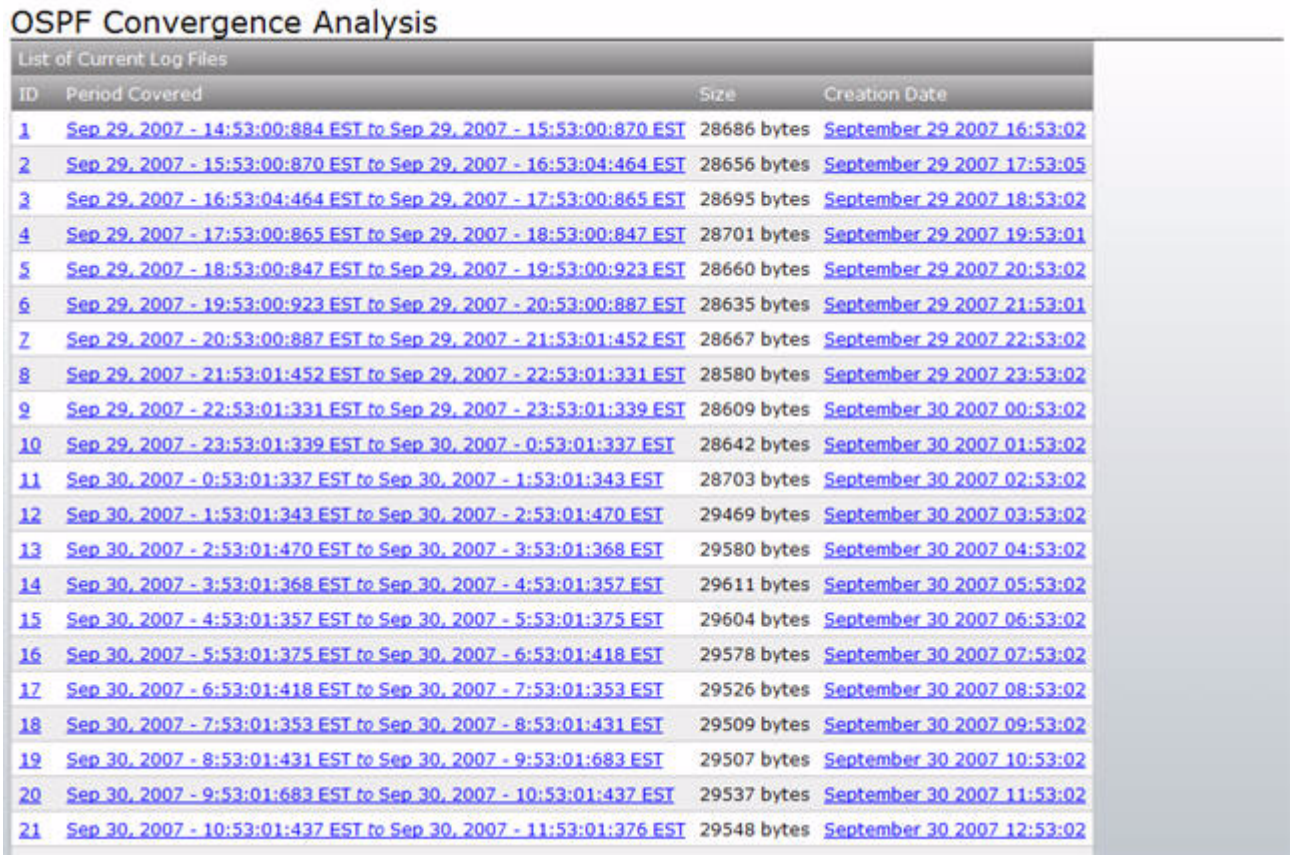
The Path Analyzer System Management Panel, Management Main Menu appears.

Step 2 Click **OSPF Convergence Log**.

The OSPF Convergence Analysis Log appears, showing a list of Convergence Activity for a designated time and date. See Figure 5-10.

Note The first log is available when the administered collection interval (the atomic time setting) has elapsed, following initial configuration.

Figure 5-10 OSPF Convergence Analysis Logs



OSPF Convergence Analysis

List of Current Log Files

ID	Period Covered	Size	Creation Date
1	Sep 29, 2007 - 14:53:00:884 EST to Sep 29, 2007 - 15:53:00:870 EST	28686 bytes	September 29 2007 16:53:02
2	Sep 29, 2007 - 15:53:00:870 EST to Sep 29, 2007 - 16:53:04:464 EST	28656 bytes	September 29 2007 17:53:05
3	Sep 29, 2007 - 16:53:04:464 EST to Sep 29, 2007 - 17:53:00:865 EST	28695 bytes	September 29 2007 18:53:02
4	Sep 29, 2007 - 17:53:00:865 EST to Sep 29, 2007 - 18:53:00:847 EST	28701 bytes	September 29 2007 19:53:01
5	Sep 29, 2007 - 18:53:00:847 EST to Sep 29, 2007 - 19:53:00:923 EST	28660 bytes	September 29 2007 20:53:02
6	Sep 29, 2007 - 19:53:00:923 EST to Sep 29, 2007 - 20:53:00:887 EST	28635 bytes	September 29 2007 21:53:01
7	Sep 29, 2007 - 20:53:00:887 EST to Sep 29, 2007 - 21:53:01:452 EST	28667 bytes	September 29 2007 22:53:02
8	Sep 29, 2007 - 21:53:01:452 EST to Sep 29, 2007 - 22:53:01:331 EST	28580 bytes	September 29 2007 23:53:02
9	Sep 29, 2007 - 22:53:01:331 EST to Sep 29, 2007 - 23:53:01:339 EST	28609 bytes	September 30 2007 00:53:02
10	Sep 29, 2007 - 23:53:01:339 EST to Sep 30, 2007 - 0:53:01:337 EST	28642 bytes	September 30 2007 01:53:02
11	Sep 30, 2007 - 0:53:01:337 EST to Sep 30, 2007 - 1:53:01:343 EST	28703 bytes	September 30 2007 02:53:02
12	Sep 30, 2007 - 1:53:01:343 EST to Sep 30, 2007 - 2:53:01:470 EST	29469 bytes	September 30 2007 03:53:02
13	Sep 30, 2007 - 2:53:01:470 EST to Sep 30, 2007 - 3:53:01:368 EST	29580 bytes	September 30 2007 04:53:02
14	Sep 30, 2007 - 3:53:01:368 EST to Sep 30, 2007 - 4:53:01:357 EST	29611 bytes	September 30 2007 05:53:02
15	Sep 30, 2007 - 4:53:01:357 EST to Sep 30, 2007 - 5:53:01:375 EST	29604 bytes	September 30 2007 06:53:02
16	Sep 30, 2007 - 5:53:01:375 EST to Sep 30, 2007 - 6:53:01:418 EST	29578 bytes	September 30 2007 07:53:02
17	Sep 30, 2007 - 6:53:01:418 EST to Sep 30, 2007 - 7:53:01:353 EST	29526 bytes	September 30 2007 08:53:02
18	Sep 30, 2007 - 7:53:01:353 EST to Sep 30, 2007 - 8:53:01:431 EST	29509 bytes	September 30 2007 09:53:02
19	Sep 30, 2007 - 8:53:01:431 EST to Sep 30, 2007 - 9:53:01:683 EST	29507 bytes	September 30 2007 10:53:02
20	Sep 30, 2007 - 9:53:01:683 EST to Sep 30, 2007 - 10:53:01:437 EST	29537 bytes	September 30 2007 11:53:02
21	Sep 30, 2007 - 10:53:01:437 EST to Sep 30, 2007 - 11:53:01:376 EST	29548 bytes	September 30 2007 12:53:02

OSPF Convergence Analysis Screen

The OSPF Convergence Analysis screen contains the following columns:

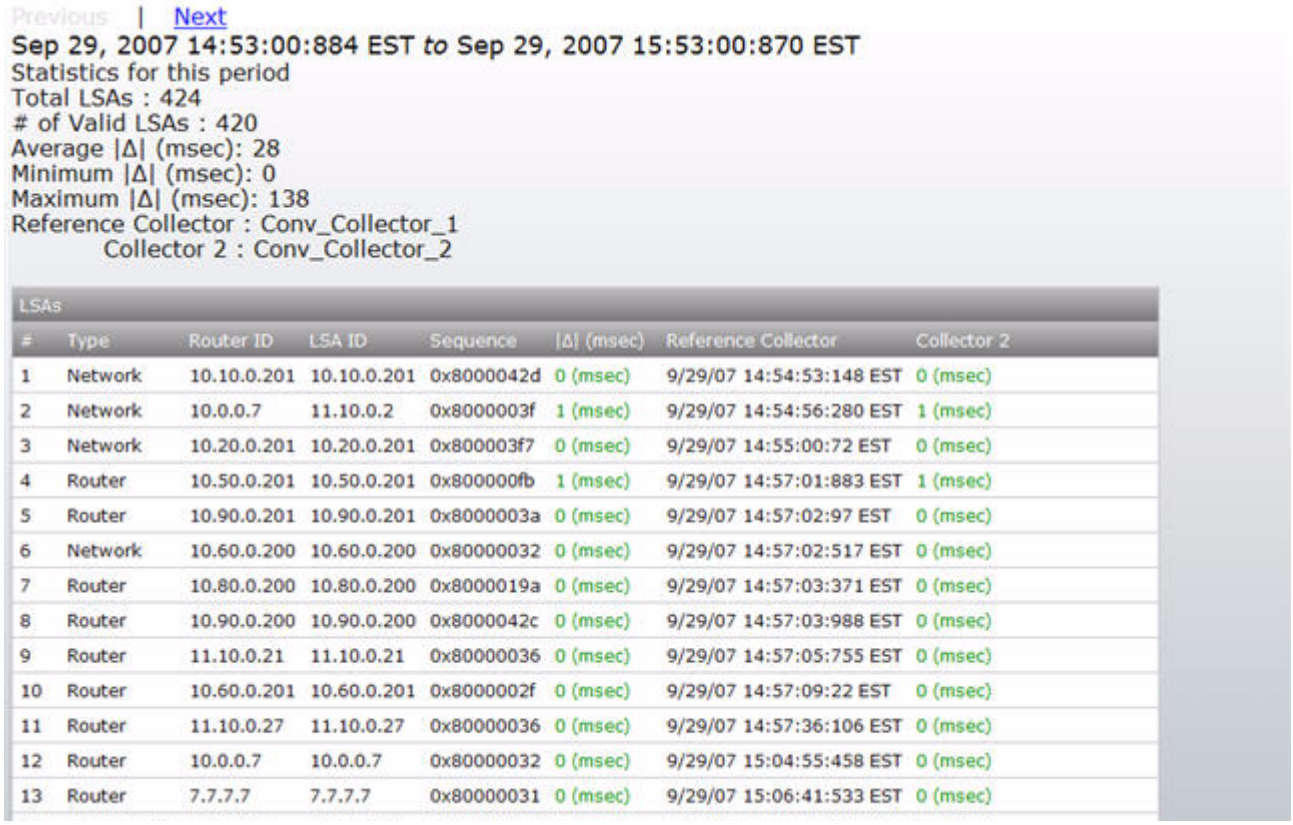
- **ID—**Convergence activity is presented sequentially by date and time. This column associates the activity period with a numeric value, starting at one.
- **Period Covered—**The convergence periods are based on the timeframe defined when configuring the Listeners. This column displays the date of the convergence followed by the user-defined time intervals for breaking down and analyzing LSAs.
- **Size—**This column presents the size of the information contained in the report. The size of the report can indicate the volume of activity that occurred during that interval and help quickly determine what reports you should view first.
- **Creation Date—**This column displays the day the report was created.

View LSA Activity for the Period

To view LSA activity for a given time period, click on the entry you want to see in the Period Covered column.

The LSA Activity screen appears (see Figure 5-11).

Figure 5-11 LSA Activity Screen


Previous | Next
Sep 29, 2007 14:53:00:884 EST *to* Sep 29, 2007 15:53:00:870 EST
Statistics for this period
Total LSAs : 424
# of Valid LSAs : 420
Average |Δ| (msec): 28
Minimum |Δ| (msec): 0
Maximum |Δ| (msec): 138
Reference Collector : Conv_Collector_1
Collector 2 : Conv_Collector_2

LSAs

#	Type	Router ID	LSA ID	Sequence	|Δ| (msec)	Reference Collector	Collector 2
1	Network	10.10.0.201	10.10.0.201	0x8000042d	0 (msec)	9/29/07 14:54:53:148 EST	0 (msec)
2	Network	10.0.0.7	11.10.0.2	0x8000003f	1 (msec)	9/29/07 14:54:56:280 EST	1 (msec)
3	Network	10.20.0.201	10.20.0.201	0x800003f7	0 (msec)	9/29/07 14:55:00:72 EST	0 (msec)
4	Router	10.50.0.201	10.50.0.201	0x800000fb	1 (msec)	9/29/07 14:57:01:883 EST	1 (msec)
5	Router	10.90.0.201	10.90.0.201	0x8000003a	0 (msec)	9/29/07 14:57:02:97 EST	0 (msec)
6	Network	10.60.0.200	10.60.0.200	0x80000032	0 (msec)	9/29/07 14:57:02:517 EST	0 (msec)
7	Router	10.80.0.200	10.80.0.200	0x8000019a	0 (msec)	9/29/07 14:57:03:371 EST	0 (msec)
8	Router	10.90.0.200	10.90.0.200	0x8000042c	0 (msec)	9/29/07 14:57:03:988 EST	0 (msec)
9	Router	11.10.0.21	11.10.0.21	0x80000036	0 (msec)	9/29/07 14:57:05:755 EST	0 (msec)
10	Router	10.60.0.201	10.60.0.201	0x8000002f	0 (msec)	9/29/07 14:57:09:22 EST	0 (msec)
11	Router	11.10.0.27	11.10.0.27	0x80000036	0 (msec)	9/29/07 14:57:36:106 EST	0 (msec)
12	Router	10.0.0.7	10.0.0.7	0x80000032	0 (msec)	9/29/07 15:04:55:458 EST	0 (msec)
13	Router	7.7.7.7	7.7.7.7	0x80000031	0 (msec)	9/29/07 15:06:41:533 EST	0 (msec)

LSA Activity Screen

Top of Screen

- **Main Menu**—The menu on the left contains links to Home, Downloads, Diagnostics, and other Path Analyzer tools. (Not pictured in Figure 5-11).
- **Prev** and **Next—**Allows you move backward and forward through the log files without returning to the previous menu.
- **Summary Period—**Shows the period this log file covers.

Statistics for the Period Area

- **Total LSAs**—Total number of Link State Advertisements during the time period.
- **# of Valid LSAs**—Total number of valid Link State Advertisements during the time period.
- **Average Delta (msecs)**—Average propagation time during the time period.
- **Minimum Delta (msecs)**—The minimum time it took for an LSA to be successfully propagated.
- **Maximum Delta (msecs)**—The maximum amount of time it took for an LSA to be successfully propagated.
- **Reference Collector—**Name of Reference Collector.
- **Collector 2**—Name of Relative Collector.

Columns in LSAs Table

- **#—**LSA activity is presented sequentially by date and time. This column associates the activity period with a numeric value, starting at one.
- **Type—**Type of LSA (router, transit, summary, etc.).
- **Router ID—**IP address of router.
- **LSA ID—**Identification number of LSA.
- **Sequence—**Sequence number of LSA.
- **Delta (msecs)**—Absolute value of time it took the LSA to be propagated.
- **Reference Collector—**Date and time LSA was received.
- **Collector 2—**The amount of time it took the LSA to be received by Collector 2 relative to Reference Collector (plus or minus).

CHAPTER 6

BGP Tagging

BGP tagging lets you label significant events so you can search for them more easily. Four constraint types, and a variety of operators let you tag those types of events that are important to you.

Most of the events collected by your Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) system are not meaningful to your enterprise. They fill up your database, retard system performance, and require a lot of resources to manage and sort. BGP tagging also lets you mark unneeded events for immediate deletion, which improves system performance and leaves room for the events that are of interest.

This chapter will explain the rules for creating BGP tags and describe the procedures for working with them using the Path Analyzer Management Console. The following topics are covered:

- Creating BGP Tags, page 6-1
- Importing BGP Tags, page 6-10
- Exporting BGP Tags, page 6-14
- Deleting BGP Tags, page 6-14
- Purging BGP Tags from the Path Analyzer Database, page 6-15

For information on applying BGP Tags, see Filtering BGP Events, page 4-20.

Creating BGP Tags

The following sections detail BGP tagging:

- Tagging Basics, page 6-1
- Sample Tag Formats, page 6-3

Tagging Basics

BGP tags are created using XML. You can create BGP Tag XML files using any standard text editor (Wordpad, Notepad, Crimson Editor, etc.). Note the following points:

- A tag can be used to:
  - delete an event (Tag and Drop), or
  - mark an event (Tag and Persist).
- A tag file can contain multiple tags.

- You can include one or more rules (constraints) within a tag.
- There are four types of rules:
  - AS Path
  - Community Attributes
  - Routes
  - Router ID's
- One tag can include any combination of the four types.
- One rule type can only be used once in a tag.
- Each rule type has a set of operators (see Table 6-1).
- AND and NOT operations are permitted among constraints.
- OR operations are not permitted among constraints.

Table 6-1 BGP Tag Data and Operators

Rule Type	Data	Operators
Router	Set of IPV4 addresses	• Equal • NotEqual
Route	Set of IPV4 routes	• Equal • NotEqual • MoreSpecificThan • LessSpecificThan
AS Path	Set of AS Path strings	• Equal • NotEqual • StartWith • NotStartWith • EndWith • NotEndWIth
	Set of AS numbers	• Contains • NotContains
	Regular expression	• Match • NoMatch
	Set of AS numbers and a path length	• StartsWithLimitedASPathLength • NotStartsWithLimitedASPathLength
	Path length	• EqualAsPathLength • NotEqualAsPathLength • GreaterAsPathLength • LessAsPathLength

Table 6-1 BGP Tag Data and Operators

Rule Type	Data	Operators
Community Attributes	Set of community strings	• Equal • NotEqual • StartWith • NotStartWith • EndWith • NotEndWith
	Set of community numbers	• Contains • NotContains
	Regular expression	• Match • NotMatch

Sample Tag Formats

Prefix Constraints

***prefix equal**

Tag the event that contained the prefix(es) listed.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<prefix_constraint type="prefix" operator="equal">
<route value="12.12.12.21/16" />
<route value="23.23.23.23/16" />
</prefix_constraint>
</tag>
```

***prefix notequal**

Tag the event that did not contain the prefix(es) listed.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<prefix_constraint type="prefix" operator="notequal">
<route value="12.12.12.21/16" />
<route value="23.23.23.23/16" />
</prefix_constraint>
</tag>
```

***prefix included**

Tag the event that included the prefix(es) listed.

```
<tags>
```

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<prefix_constraint type="prefix" operator="included">
<route value="12.12.12.21/16" />
<route value="23.23.23.23/16" />
</prefix_constraint>
</tag>
</tags>
```

***prefix notincluded**

Tag the event that did not include the prefix(es) listed.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<prefix_constraint type="prefix" operator="notincluded">
<route value="12.12.12.21/16" />
<route value="23.23.23.23/16" />
</prefix_constraint>
</tag>
</tags>
```

IP Constraints

***ipaddr_addr equal**

Tag the event that originated from a router listed here.

```
<tags>
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<ip_constraint type="ipaddr_addr" operator="equal">
<ipaddrd value="10.10.1.1" />
<ipaddrd value="10.10.3.1" />
</ip_constraint>
</tag>
```

***ipaddr_addr notequal**

Tag the event that did not originate from a router listed here.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<ip_constraint type="ipaddr_addr" operator="notequal">
<ipaddrd value="10.10.1.1" />
<ipaddrd value="10.10.3.1" />
</ip_constraint>
```

```
</tag>
```

***ipaddr_route included**

Tag the event from a router directly listed here or a subset thereof.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<ip_constraint type="ipaddr_route" operator="included">
<route value="10.10.1.1/24" />
<route value="10.10.2.1/24" />
</ip_constraint>
</tag>
```

***ipaddr_route notincluded**

Tag the event from a router NOT directly listed here or not a subset thereof.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<ip_constraint type="ipaddr_route" operator="notincluded">
<route value="10.10.1.1/24" />
<route value="10.10.2.1/24" />
</ip_constraint>
</tag>
```

BGP Path Constraints

*** aspath_length equal**

Tag the event listing a number of AS's equal to this number.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<bgp_path_constraint type="aspath_length" operator="equal">
<length value="5" />
</bgp_path_constraint>
</tag>
```

*** aspath_length notequal**

Tag the event listing a number of AS's not equal to this number.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<bgp_path_constraint type="aspath_length" operator="notequal">
<length value="5" />
</bgp_path_constraint>
</tag>
```

*** aspath_length more**

Tag the event listing a number of AS's more than this number.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<bgp_path_constraint type="aspath_length" operator="more">
<length value="5" />
</bgp_path_constraint>
</tag>
```

*** aspath_length less**

Tag the event listing a number of AS's less than this number.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<bgp_path_constraint type="aspath_length" operator="less">
<length value="4" />
</bgp_path_constraint>
</tag>
```

*** aspath_set included**

Tag the event that includes any members of this set.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<bgp_path_constraint type="aspath_set" operator="included">
<asnumber value="55" />
<asnumber value="95" />
<asnumber value="79" />
<asnumber value="20320" />
<asnumber value="9150" />
<asnumber value="61268" />
<asnumber value="58138" />
<asnumber value="24159" />
</bgp_path_constraint>
</tag>
```

*** aspath_set notincluded**

Tag the event that does NOT include any members of this set.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<bgp_path_constraint type="aspath_set" operator="notincluded">
<asnumber value="55" />
<asnumber value="95" />
<asnumber value="79" />
<asnumber value="20320" />
```

```
<asnumber value="9150" />
<asnumber value="61268" />
<asnumber value="58138" />
<asnumber value="24159" />
</bgp_path_constraint>
</tag>
```

*** aspath_start_length equal_limited**

The logic is TAG any event with a list of AS's starting with a member on the list AND TAG any list of AS's shorter then the limit_value.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<bgp_path_constraint type="aspath_start_length" operator="equal_limited">
<asstring value="53" />
<asstring value="55" />
<asstring value="60-" />
<asstring value="95-" />
<asstring value="79-" />
<asstring value="4-52334-20320" />
<asstring value="49556" />
<asstring value="43093" />
<limit value="15"/>
</bgp_path_constraint>
</tag>
```

*** aspath_start_length notequal_limited**

The logic is TAG any event with a list of AS's not starting with a member on the list OR TAG any list of AS's LONGER then the `limit_value`.

The `<asnumber value="0" />` is necessary to avoid tagging BGP withdrawals, which arrive with no `asnumber` announcements, or `asnumber value = 0`.

```
<tag name="test5" enabled="yes" domain="AS100" description="drop4_18" target=" bgp"
scope="ever" lifetime="1000">
<bgp_path_constraint type="aspath_start_length" operator="notequal_limited">
<asnumber value="0" />
<asnumber value="53" />
<asnumber value="55" />
<asnumber value="60" />
<asnumber value="95" />
<asnumber value="79" />
<asnumber value="20320" />
<asnumber value="49556" />
```

```
<asnumber value="43093" />
<asnumber value="39" />
<asnumber value="33" />
<asnumber value="60" />
<asnumber value="45" />
<asnumber value="60" />
<asnumber value="54" />
<asnumber value="43" />
<asnumber value="12" />
<asnumber value="53" />
<asnumber value="70" />
<asnumber value="90" />
<asnumber value="54" />
<asnumber value="41" />
<asnumber value="16154" />
<limit value="30"/>
</bgp_path_constraint>
</tag>
```

Multiple Constraints

Operation in a Single Tag

Within one tag, multiple constraints are ANDed.

```
<tag name="test_4" enabled="yes" domain="AS100" description="find_date_4" target="bgp"
scope="ever" lifetime="1000">
    <ip_constraint type="ipaddr_addr" operator="equal">
    <ipaddrd value="10.10.9.1" />
    </ip_constraint>
    <prefix_constraint type="prefix" operator="included">
    <route value="68.64.52.0/8"/>
    <route value="69.28.128.0/8"/>
    <route value="12.12.12.0/8"/>
    </prefix_constraint>
    <bgp_path_constraint type="aspath_start_length" operator="notequal_limited">
    <asnumber value="3356"/>
    <asnumber value="7018"/>
    <asnumber value="7132"/>
    <limit value="0"/>
    </bgp_path_constraint>
```

```
    </tag>
```

Each event is tagged if it meets the IP constraint and the prefix constraint and the BGP constraint.

Operation Within Several Tags

If you want an OR condition, consider different tags for each set of constraints.

```
<tag name="test_1" enabled="yes" domain="AS100" description="find_date_1" target="bgp"
scope="ever" lifetime="1000">
    <ip_constraint type="ipaddr_addr" operator="equal">
    <ipaddrd value="10.10.9.1" />
    </ip_constraint>
    </tag>
<tag name="test_2" enabled="yes" domain="AS100" description="find_date_2" target="bgp"
scope="ever" lifetime="1000">
    <prefix_constraint type="prefix" operator="included">
    <route value="12.12.12.25/32"/>
    </prefix_constraint>
    </tag>
<tag name="test_3" enabled="yes" domain="AS100" description="find_date_3" target="bgp"
scope="ever" lifetime="1000">
    <bgp_path_constraint type="aspath_start_length" operator="equal_limited">
    <asnumber value="3356"/>
    <asnumber value="7018"/>
    <asnumber value="7132"/>
    <asnumber value="87"/>
    <asnumber value="73"/>
    <limit value="10"/>
    </bgp_path_constraint>
    </tag>
```

Where the operation is tag1 OR tag2 OR tag3 for each event.

Working with BGP Tags

You can perform the following procedures with BGP tags:

- Importing BGP Tags, page 6-10
- Viewing BGP Tags, page 6-12
- Exporting BGP Tags, page 6-14
- Deleting BGP Tags, page 6-14
- Purging BGP Tags from the Path Analyzer Database, page 6-15

Importing BGP Tags

Once you have created BGP tags in XML format, you can import them into the Path Analyzer database using the Tag Creation Wizard, which is accessed from the Configure tab of the Tag Administration screen.

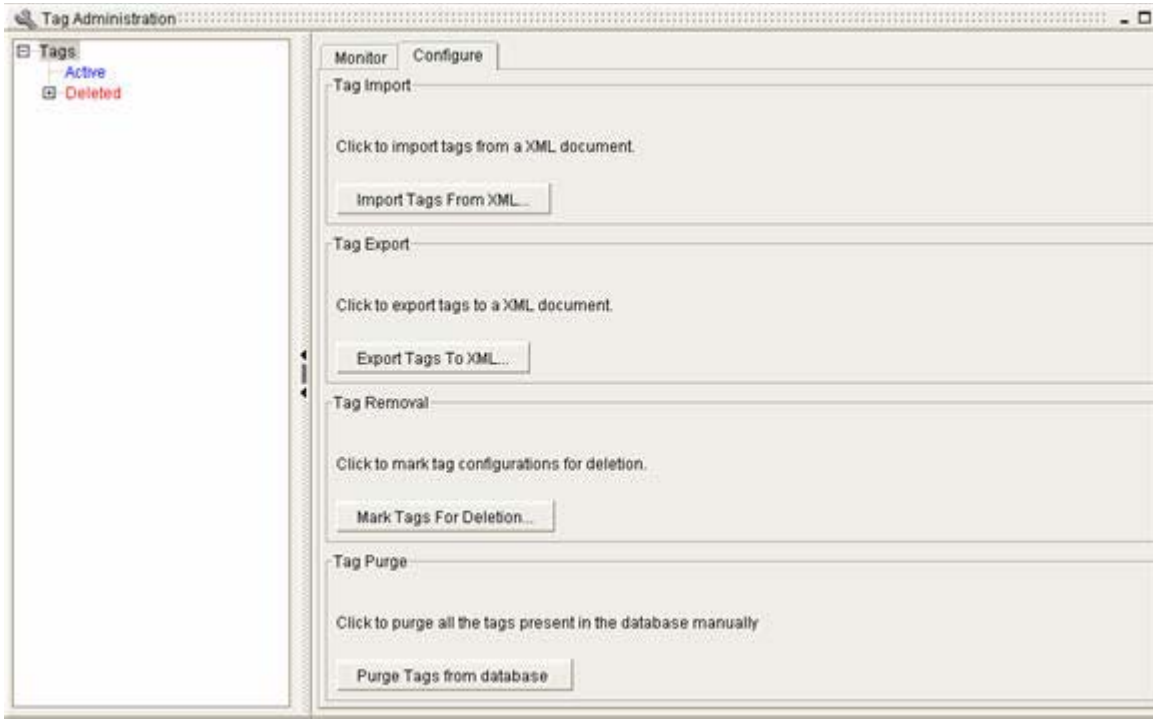
To Import BGP tags:

Step 1 Click **Start > Administration > Tagging**.

The Tag Administration screen appears (see Figure 6-1).

Step 2 Click the **Configure** tab.

Figure 6-1 Configure Tab of Tag Administration Screen



Step 3 In the Configure tab, click **Import Tags From XML**.

The Tag Creation Wizard appears.

Step 4 (Optional) Deselect the check box **Do not show this screen again** in the initial welcome screen, and click **Next**.

The Select the XML File screen appears (see Figure 6-2).

Figure 6-2 Select XML File Screen in Tag Creation Wizard

Select XML File to Import:

Step 5 Using the Look in drop-down menu, navigate to the directory where you have stored your XML tags, and click the tag you wish to import.

The tag appears in the File name field.

Step 6 Click **Next**.

The Select type of import screen appears (see Figure 6-3).

Figure 6-3 Select Type of Import Screen in Tag Creation Wizard

Select Type of Import:

Step 7 Select one of the following radio buttons to Choose an import type:

- **Add to Existing Configuration** (default)—Imports a tag file and enters it in the database, while retaining existing tags.
- **Import Configuration from Scratch**—Imports a tag file and removes all tags currently in database that are not in the imported file.

Step 8 Click **Next**.

After a short wait, the message displays, “Import of Tag Configurations complete.”

Step 9 Click **Finish**.

The new tag name is displayed under the Monitor tab. See Viewing BGP Tags, page 6-12.

Viewing BGP Tags

Information about tags is viewed in the Monitor tab of the Tag Administration screen.

View both Active and Deleted tags

To view both active and deleted tags, click **Start** > **Administration** > **Tagging**.

The Monitor tab of the Tag Administration screen appears, displaying both Active and Deleted tags, as shown in Figure 6-4.

View either Active or Deleted tags

Step 1 From the Path Analyzer taskbar click **Start** > **Administration** > **Tagging**.

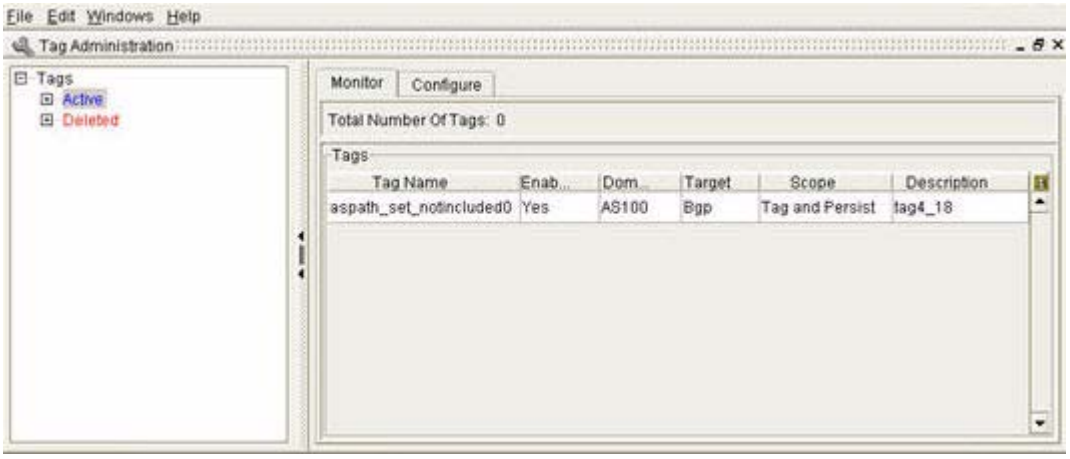
The Monitor tab of the Tag Administration screen appears, displaying both Active and Deleted tags, as shown in Figure 6-4.

Step 2 To view either Active or Deleted tags:

- Click **Active** in the menu hierarchy on the left side of the screen, or
- Click **Deleted** in the menu hierarchy on the left side of the screen.

Deleting a tag does not remove it from the database. Deleted tags remain in the database until all related events are deleted.

Figure 6-4 View Active Tags in Tag Administration Screen



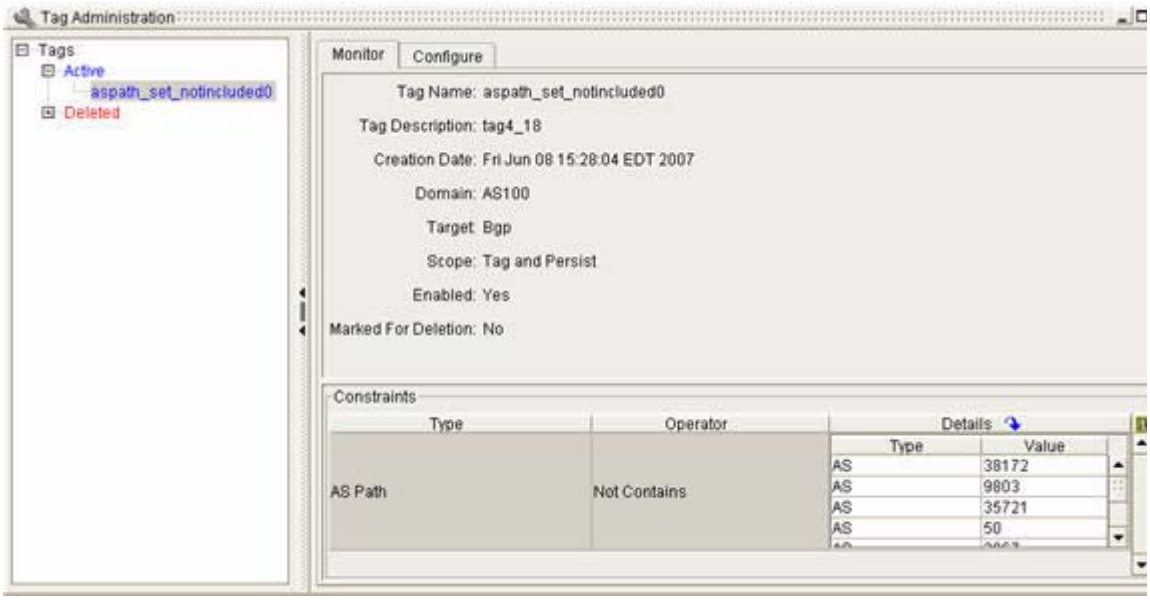
The following information is provided for both active and deleted tags.

- Tag Name—The name you used to identify the tag in the XML file.
- Enabled—Whether the tag is active or deleted.
- Domain—The domain where the tag is applied.
- Target—Border Gateway Protocol (BGP).
- Scope—Tag and Persist or Tag and Drop.
- Description—The description of the tag you entered in the XML file.

Step 3 Click **Active** or **Deleted** in the menu hierarchy to view the details of a specific tag. This reveals the tag names listed below.

Step 4 Click the name of the tag you wish to view in the Tag Detail screen, as shown in Figure 6-5

Figure 6-5 Tag Detail Screen.



The following information is provided in the Tag Detail screen.

- Tag Name, Enabled, Domain, Target, Scope and Description (described in Figure 6-4View Active Tags in Tag Administration Screen, page 6-12).
- Creation Date—The date the tag was imported.
- Marked for Deletion—Deleted tags are marked with Yes, Active tags are marked with No.
- Type—Tags can be one of the following types: Router ID, Route, AS Path, or Community Attribute.
- Operator (depends on Type)—Equal, NotEqual, MoreSpecificThan, LessSpecificThan, StartWith, NotStartWith, EndWith, NotEndWith, Contains, NotContains, Match, NoMatch, EqualAsPathLength, NotEqualAsPathLength, GreaterAsPathLength, LessAsPathLength, StartsWithLimitedPathLength, NotStartsWithLimitedPathLength.
- Under Details:
  - Type—Router ID, Route, AS Path, or Community Attribute.
  - Value—The value of Router ID, Route, AS Path, or Community Attribute.

Exporting BGP Tags

You can export an existing tag from the Path Analyzer database if you wish to modify it. An exported tag is not removed from the database, but copied to the directory you select.

Note You cannot import a tag with a name that is identical to one already in the Path Analyzer database. If you wish to re-import a modified tag, you will need to change file name of the tag, and the tag name within the XML file.

To export an existing tag:

Step 1 Click **Start** > **Administration** > **Tagging**.

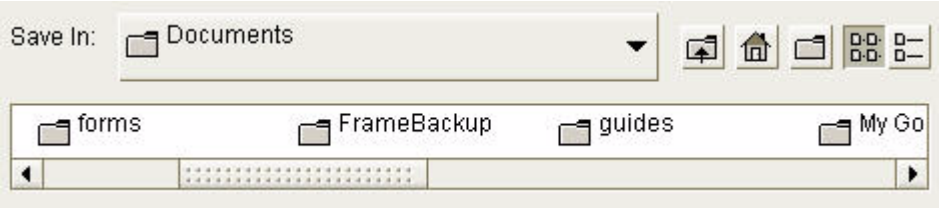
The Monitor tab of the Tag Administration screen appears.

Step 2 Click the **Configure** tab.

Step 3 Click the **Export Tags To XML** button.

Step 4 The Tag Export Wizard appears. If this is your first time using the Tag Export Wizard, click **Next** to dismiss the initial welcome screen.

Step 5 Navigate to the directory where you want to store your XML tag in the **Save in** field, using the navigational buttons next to the directory drop-down.



Step 6 Enter the name of the tag you are exporting in the File name field.

Step 7 To save the file as an .xml file, leave the Files of type drop-down menu to “Extensible Markup Language.”

Step 8 Click **Next**.

An **Export in progress** message is displayed.

Step 9 Click **Finish** when the export completes.

The file is saved in the directory you selected, and can be opened in the text editor of your choice.

Deleting BGP Tags

When you delete a BGP tag, it can no longer be used to tag events. The deleted tag appears as **Deleted** under the **Monitor** tab. However, it will remain in the Tag Mask Table until you purge it from the Path Analyzer database. See Purging BGP Tags from the Path Analyzer Database, page 6-15.

To delete a BGP tag:

Step 1 Click **Start** > **Administration** > **Tagging**.

The Monitor tab of the Tag Administration screen appears.

Step 2 Click the **Configure** tab.

Step 3 Click the **Remove Tags** button in the Tag Removal section.

The Tag Removal Wizard appears (see Figure 6-6). If this is your first time using the Tag Removal Wizard, click **Next** to dismiss the initial welcome screen.

Step 4 Select the tag(s) you wish to remove in the Remove One or More Tag Configurations screen by clicking on them.

Figure 6-6 Tag Removal Wizard

Step 5 Click **Next** when you have highlighted all of the tags you wish to remove.

A Tags are being removed message appears.

Step 6 Click **Finish** when the removal is complete.

Purging BGP Tags from the Path Analyzer Database

If you use a large number of BGP tags, you will need to purge the Tag Mask Table periodically, ensuring that it doesn't become full of unused tags.

Note If there are any events in the database associated with a tag, the purge will not remove that tag.

The purging process can take an hour or more, depending on the size of the Tag Mask Table. You should make tag purging one of your routine maintenance procedures, and schedule it at an appropriate time.

To purge tags from the Path Analyzer database:

Step 1 Click **Start > Administration > Tagging**.

The Monitor tab of the Tag Administration screen appears.

Step 2 Click the **Configure** tab.

Step 3 Click the **Purge Tags from database** button n the Tag Purge section.

The warning message, The purge of tags will take a long time to complete, Continue? appears.

Step 4 Click **OK**.

Path Analyzer purges tags from the database.

CHAPTER 7

MP-BGP Instrumentation

Multiprotocol BGP Extensions (MP-BGP)

This section introduces multiprotocol BGP, and details the following information:

- MP-BGP Defined, page 7-1
- Path Analyzer MP-BGP VPN Instrumentation, page 7-1

MP-BGP Defined

BGP4 was originally designed to carry routing information for the IPv4 address family. IETF RFC 2858 (http://www.apps.ietf.org/rfc/rfc2858.html) extends BGP4 capability by standardizing multiprotocol extensions for BGP4.

MP-BGP allows BGP to carry routing information for the multiple network layer protocols, including:

- IPV6
- IPX
- VPN-IPV4

Cisco Service Path Analyzer (herein referred to as the Path Analyzer) supports unicast, multicast, and VPN-IPV4 instrumentation.

Path Analyzer MP-BGP VPN Instrumentation

The following MP-BGP VPN information is covered in this section:

- VPN Instrumentation Using VRFs, page 7-2
- Creating a VRF Definition, page 7-2
- Direct and Indirect Instrumentation, page 7-2
- Local/Remote Routes in VRF, page 7-2
- Working with VRFs using the Path Analyzer GUI, page 7-3
- VPN Events, page 7-3
- Master/Slave VRFs, page 7-3
- Common Instrumentation Mistakes, page 7-4

VPN Instrumentation Using VRFs

The basic building block in MP-BGP VPN instrumentation is Virtual Routing and Forwarding (VRF). VRF is a networking technology that simultaneously supports multiple instances of a routing table within the same router. For more information on VPNs, see IETF RFC 4364 (http://www.ietf.org/rfc/rfc4364.txt).

A VRF is a entity configured within the network; it is not defined/discovered through instrumentation of the MP-BGP protocol.

Creating a VRF Definition

To create a VRF definition, you first create an XML file by entering the Route Distinguisher (RD) and the import/export policies for each VRF. For an example, see Sample VRF XML File, page 7-4. Next, you import the XML file into Path Analyzer. A VRF Configuration Wizard lets you add, remove, and change VRF definitions within the Path Analyzer database. The complete VRF importation process is explained in the Managing VRF Tables section of Chapter 5 in the *Cisco Service Path Analyzer Administration Guide*.

Path Analyzer applies the configuration information to the collected MP-BGP advertisements (through Collectors) to populate the VRFs (finding out which VRF installs what routes). This dual nature is very important: configuration information plus the network information creates the VRFs and their content. Any change to one of those sources will cause changes in the VRFs.

The XML configuration not only defines VRF entities, it also defines how Collectors and VRFs are associated with each other. You have two choices: direct and indirect instrumentation.

Direct and Indirect Instrumentation

- **Direct Instrumentation**—Instrument all Provider Edge (PE) routers directly, so that each VRF is populated using the information received from the owner PE (the PE router on which VRF is defined), or
- **Indirect Instrumentation**—Instrument a single router (generally a Route Reflector Server, or a set of routers), and then use the information received through that limited set to populate the all VRF contents.

Indirect instrumenting is recommended because it decreases the load on the network. When the indirect approach is chosen, you must define a source router—an instrumented router—in addition to the owner router.

Owner routers must be PE routers, but source routers can be PE routers or Route Reflector Servers. This approach is supported only for the VPN address family. The owner routers are displayed in the BGP topology, even if they are not instrumented, so that they can be used as VRF containers.

Local/Remote Routes in VRF

The routes installed into each VRF are divided into two groups:

- **Local**—Routes originated by the current VRF.
- **Remote**—Routes that are originated by other VRFs and installed inside the current VRF.

Path Analyzer inspects the RD value of the received advertisement to find out which VRF originated the route. From the route perspective, the VRF that originates the route is called a Local VRF, and the VRFs that install that route are called Remote VRFs.

Working with VRFs using the Path Analyzer GUI

You can use the Path Analyzer graphical user interface to perform the following VRF-related activities:

- View all VRF information within an autonomous system (AS). See, View Details of an Autonomous System, on page 2-55.
- Compare routing tables for Virtual Routing and Forwarding (VRF) ID's. See, Router Information Base (RIB) Comparison, on page 2-50.
- Filter events using VRF ID's (local and remote) as well as other VPN-related filters. See, BGP Filtering Example 2: IPV4 VPN Events, on page 4-28.

VPN Events

For each network advertisement received from an MP-BGP Collector:

- First, all the VRFs that have a matching import policy are retrieved.
- Second, the VRFs that are mapped to that Collector are located. That is,
  - for the indirect method, all VRFs that have that Collector in their sourcePE tag are located.
  - for the direct method, all VRFs that have that Collector in their PE tag are located.
- After this discovery phase, Path Analyzer creates one VPN network event entry in the database for each VRF that installs, uninstalls, or updates the advertisement. If the originator VRF (local VRF) is found, it is persisted in each event.

Example:

Step 1 An advertisement is received by VRF "A."

Step 2 After checking the Route Target (RT) value of the advertisement, it is determined that VRF "B" and VRF "C" will install that route.

Step 3 Path Analyzer creates three VPN network events in the database for VRFs "A," "B," and "C," where VRF "A" is the Local VRF in all events.

Master/Slave VRFs

The Path Analyzer system uses Virtual Routing and Forwarding as a building block for MP-BGP VPN instrumentation. This is different from how unicast and multicast routes are handled.

With VRFs, there is a database entry for each VRF that installs that advertisement, and not for each received advertisement. This approach may cause a problem in networks that have a lot VRFs with the same import policy.

To handle this problem, a Master VRF is used. The Master VRF is a special VRF created internally for each normal VRF (also called a Slave VRF) supported by the user. The Master VRF inherits the import policy of its linked Slave VRF. All Slave VRFs that have same import policy will get linked to the same Master VRF.

Note A Master VRF can only be enabled during the creation of a BGP AS. It cannot be changed later.

Whenever a network advertisement is received, it is installed on the Master VRF as a single database entry. There is an additional entry for the VRF that originates the advertisement. The Master VRF summarizes all the remote routes installed in all the VRFs that have same import policy.

For example, if there are 20 VRFs that have same import policy, they will all be linked to a single Master VRF. For each received advertisement, there will be only two entries in the database, (one for local VRF and one for remote VRF), instead of 20 entries (assuming that one of those 20 VRFs originated the advertisement).

The Master/Slave model won't change the user's GUI experience, nor will it affect other functionality. It does, however, affect how network events are generated and stored in the database.

Common Instrumentation Mistakes

The following mistakes are commonly made when instrumenting VRFs:

- Picking the wrong source PE router. The router must be an instrumented router that contains MP-BGP VPN information.
- Not defining the Route Reflector client configuration for the VPN address family at the router instrumented for the Path Analyzer Collector.
- Any change in the VRF configuration causes the Collectors (that are used to populate the VRFs) to flap, because the administration state of the Collector must be set to "down," and then reset to "up" to force a resynchronization on the server side. To prevent this, first define the VRFs (via XML import), and then enable the Collectors.

For a sample VRF XML file, see Sample VRF XML File, page 7-4.

Creating VRF XML Files

This section provides a sample VRF XML file, as well as an explanation.

Sample VRF XML File

```
<vrfs>
    <domain>
        <vrfIdMethod>FullRD</vrfIdMethod>
        <vrfMapMethod>indirect</vrfMapMethod>
        <!-- for each VRF -->
        <vrf>
            <RD>60:60</RD>
            <importRT>
                  <RT>70:70</RT>
                  <RT>80:80</RT>
            </importRT>
            <PE>192.168.30.233</PE>
```

```
            <!-- present if indirect mapping is enabled -->

            <sourcePE>192.168.30.233</sourcePE>
            <exportRT>
            <RT>60:60</RT>
            </exportRT>
                        <name>XY</name>
                        <description>Customer X on site Y</description>
        </vrf>
    </domain>
</vrfs>
```

Explanation of Sample File

If

If the Path Analyzer server uses the `vrfIdMethod id FullRD` (the only supported value in this Path Analyzer release) to identify the VRF (used as VRF ID), and the originator of a VPN router advertisement.

The `vrfMapMethod` is explained in the previous section; it can be indirect or direct.

Then

Then, for each VRF, a vrf section must be defined. The first tag is the `RD` tag, then the `importRT` tag; the user can define as many Route Target (RT) values as required to define import policy for the VRF.

The next tag contains the Router ID of the owner PE routers. If the indirect approach is chosen, you must define a source PE router. The network information gathered by instrumenting this router is used to populate the VRF.

The rest of the tags are optional. The first one is the `exportRT` tag, which contains the RT values used in the export policy of the VRF. After that, the file contains the `name` and `description` tags.

CHAPTER 8

Setting and Monitoring Alarms

Setting and Receiving Notifications of Real-time Changes

Alarms are automated notifications of a change, or a selected series of changes that occur in your network. Alarms can be exported to your network management system (NMS).

Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) provides an Alarm Monitor from which you can set Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and service alarm notifications.

Changes that Trigger Alarms

In Path Analyzer, OSPF Listeners forward routing information derived from the Link State Advertisements (LSAs) of OSPF routers, to the Path Analyzer Server, which processes them.

Similarly, BGP Listeners forward BGP update messages to the Path Analyzer Server. Router messages carried over OSPF and BGP protocols provide insight into the state and availability of the service paths that carry data across your network.

When the Path Analyzer Server detects a selected routing change or preset sequence of changes, it generates a visual notification in the Alarm Monitor window.

The Alarm Monitor allows you to set service alarms that issue notifications about changes to configured services and service paths. For information about configuring a service path, see Chapter 3, “Monitoring Unicast and Multicast Services”.

Persist Alarms

The Path Analyzer Server database persists alarms, providing a historical record of all alarms and the events that triggered them.

You can set, view, and acknowledge OSPF, BGP, and service alarms in the Path Analyzer Alarm Monitor. Icons indicate when an alarm has been triggered and requires immediate attention. Each triggered alarm is accompanied by a list of changes to the routing patterns that activated the alarm. These changes, referred to as alarm triggers, answer the question: “What events caused the alarm?”

View Real-time Alarms

The real-time view of the Alarm Monitor presents a current and dynamic display of alarms.

Note The Alarm Monitor is not supported in Historical Mode.

Alarm Triggers in the Trigger Log

Use the Trigger Log to view and browse through alarm triggers. You can also acknowledge triggered alarms after you have resolved them. See Indicators of Triggered Alarms, page 8-61 for information.

Export Alarm Triggers Your NMS

You can export alarm triggers to a syslog host or an SNMP agent for notification in your network management system (NMS). When an alarm is created in Path Analyzer, once it occurs, its triggers are exported to the appropriate destinations.

For information about exporting alarms, see Chapter 8, Exporting Alarm Triggers, in the *Cisco Service Path Analyzer System Administration Guide*.

For information about all the alarms available in Alarm Monitor, see the *Cisco Service Path Analyzer Alarm Reference.*

Alarm Configuration Wizards

The Alarm Monitor provides an Alarm Configuration Wizard for BGP, OSPF, and services to help you set predefined alarms. Alarms can be set on:

- BGP advertisements, BGP threshold per router, BGP routes, BGP threshold per AS.
- OSPF interfaces, routers, Transit networks, advertisements, routes, threshold, and errors such as duplicate IP addresses assigned to interfaces in the same area.
- Services and service paths, which you create in Service Monitor.

View the Root Cause of Service Path Alarms

You can view the root cause of a service path alarm trigger from the **Trigger Log** or **Last 10 Triggers** field. Knowing the root cause of an alarm can help you:

- discover the cause of the alarm trigger.
- determine why the alarm was triggered on a service path.

The root cause of an alarm trigger answers the question: “Why did this particular sequence of events occur in the network?”

For information about viewing the root cause of a service path alarm trigger in the Alarm Monitor for Services, see Show the Root Cause of a Service Path Alarm Trigger, page 8-71.

Similarly, you can view the root cause of issues affecting a service path from Service Monitor. See View the Root Cause of a Change to a Unicast Service Path, page 3-23.

Alarm Setting and Viewing Tasks

- Starting Alarm Monitor, page 8-3
- Configuring Alarms, page 8-4
- Viewing and Managing Alarms, page 8-55
- Working in the Trigger Log, page 8-68

Starting Alarm Monitor

Start Alarm Monitor to view the current and dynamic list of alarms.

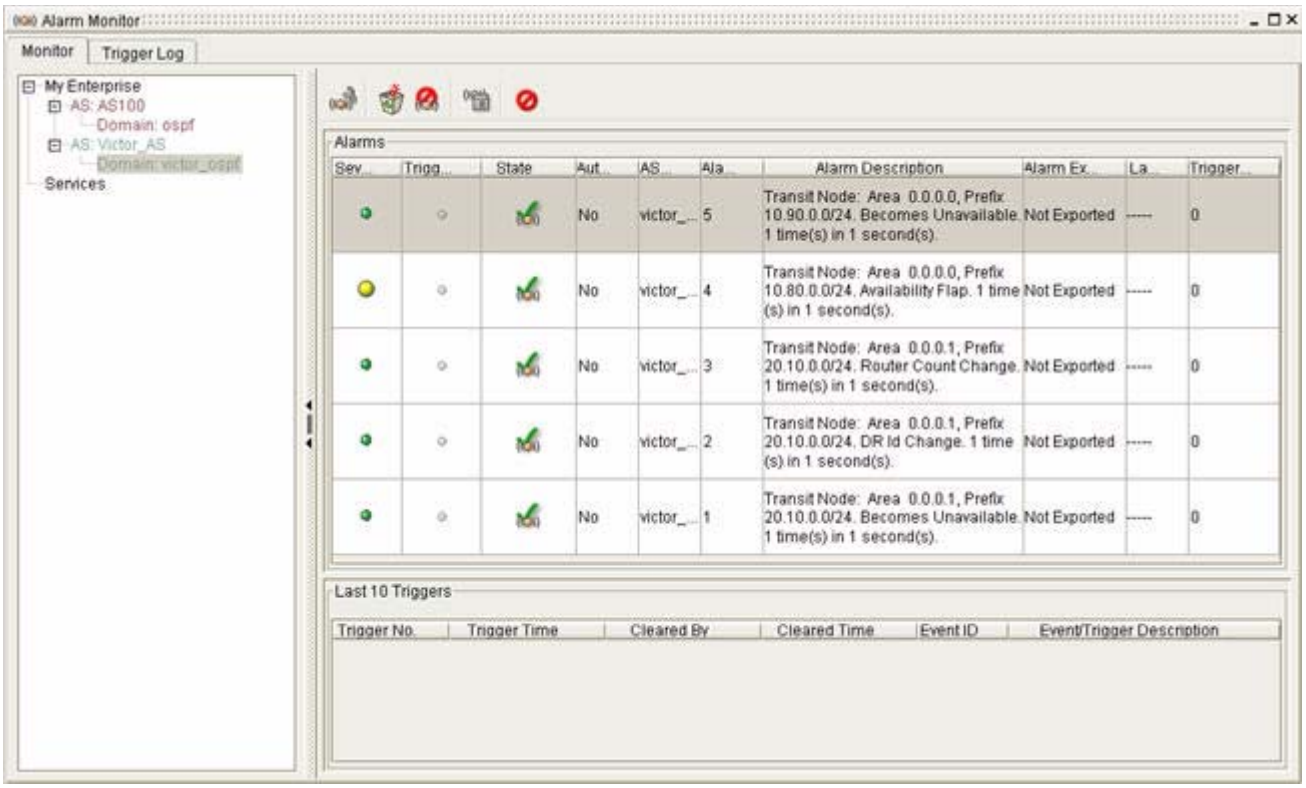
Start Alarm Monitor

To start Alarm Monitor from the Path Analyzer taskbar, click **Start > Alarm Monitor**.

The Alarm Monitor opens in the Route Dynamics Management Console (see Figure 8-1).

For information about the fields and buttons of the Alarm Monitor, see Alarm Monitor, page 8-72.

Figure 8-1 Alarm Monitor Screen



Configuring Alarms

Using the BGP, OSPF, or Services Alarm Configuration wizards, you can configure an alarm to notify your team of a change, or a selected series of changes, in your network. For information about the types of alarms you can create, see Supported Alarms, page 8-57.

To configure an alarm, you will need to select the following attributes:

- **Type—**Alarm type: BGP, OSPF, or Services.
- **Entity type**—Type of entity to monitor for changes, for example: router, route, interface, advertisement, service, or service path.
- **Alarm type**—Specify the type of alarm to set. For example:
  - Change in the availability of a router or route.
  - Change in the cost metric of an interface.
  - Change in conformity of a service path.

or

  - Error alarm that identifies duplicate IP addresses, duplicate routes, or overlapping network masks.
- **Alarm severity**—Severity assigned to the alarm: Critical, High, Medium, or Low.
- For information about alarm severities, see Severity Values of Alarms, page 8-61.
- **Count—**Number of times the change must occur within a selected period of time (see **Time window** below) to trigger the alarm.
- **Time window**—Selected period of time in which the change must occur.
- **Auto Clear—**Enables an alarm to clear automatically from Alarm Monitor after its trigger condition has been detected and resolved.

Note For all alarms (BGP, OSPF, and Services), if a count greater than 1 is entered, **Auto Clear** is disabled automatically. **Auto Clear** can be set only if count equals 1.

Configure a BGP Alarm

To configure a BGP alarm, complete the following steps:

- Start the BGP Alarm Configuration Wizard, page 8-5
- Select a Category of BGP Alarms, page 8-5

Once you have started the wizard, you can configure the following BGP alarms:

- Configure a BGP Advertisement Alarm, page 8-6
- Configure a BGP Threshold per Router Alarm, page 8-9
- Configure a BGP Route Alarm, page 8-12
- Configure a BGP Threshold per AS Alarm, page 8-14
- Configure a BGP Next Hop Alarm, page 8-17

Start the BGP Alarm Configuration Wizard

To start the BGP alarm configuration wizard:

Step 1 Select **Start** > **Alarm Monitor**.

The Alarm Monitor window appears in the Path Analyzer Management Console. By default, the Monitor tab is selected.

Step 2 Select an Autonomous System (AS) from the Enterprise hierarchy on the left side of the screen.

Step 3 Click **Configure Alarms** in the Alarm Monitor Toolbar, page 8-73.

The Alarm Configuration Wizard appears, featuring options for BGP alarms (see Figure 8-2).

Figure 8-2 BGP Alarm Configuration Wizard

Select a Category of BGP Alarms

To select a category of BGP alarms:

Step 1 Click on the appropriate radio button to select the type of alarm to create:

- **Advertisement**—Set alarms on BGP route advertisements. See Configure a BGP Advertisement Alarm, page 8-6.
- **Threshold per Router**—Set alarms to trigger when the number of advertisements for a router or the rate of advertisement events for a router deviates from the normal value by a set percentage. See Configure a BGP Threshold per Router Alarm, page 8-9.
- **Route**—Set alarms on a BGP route. See Configure a BGP Route Alarm, page 8-12.

- **Threshold per AS—**Set alarms to trigger when the number of routes in an AS or the rate of route events in an AS deviates from the normal value by a set percentage. See Configure a BGP Threshold per AS Alarm, page 8-14.
- **BGP Next Hop—**Sets alarm to trigger when the next hop is no longer available using an OSPF route. See Configure a BGP Next Hop Alarm, page 8-17.

Step 2 Select the category of Alarm and click **Next**.

A configuration wizard will appear for the type of alarm you have selected.

Configure a BGP Advertisement Alarm

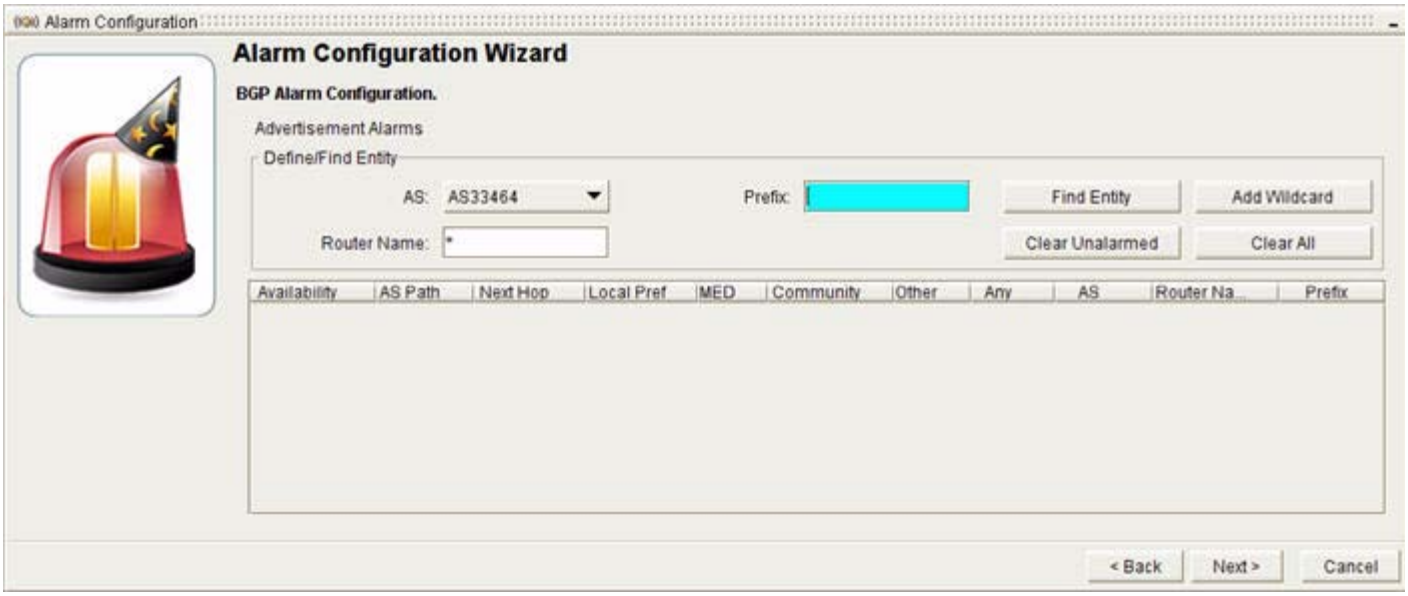
To configure a BGP advertisement alarm:

Step 1 Use the procedure to Start the BGP Alarm Configuration Wizard, page 8-5.

Step 2 Select the **Advertisement Alarm** radio button and click **Next**.

The BGP Alarm Configuration, Advertisement Alarms wizard screen appears (see Figure 8-3).

Figure 8-3 BGP Advertisement Alarm Screen in BGP Alarm Configuration Wizard



Step 3 To view all possible BGP route advertisements exchanged by routers in the domain, click **Find Entity**.

or

a. Narrow down your option set by completing any of the following fields before clicking **Find Entity**:

- In the AS field, the AS appears by default.
- In the Prefix field, enter the prefix of the advertised route in the form of an IP address and subnet mask. Example: When you click **Find Entity** for the prefix 1.1.0.0/16, this prefix and the set of more specific prefixes are returned.
- In the Router Name field, enter the host name or Router ID of the router that issues the route advertisements you want to set an alarm for.

b. Click **Find Entity**.

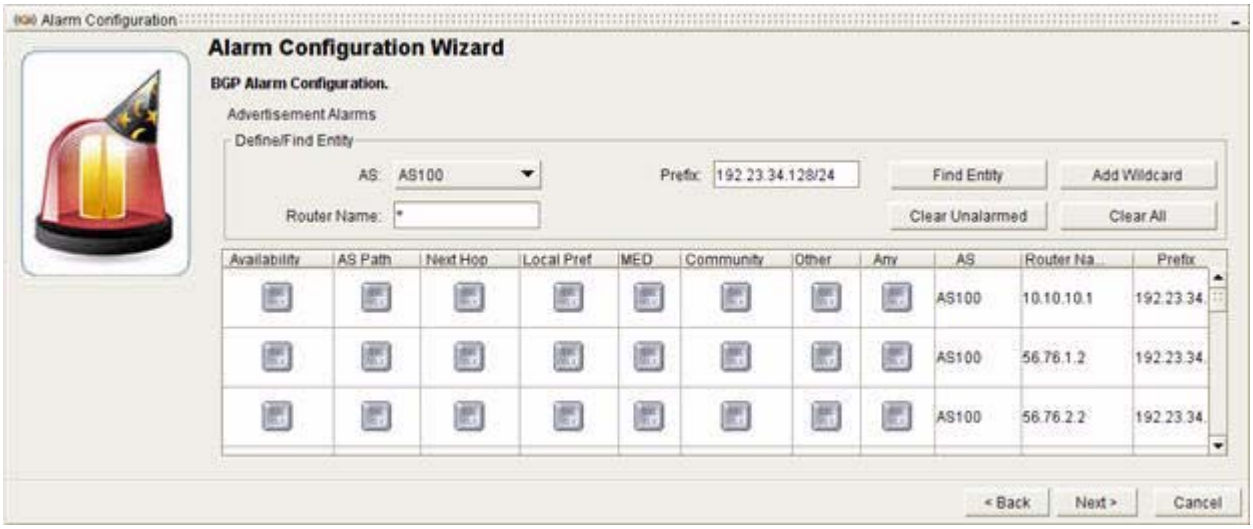
A narrower set of advertisements is displayed.

Step 4 (Optional) Click **Add Wildcard** to add options for setting wildcard alarms on advertisements that match the configuration parameters you selected previously.

Note If you decide to set wildcard alarms on all advertisements within the selected autonomous system (listed in the AS field), manually delete settings you entered in the Prefix and Router Name fields, enter an asterisk (*) in each field, and click **Add Wildcard** to set wildcard alarms on all advertisements in the selected autonomous system. For example, a wildcard alarm on an AS Path change is triggered if any BGP advertisement undergoes an AS Path change.

Set the Alarm Type

Figure 8-4 Set Alarm-Type Screen for BGP Advertisement Alarm



To set the alarm type, double-click any of the following buttons (see Figure 8-4):

- **Availability**—Notifies of changes in the availability of a BGP advertisement or if the advertisement flaps (becomes intermittently available and unavailable in the network). Sets a BGP Advertisement Availability Alarm.
- **AS Path**—Notifies of changes to the AS Path attribute of a BGP advertisement. Sets a BGP Advertisement AS Path Change alarm.
- **Next Hop**—Notifies of changes to the Next Hop attribute of a BGP advertisement. Sets a BGP Advertisement Next Hop Change alarm.
- **Local Pref—**Notifies of changes to the Local Pref attribute of a BGP advertisement. Sets a BGP Advertisement Local Pref Change alarm.
- **MED—**Notifies of changes to the Multi-Exit Discriminator (MED) attribute of a BGP advertisement. Sets a BGP Advertisement MED Change alarm.
- **Community**—Notifies of changes to the Community attribute of a BGP advertisement. Sets a BGP Advertisement Community Change alarm.

- **Other**—Notifies of changes to all other BGP attributes documented in RFC 1771 (http://www.ietf.org/rfc/rfc1771.txt) that are not listed in the BGP Alarm Configuration, Advertisement Alarms wizard page. Sets a BGP Advertisement Other Attribute Change alarm.
- **Any**—Notifies of any change to a selected BGP advertisement. Sets a BGP Advertisement Wildcard Alarm.

Provide Alarm Settings

Figure 8-5 Alarm Settings Screen for BGP Advertisement Alarm

Not all of the alarm settings are available for each type of alarm. You must provide the following alarm settings:

- The Availability Alarm has all settings listed below, a–f.
- The rest of the alarms have settings c, d, and e only, as listed below.

To provide alarm settings (see Figure 8-5):

Step 1 Provide alarm settings:

a. Select the degree of specificity for the route(s) that will cause the alarm to trigger. Select one of the following options from the Alarm On drop-down menu:

- **Exact**—Alarm will trigger when there is a change in availability of the exact route prefix you entered in the Prefix field.
- **More Specific**—Alarm will trigger when there is a change in availability of a more specific route prefix.
- **Less Specific**—Alarm will trigger when there is a change in availability of a less specific route prefix.
- **Exact Mask Length**—Alarm will trigger when there is a change in the availability of a prefix that has the same mask length as the value you entered.
- **Greater Mask Length**—Alarm will trigger when there is a change in availability of a prefix with a greater mask length than the prefix you entered.
- **Lesser Mask Length**—Alarm will trigger when there is a change in availability of a prefix with a lesser mask length than the prefix you entered.

b. Indicate the route condition that will trigger an alarm notification. Select one of the following options from the Alarm Type drop-down menu:
   - **Advertised**—Is advertised.
   - **Withdrawn**—Is withdrawn.
   - **Flap**—Is advertised and withdrawn intermittently.

c. For the Alarm Severity, select one of the following radio buttons:
   - **Critical**
   - **High**
   - **Medium**
   - **Low**

   For more information, see Severity Values of Alarms, page 8-61.

d. In the Count field, enter the number of times the change that must occur within the given time period (see the Time Window field below) before triggering the alarm. By default, the Count value is set to 1, to indicate one change within the time window.

e. In the **Time Window** field, enter the period of time in which the change must occur.

   By default, the Time Window value is set to 1, to indicate a one-second time window. For information about setting the Count and Time Window, see Time Window for Alarm Triggering, page 8-63.

f. (Optional) Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the Availability Alarm (if selected) displays a triangle with a red star, indicating that the alarm has been configured.

The DBL CLK button under the other alarm types (if selected) displays two triangles, each with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the **Alarm** section of the Alarm Monitor window.

Configure a BGP Threshold per Router Alarm

Step 1 Use the procedure to Start the BGP Alarm Configuration Wizard, page 8-5.

Step 2 Select the **Threshold per Router** radio button and click **Next**.

The BGP Alarm Configuration, Threshold per Router Alarms Wizard screen appears.

Step 3 Click **Find Entity** to view all possible BGP routers in the selected autonomous system. (See Figure 8-6.)

or

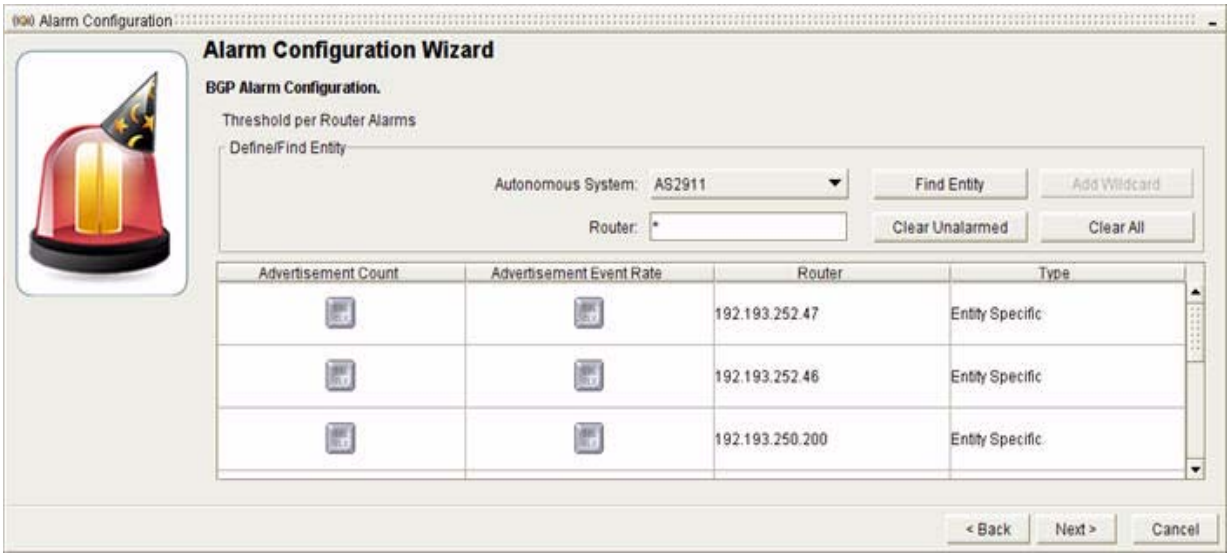
a. Narrow down your option set by completing any of the following fields before clicking **Find Entity**:
   - In the AS field, the autonomous system appears by default.
   - In the Router Name field, enter the router name.

b. Click **Find Entity**.

A narrower set of entities is displayed. The router appears if it is present.

Set the Alarm Type

Figure 8-6 Threshold per Router Alarm Screen in BGP Alarm Configuration Wizard

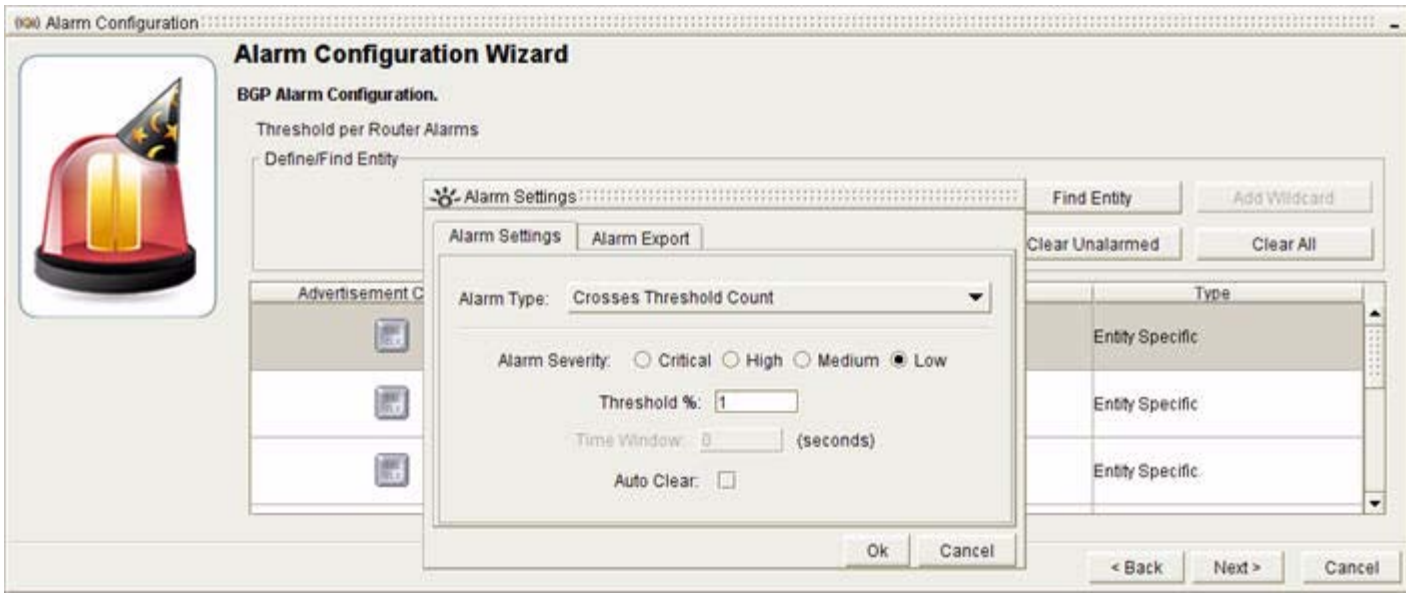


To set the alarm type, double-click any of the following buttons (see Figure 8-6):

- **Advertisement Count—**This alarm is triggered when the number of routes deviates from the average value by at least the defined percentage.
- **Advertisement Event Rate—**This alarm is triggered when the rate of advertisement events for a router exceeds the threshold by more than the defined percentage.

The Alarm Settings screen appears (see Figure 8-7).

Figure 8-7 Alarm Settings Screen for Threshold per Router Alarms



Provide Alarm Settings

To provide alarm settings:

Step 1 Provide alarm settings for either (or both) the Threshold Entity Count Alarm and the Threshold Event Rate Alarm.

a. In the Alarm Type field, Crosses Threshold Rate appears by default.

b. Select one of the following radio buttons for the Alarm Severity:

- **Critical**
- **High**
- **Medium**
- **Low**

See Severity Values of Alarms, page 8-61.

c. Enter a percentage in the Threshold % field. By default, the Threshold Percentage value is set to 1, to indicate 1 percent.

d. The Time Window drop-down menu is defaulted to 0.

e. (Optional) Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the selected Alarm displays two triangles, each with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

Configure a BGP Route Alarm

To configure a BGP route alarm:

Step 1 Use the procedure to Start the BGP Alarm Configuration Wizard, page 8-5.

Step 2 Select the **Route** radio button, and click **Next**.

The BGP Alarm Configuration, Route Alarms wizard screen appears.

Step 3 Click **Find Entity** to view all possible BGP routes exchanged by BGP speakers in the selected autonomous system.

or

a. Narrow down your option set by completing any of the following fields before clicking **Find Entity**:
   - In the **AS** field, the autonomous system appears by default.
   - In the **Prefix** field, enter the prefix of the advertised route in the form of an IP address and subnet mask. Example: When you click **Find Entity** for the prefix 1.1.0.0/16, this prefix and the set of more specific prefixes are returned.

b. Click **Find Entity**.

A narrower set of routes is displayed.

(Optional) Click **Add Wildcard** to add options for setting wildcard alarms on routes that match the configuration parameters you selected previously.

Note If you decide to set wildcard alarms on all routes within the selected autonomous system (listed in the **AS** field), manually delete settings you entered in the **Prefix** field, enter an asterisk (*) in the field, and click **Add Wildcard** to set wildcard alarms on all routes in the selected autonomous system.

Set the Alarm Type

To set the alarm type:

Step 1 Double-click one of the following buttons:

- **Availability**—Notifies of changes in the availability of a BGP route or if the route flaps (becomes intermittently available and unavailable in the network). Sets a BGP Route Availability Alarm.
- **Redundancy**—Notifies of changes in the redundancy of a route or if the route flaps (becomes intermittently available and unavailable in the network). A route is redundant when it has more than one way to reach the destination of the route. Sets a BGP Route Redundancy Change alarm.

The Alarms Setting screen appears (see Figure 8-8).

Figure 8-8 Alarms Setting Screen in BGP Route Alarms

Step 2 Provide alarm settings:

- **For the BGP Route Availability Alarm:**

a. Select the degree of specificity to the route to cause the alarm to trigger. In the Alarm On drop-down menu, select one of the following options:

- **Exact**—Alarm will trigger when there is a change in availability of the exact route prefix you entered in the Prefix field.
- **More Specific**—Alarm will trigger when there is a change in availability of a more specific route prefix.
- **Less Specific**—Alarm will trigger when there is a change in availability of a less specific route prefix.
- **Exact Mask Length**—Alarm will trigger when there is a change in the availability of a prefix that has the same mask length as the value you entered.
- **Greater Mask Length**—Alarm will trigger when there is a change in availability of a prefix with a greater mask length than the prefix you entered.
- **Lesser Mask Length**—Alarm will trigger when there is a change in availability of a prefix with a lesser mask length than the prefix you entered.

b. Select one of the following from the Alarm Type drop-down menu:

- **Advertised**—Route is advertised.
- **Withdrawn**—Route is withdrawn.
- **Flap**—Route is intermittently advertised and withdrawn.

Note When you select **Withdrawn** from the Alarm Type drop-down box, you must select either **Normal Withdraw** or **Withdrawn and Non-Reachable** by selecting the appropriate radio button. Normal Withdraw indicates that the route is withdrawn but still reachable through some other less specific prefix. Withdrawn and Non-reachable indicate that the route can no longer be reached even through some other less specific prefix.

- **For a BGP Route Redundancy Alarm:**

a. Select of the following options from the Alarm Type drop-down menu:
   - **Becomes Redundant—**Route is redundant.
   - **Becomes Non Redundant—**Route is not redundant.
   - **Flap**—Route intermittently changes redundancy status.

- **For both BGP Route Availability Alarm and BGP Route Redundancy Alarm:**

b. Select one of the following options for the Alarm Severity radio buttons:
   - **Critical**
   - **High**
   - **Medium**
   - **Low**

   See Severity Values of Alarms, page 8-61.

c. Enter the number of times the change must occur within a selected period of time in the Count field (see Time Window below) to trigger the alarm.

d. Enter the number of seconds for the Count In the Time Window field.

   For information about setting the Count and Time Window see, Time Window for Alarm Triggering, page 8-63.

e. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 3 Click **OK**.

The DBL CLK button under the selected Alarm displays a triangle with a red star, indicating that the alarm has been configured.

Step 4 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 5 Click **Finish**.

Alarms are displayed in the **Alarm** section of the Alarm Monitor window.

Configure a BGP Threshold per AS Alarm

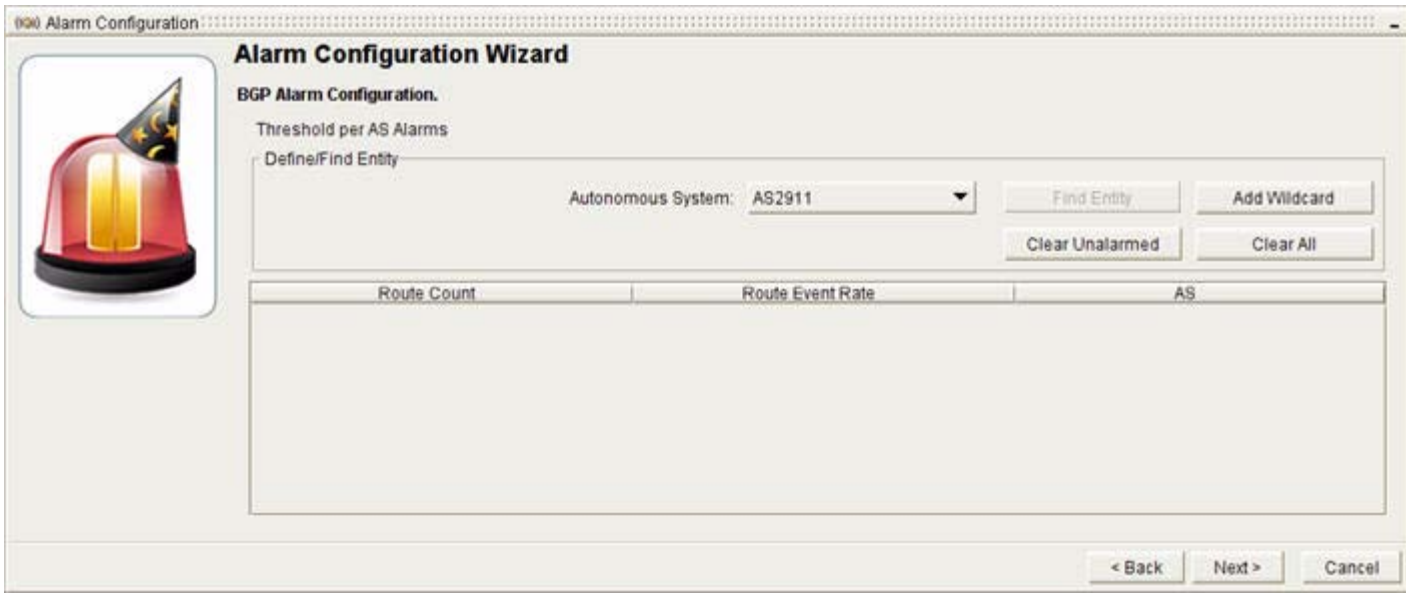
To configure a BGP threshold per AS alarm:

Step 1 Use the procedure to Start the BGP Alarm Configuration Wizard, page 8-5.

Step 2 Select the **Threshold per AS** radio button and click **Next**.

The BGP Alarm Configuration, Threshold per AS Alarms wizard screen appears (see Figure 8-9).

Figure 8-9 Threshold per AS Alarm Screen in BGP Alarm Configuration Wizard



Step 3 Click **Add Wildcard** to set a Threshold per AS alarm on any change in the count of BGP routes or rate of BGP route events.

Set the Alarm Type

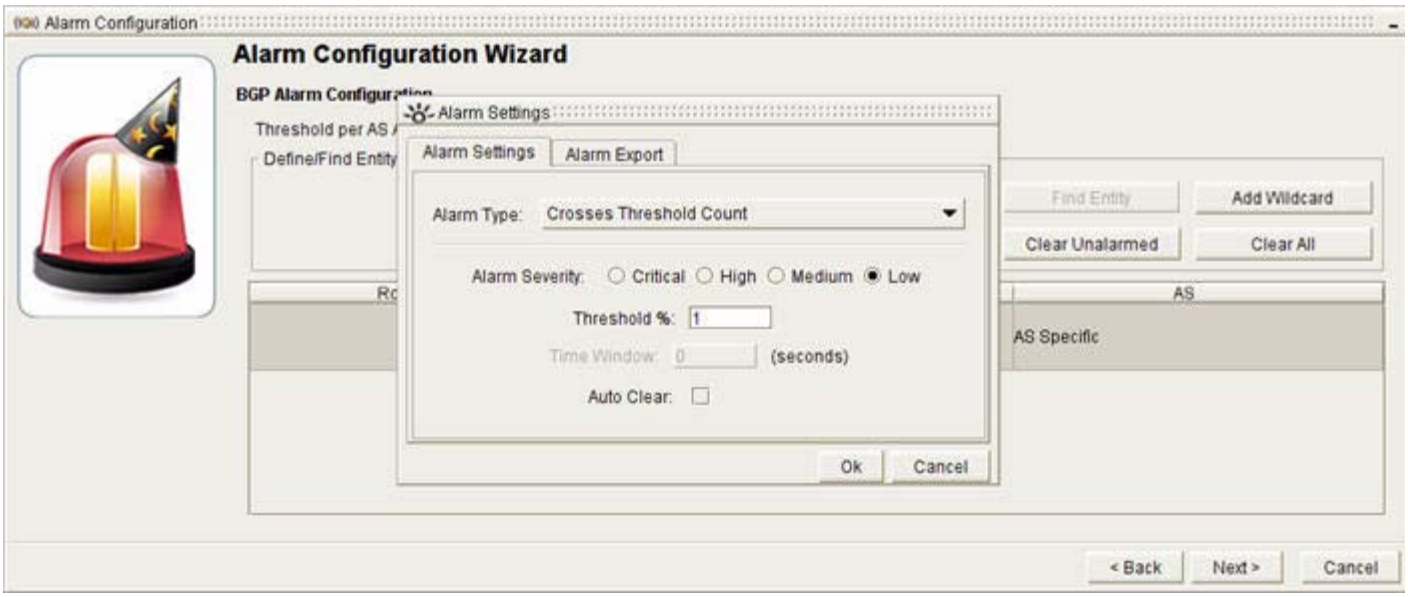
To set the alarm type:

Step 1 Double-click any of the following buttons:

- **Route Count—**This alarm is triggered when the number of routes in an autonomous system deviates from the defined set percentage.
- **Route Event Rate—**This alarm is triggered when the rate of route events in an autonomous system exceeds the threshold by more than the defined percentage.

The Alarm Settings screen appears (see Figure 8-10).

Figure 8-10 Alarm Settings Screen in Threshold per AS Alarms



Step 2 Provide alarm settings:

You can set either or both Threshold Entity Count Alarm and Threshold Event Rate Alarm:

a. **Crosses Threshold Rate** appears by default in the **Alarm Type** drop-down menu.

b. Select one of the following options for the **Alarm Severity** radio buttons:

- **Critical**
- **High**
- **Medium**
- **Low**

See Severity Values of Alarms, page 8-61.

c. Enter a percentage in the Threshold Percentage field.

The Threshold Percentage value is set to 1 by default to indicate one percent.

Note The Time Window setting is not needed for Threshold per AS alarms.

d. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 3 Click **OK**.

The DBL CLK button under the selected Alarm displays two triangles, each with a red star, indicating that the alarm has been configured.

Step 4 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 5 Click **Finish**.

Alarms are displayed in the **Alarm** section of the Alarm Monitor window.

Configure a BGP Next Hop Alarm

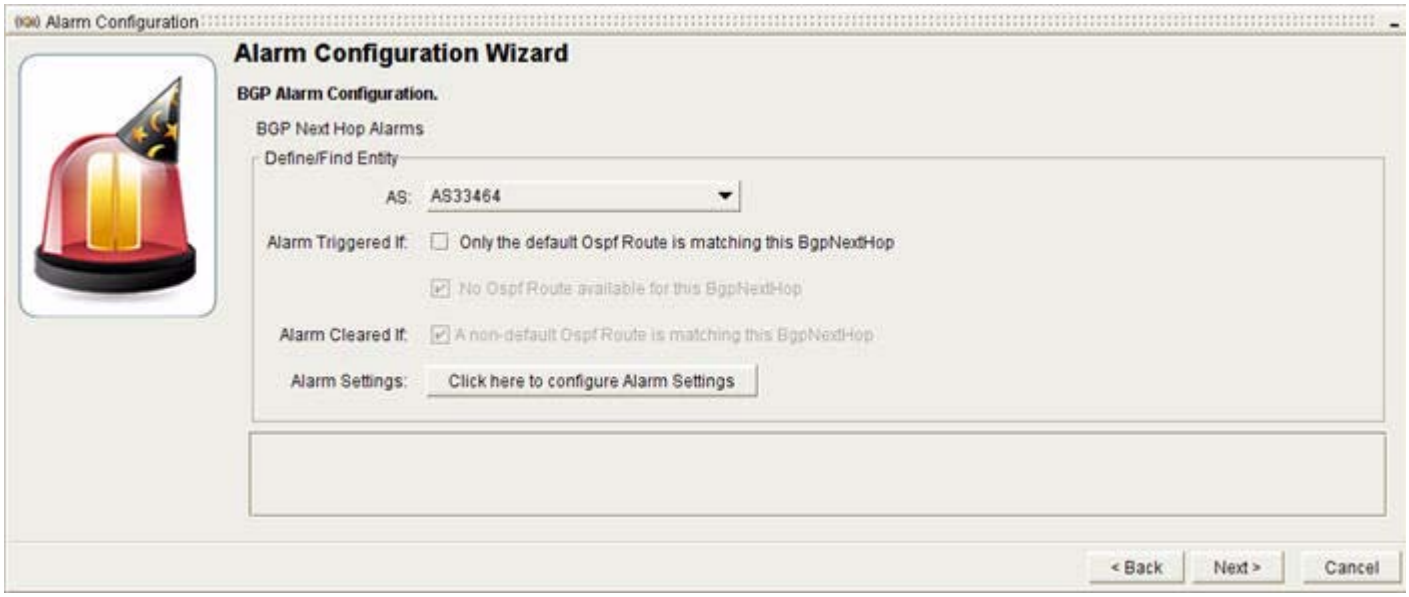
To configure a BGP next hop alarm:

Step 1 Use the procedure to Start the BGP Alarm Configuration Wizard, page 8-5.

Step 2 Select the **BGP Next Hop** radio button and click **Next**.

The BGP Alarm Configuration, Next Hop wizard screen appears (see Figure 8-11).

Figure 8-11 BGP Next Hop Alarm Screen in BGP Alarm Configuration Wizard



Set the Alarm Type and Settings

To set the alarm type and settings:

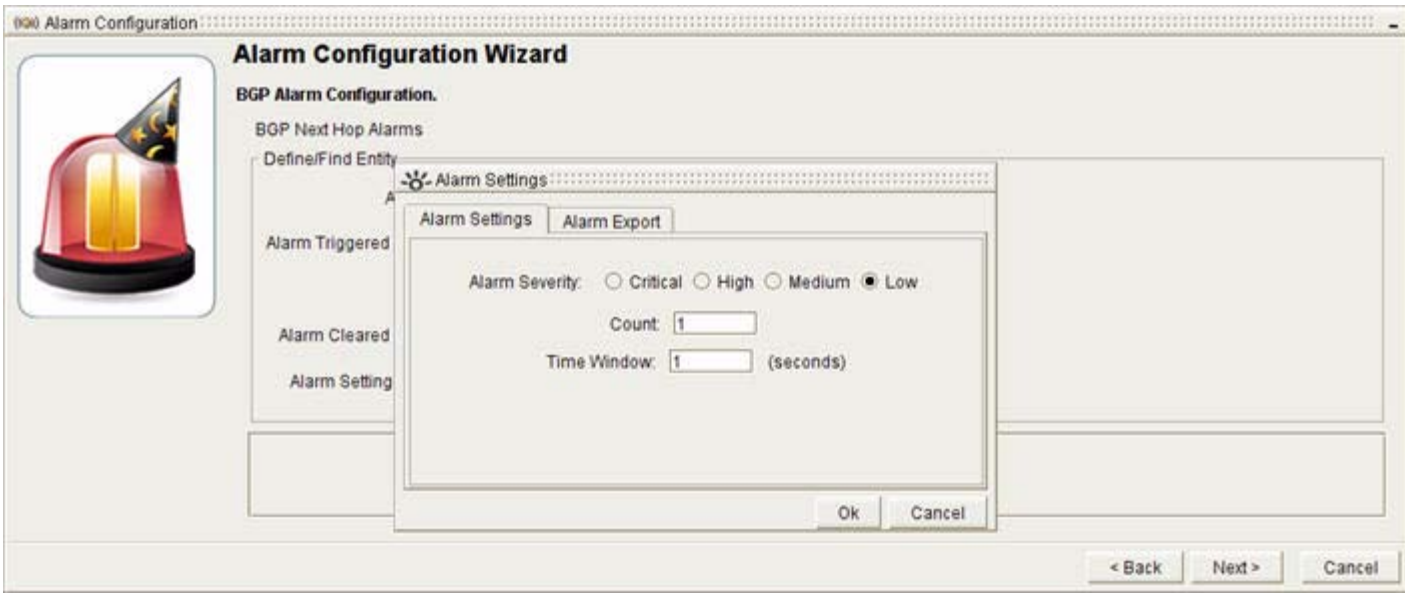
Step 1 Set the alarm type by selecting the **Only the default Ospf Route is matching the BgpNextHop** check box if you want the alarm to trigger only when the default OSPF route is matching the BGP Next Hop

- The alarm will always trigger when there is no OSPF route available.
- The alarm will always clear if a non-default route matches the BGP Next Hop.

Step 2 Click the **Click Configure here to provide Alarm Settings** button.

The Alarm Settings screen appears (see Figure 8-12).

Figure 8-12 Alarm Settings Screen in BGP Next Hop Alarm



Provide Alarm Settings

To provide alarm settings:

Step 1 Provide alarm settings for the BGP Next Hop Alarm.

a. Select one of the following radio buttons for the **Alarm Severity** radio buttons:

- **Critical**
- **High**
- **Medium**
- **Low**

See Severity Values of Alarms, page 8-61.

b. Enter the number of times the change must occur within a selected period of time in the Count field (see Time Window below) to trigger the alarm.

c. Enter the number of seconds for the Count in the Time Window field.

For information about setting the Count and Time Window see, Time Window for Alarm Triggering, page 8-63.

Step 2 Click **OK**.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the **Alarm** section of the Alarm Monitor window.

Configure an OSPF Alarm

To configure an OSPF alarm:

Step 1 Select **Start > Alarm Monitor**.

The Alarm Monitor window appears in the Path Analyzer Management Console. By default, the Monitor tab is selected. If it is not, click the **Monitor** tab.

Step 2 Select a domain from the Enterprise hierarchy on the left side.

Start the OSPF Alarm Configuration Wizard

To start the OSPF alarm configuration wizard, click **Configure Alarms**. in the Alarm Monitor toolbar.

The Alarm Configuration wizard appears, featuring options for OSPF alarms (see Figure 8-13).

Figure 8-13 OSPF Alarm Configuration Wizard

Select a Category of OSPF Alarms

To select a category of OSPF alarms:

Step 1 Select the type of alarm to create by selecting the appropriate radio button:

- **Interface—**Set alarms on NP2P, UP2P, and transit interfaces. See Configure an OSPF Interface Alarm, page 8-20.
- **Router**—Set alarms on a router. See Configure an OSPF Router Alarm, page 8-24.
- **Transit Network**—Set alarms on a Transit network. See Configure an OSPF Transit Network Alarm, page 8-27.
- **Advertisement**—Set alarms on an OSPF advertisement. See Configure an OSPF Advertisement Alarm, page 8-30.
- **Route—**Set alarms on a route. See Configure an OSPF Route Alarm, page 8-34.
- **Threshold**—Set threshold alarms on the following entities: routers, external routes, stub routes, Transit networks, numbered point-to-point interfaces, unnumbered point-to-point interfaces, and transit interfaces. This alarm is triggered when the behavior of an entity deviates from the system-perceived behavior by a certain percentage defined by the user. See Configure a Threshold Alarm, page 8-37.
- **Errors**—Set alarms on Internet addressing conflicts, such as the assignment of the same IP address to two different interfaces in the same area. See Configure an Error Alarm, page 8-40.

Step 2 Click **Next**.

A configuration wizard appears for the type of alarm you have selected.

Configure an OSPF Interface Alarm

Step 1 Use the procedure to Start the OSPF Alarm Configuration Wizard, page 8-19.

Step 2 Select the **Interface** radio button and click **Next**.

The OSPF Alarm Configuration, Interface Alarms wizard screen appears (see Figure 8-14).

Figure 8-14 Interface Alarms Screen in OSPF Alarm Configuration Wizard

Choose Interfaces Type(s)

Step 1 Select one or more of the following interface types:

- **Numbered P2P**—To set an alarm on one or more, selected or all, NP2P interfaces.
- **Unnumbered P2P**—To set an alarm on one or more, selected or all, UP2P interfaces.
- **Transit—**To set an alarm on one or more, selected or all, Transit interfaces.

By default, an asterisk (*) is displayed as a wildcard in the Interface or MIB, Neighbor Name, Area, and Router Name fields.

Step 2 Click **Find Entity** to view all possible interfaces of the selected type(s) in the domain.

or

a. Narrow down your option set by completing any of the following fields before clicking **Find Entity**:

- In the Domain field, the domain is displayed by default.
- In the Interface or MIB field, enter an IP address of an NP2P interface or Transit address or an integer that represents the MIB index of a UP2P interface.
  - If you previously selected both NP2P and UP2P options and entered an IP address of an NP2P interface in the Interface or MIB field, you will let the wizard apply a wildcard for all UP2P interfaces.
  - If you previously selected both NP2P and UP2P options and entered an integer that represents the MIB Index value of a UP2P interface in the Interface or MIB field, you will let the wizard apply a wildcard value for all NP2P interfaces.
  - The Interface or MIB value for a transit interface is always a wildcard, regardless of the value you enter.
- In the Neighbor Name field, enter the Router ID of the neighboring router that shares the NP2P or UP2P link.
- In the Area field, enter the area in which the interface resides.
- In the Router Name field, enter the Router ID or hostname of the router configured with the interface.

b. Click **Find Entity**.

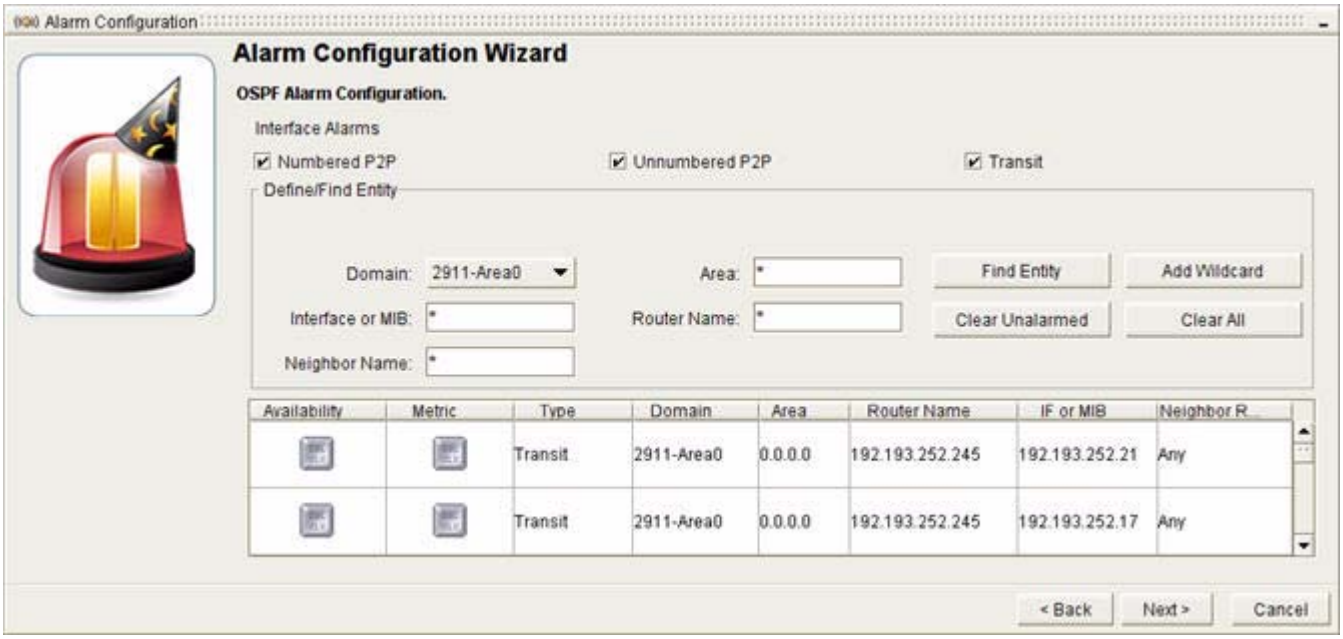
A specific set of interfaces or a single interface is displayed.

Step 3 (Optional) Click **Add Wildcard** to add options for setting wildcard alarms on interfaces that match the configuration parameters you selected previously.

Note If you decide to set wildcard alarms on all interfaces within the selected domain (listed in the Domain field), manually delete settings you entered in the Interface or MIB, Neighbor Name, Area, or Router Name fields, enter an asterisk (*) in each field, and click **Add Wildcard** to set wildcard alarms on all interfaces in the selected OSPF area.

Set the Alarm Type

Figure 8-15 Interface Alarm Screen Showing Selected Interfaces in OSPF Alarm Configuration Wizard

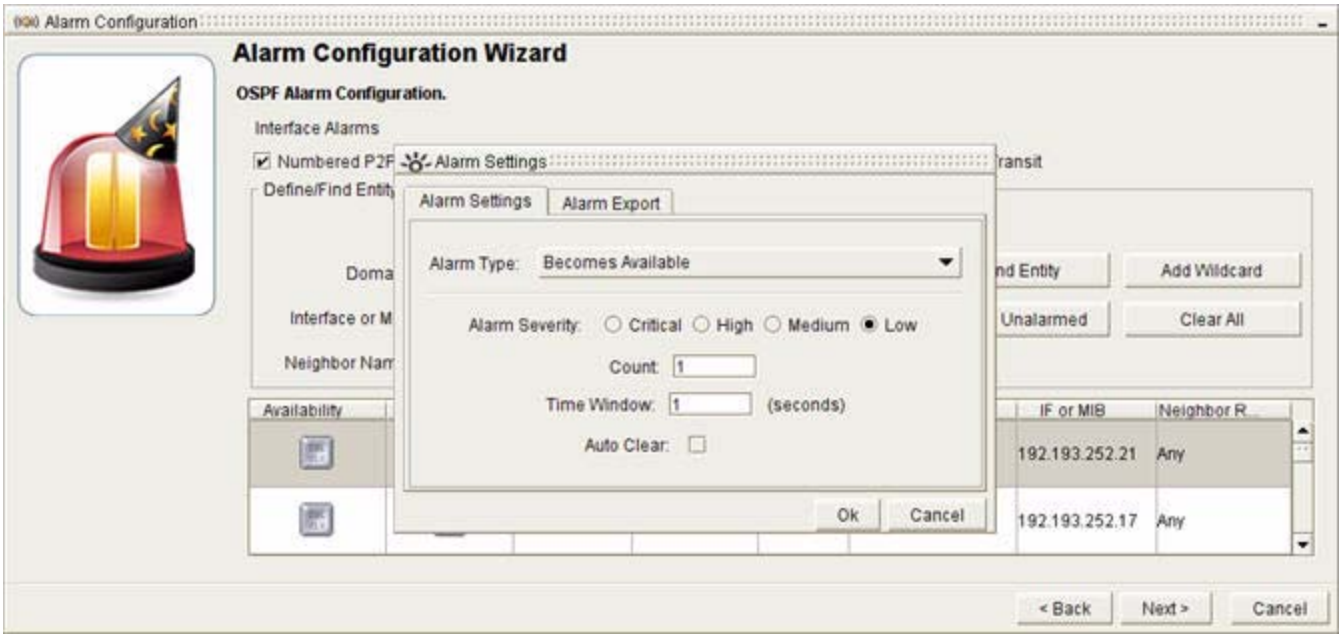


To set the alarm type, double-click any of the following buttons (see Figure 8-15):

- **Availability**
- **Metric**

The Alarm Settings screen appears (see Figure 8-16).

Figure 8-16 Alarm Settings Screen for Interface Availability Alarm



Provide Alarm Settings

To provide alarm settings:

Step 1 Provide alarm settings. For the Interface Availability Alarm, complete steps a–e, below. For the Interface Metric Change Alarm, complete steps b–d, below.

a. Select the Alarm Type from the drop-down menu. Alert with notifications if the interface:
   - **Becomes Available.**
   - **Becomes Unavailable.**
   - **Flap**—Intermittently becomes available and unavailable.

b. Select one of the following options for the **Alarm Severity** radio buttons:
   - **Critical**
   - **High**
   - **Medium**
   - **Low**

   See Severity Values of Alarms, page 8-61.

c. Enter the number of times the change must occur within a selected period of time in the Count field (see Time Window below) to trigger the alarm.

d. Enter the number of seconds for the Count In the Time Window field.

   For information about setting the Count and Time Window, see Time Window for Alarm Triggering, page 8-63.

e. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the Interface Availability Alarm (if selected) displays a triangle with a red star, indicating that the alarm has been configured.

The DBL CLK button under the Interface Metric Alarm (if selected) displays two triangles, each with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

Configure an OSPF Router Alarm

To configure an OSPF router alarm:

Step 1 Use the procedure to Start the OSPF Alarm Configuration Wizard, page 8-19.

Step 2 Select the **Router** radio button and click **Next**.

The OSPF Alarm Configuration, Router Alarms wizard screen appears (see Figure 8-17).

- The **Router** check box is selected, by default.
- An asterisk (*) is displayed as a wildcard in the Router Name field by default.

Figure 8-17 Router Alarm Screen in OSPF Alarm Configuration Wizard

Define/Find Entity

To find and define entities:

Step 1 Click **Find Entity** to view all possible routers in the domain.

or

a. Narrow down your option set by completing any of the following fields before clicking **Find Entity**:

- In the Domain field, the domain appears by default.
- In the Router Name field, enter the Router ID or hostname of the router configured with the interface.

b. Click **Find Entity**.

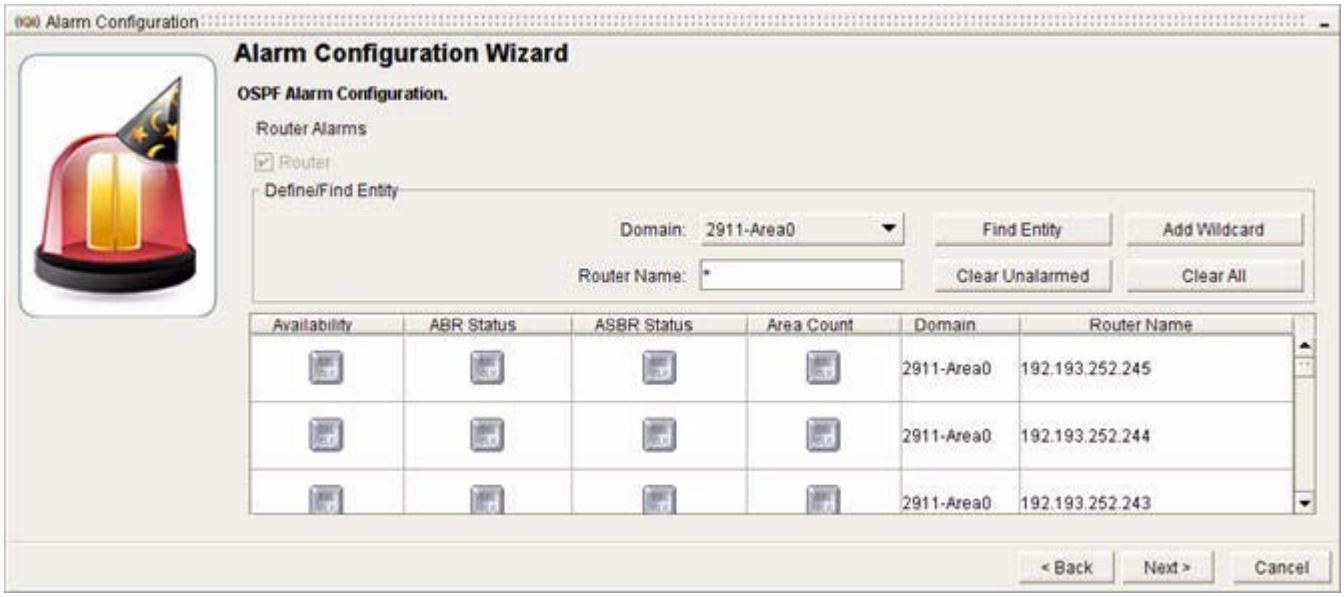
A narrower set of routers or a single router is displayed.

Step 2 (Optional) Click **Add Wildcard** to add options for setting wildcard alarms on routers that match the configuration parameters you selected previously.

Note If you decide to set wildcard alarms on all routers within the selected domain (listed in the Domain field), manually delete settings you entered in the Router Name field, enter an asterisk (*) the field, and click **Add Wildcard** to set wildcard alarms on all routers in the selected OSPF area.

Set the Alarm Type

Figure 8-18 Router Alarm Screen Showing Alarm Options in OSPF Alarm Configuration Wizard

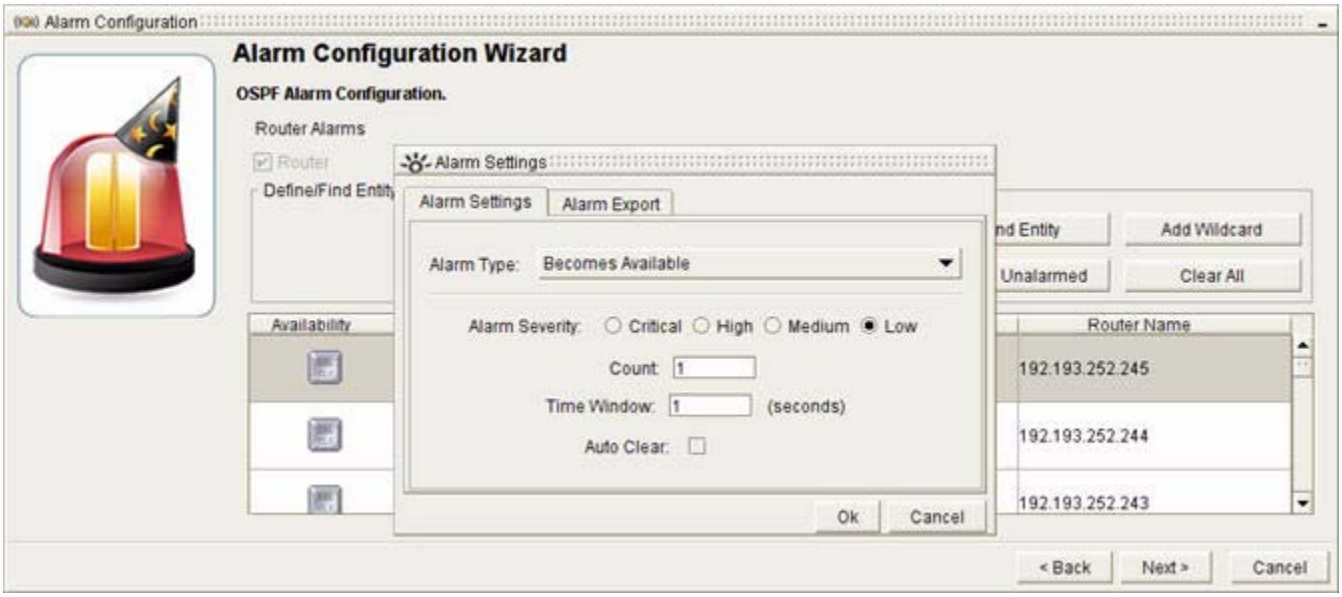


To set the alarm type, double-click any of the following buttons (see Figure 8-18):

- **Availability**
- **ABR Status**
- **ASBR Status**
- **Area Count**

Provide Alarm Settings

Figure 8-19 Alarm Settings Screen for OSPF Router Alarm



To provide alarm settings (see Figure 8-19):

Step 1 Provide alarm settings. (The Area Count Alarm does not support Steps a. and e., below.)

a. Select from the Alarm Type drop-down menu, alert with notifications if the interface:

- **Becomes Available.**
- **Becomes Unavailable.**
- **Flap**—Intermittently becomes available and unavailable.

b. Select one of the following options for the Alarm Severity radio buttons:

- **Critical**
- **High**
- **Medium**
- **Low**

See Severity Values of Alarms, page 8-61.

c. Enter the number of times the change must occur within a selected period of time (see Time Window below) to trigger the alarm in the Count field.

d. Enter the number of seconds for the Count in the Time Window field.

For information about setting the Count and Time Window, see Time Window for Alarm Triggering, page 8-63.

e. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK buttons under the Availability, ABR Status, and ASBR Status alarms (if selected) displays a triangle with a red star, indicating that the alarm has been configured.

The DBL CLK button under the Area Count Alarm (if selected) displays two triangles, each with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

Configure an OSPF Transit Network Alarm

To configure an OSPF transit network alarm:

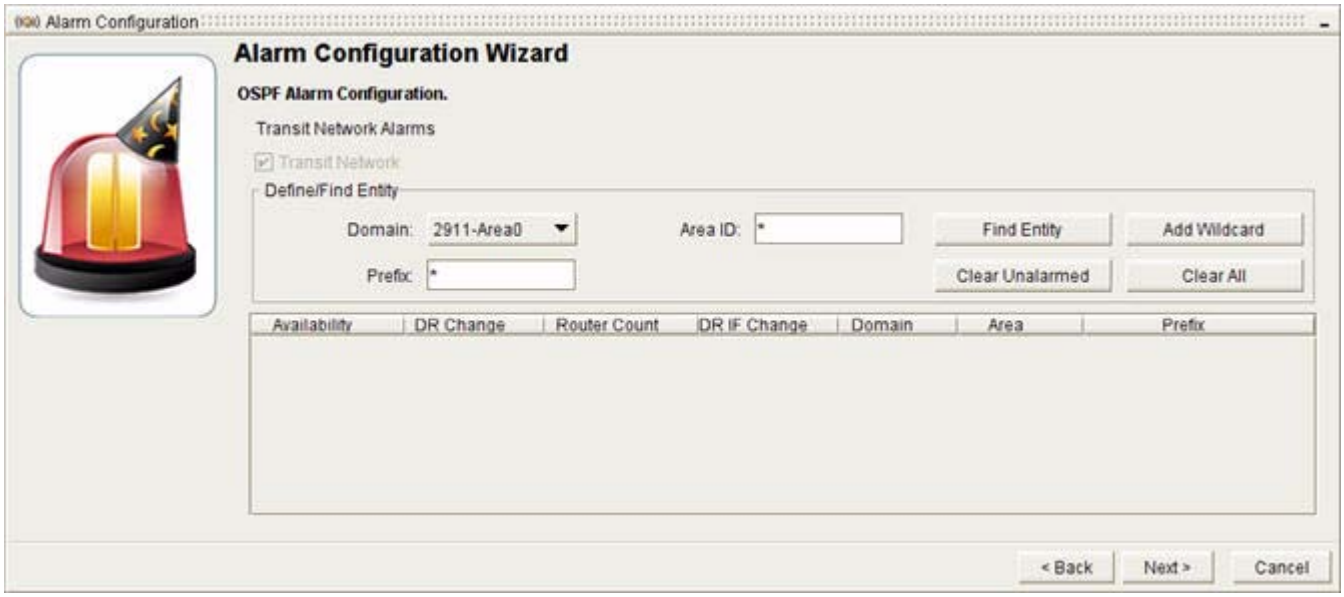
Step 1 Use the procedure to Start the OSPF Alarm Configuration Wizard, page 8-19.

Step 2 Select the **Transit Network** radio button and click **Next**.

The OSPF Alarm Configuration, Transit Network Alarms Wizard screen appears (see Figure 8-20).

- The **Transit Network** check box is selected, by default.
- An asterisk (*) is displayed as a wildcard in the Prefix and Area ID fields, by default.

Figure 8-20 Transit Network Alarm Screen in OSPF Alarm Wizard



Define/Find Entity

To find and define entities:

Step 1 Click **Find Entity** to view all possible Transit networks in the domain.

or

a. Narrow down your option set by completing any of the following fields before clicking **Find Entity**:
   - In the Domain field, the domain in which the Transit network is located appears by default.
   - In the Prefix field, enter the IP address and subnet mask of the Transit network. Example: `10.10.0.1/24`
   - In the Area ID field, enter the Area in which the Transit network is located.

b. Click **Find Entity**.

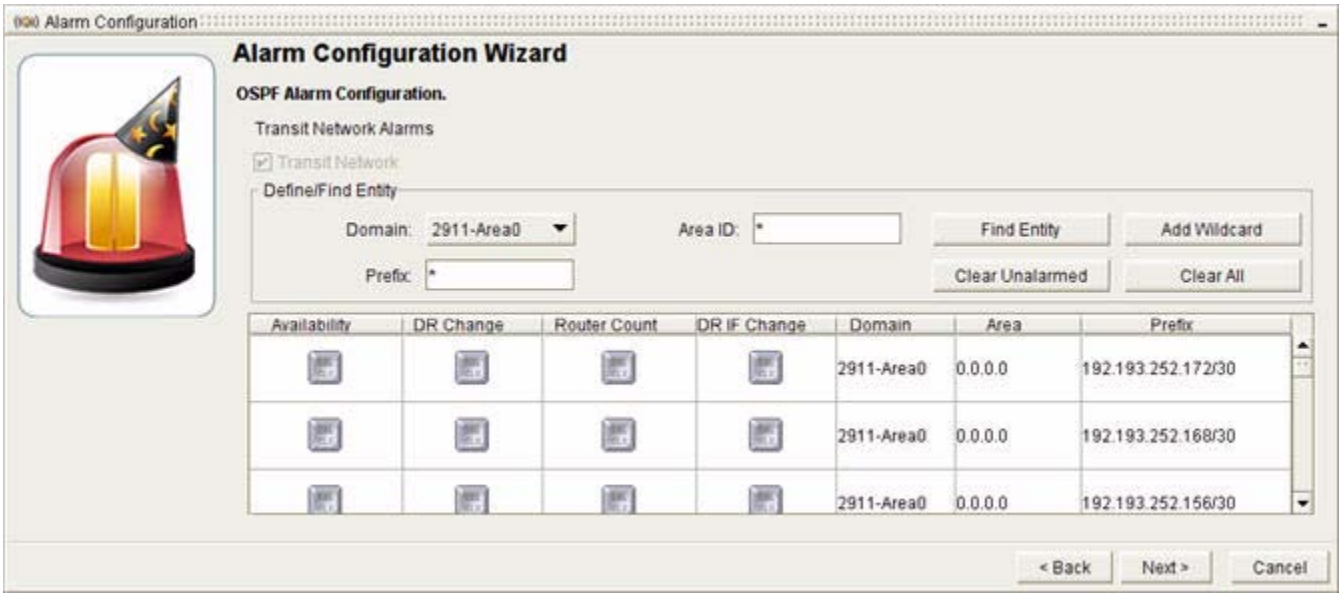
   A narrower set of Transit networks or a single Transit network is displayed.

Step 2 (Optional) Click **Add Wildcard** to add options for setting wildcard alarms on Transit networks that match the configuration parameters you previously selected.

Note If you decide to set wildcard alarms on all Transit networks within the selected domain (listed in the Domain field), manually delete settings you entered in the Prefix and Area ID fields, enter an asterisk (*) in each field, and click **Add Wildcard** to set wildcard alarms on all Transit networks in the selected OSPF area.

Set the Alarm Type

Figure 8-21 Transit Network Alarm Screen Showing Alarm Options in OSPF Alarm Configuration Wizard

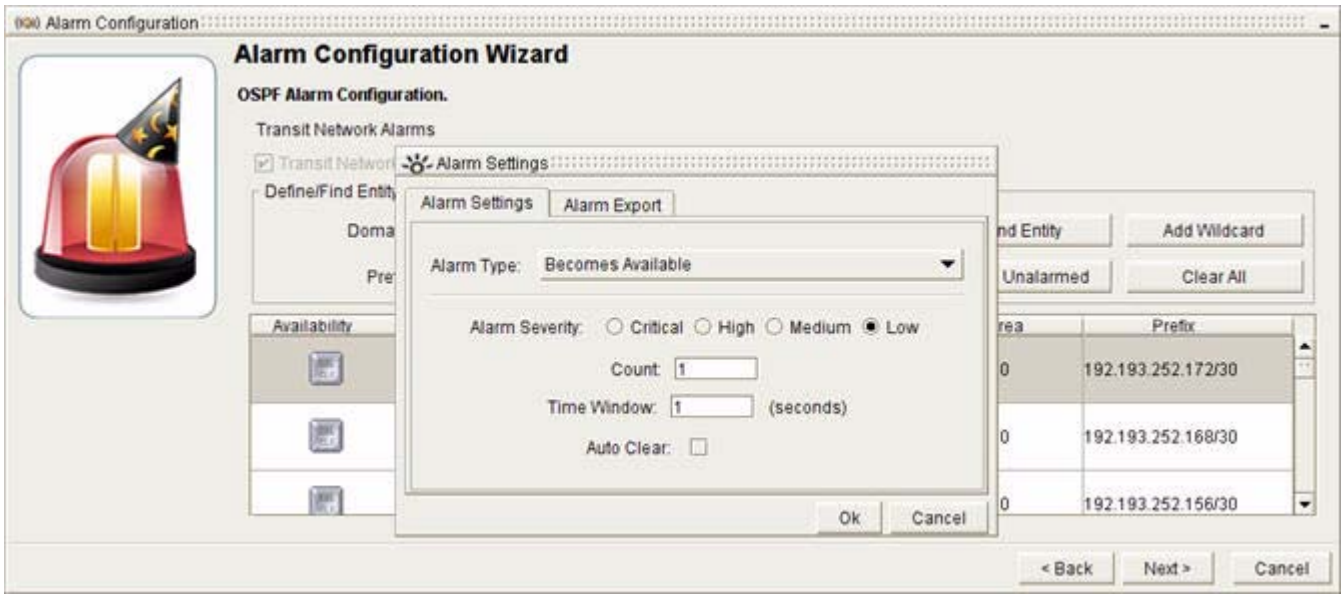


To set the alarm type, double-click any of the following buttons (see Figure 8-21):

- **Availability**
- **DR Change**
- **Router Count**
- **DR IF Change**

Provide Alarm Settings

Figure 8-22 Settings Screen in Transit Network Alarms



To provide alarm settings (see Figure 8-22):

Step 1 Provide alarm settings. (Only the Availability Alarm supports Steps a and e, below.)

a. Select the Alarm Type from the drop-down menu, alert with notifications if the interface:

- **Becomes Available.**
- **Becomes Unavailable.**
- **Flap**—Intermittently becomes available and unavailable.

b. Select one of the following options from the Alarm Severity field:

- **Critical**
- **High**
- **Medium**
- **Low**

See Severity Values of Alarms, page 8-61.

c. Enter the number of times the change must occur within a selected period of time (see Time Window below) to trigger the alarm in the Count field.

d. Enter the number of seconds for the Count in the Time Window field.

For information about setting the Count and Time Window, see Time Window for Alarm Triggering, page 8-63.

e. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the Available Alarm (if selected), displays a triangle with a red star, indicating that the alarm has been configured.

The DBL CLK buttons under the DR Change, Router Count, and DR IF Change alarms (if selected), displays two triangles, each with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

Configure an OSPF Advertisement Alarm

To configure an OSPF advertisement alarm:

Step 1 Use the procedure to Start the OSPF Alarm Configuration Wizard, page 8-19.

Step 2 Select the **Advertisement** radio button and click **Next**.

The OSPF Alarm Configuration, Advertisement Alarms wizard screen appears (see Figure 8-23).

Figure 8-23 Advertisement Alarms Screen in OSPF Alarm Configuration Wizard

Step 3 Select the Advertisement type(s) by clicking the check box(es):

- **Stub**—Sets alarms on advertisements of routes with destinations inside a Stub network.
- **External**—Sets alarms on advertisements of routes with destinations inside an External network.

An asterisk (*) is displayed as a wildcard in the Prefix, Area ID and Router Name fields, by default.

Step 4 Click **Find Entity** to view all possible stub or external route advertisements in the domain.

or

a. Narrow down your option set by completing any of the following fields before clicking **Find Entity**:

- In the Domain field, enter the domain in which the advertisement is appears by default.
- In the Prefix field, enter the IP address and subnet mask of the stub or external network that is advertised in the route advertisement. Example: `10.10.0.1/24`
- In the Area ID field, enter the Area advertised in the route advertisement.
- In the Router Name field, enter the router ID of the router that advertises the route, and issues the route advertisement.

b. Click **Find Entity**.

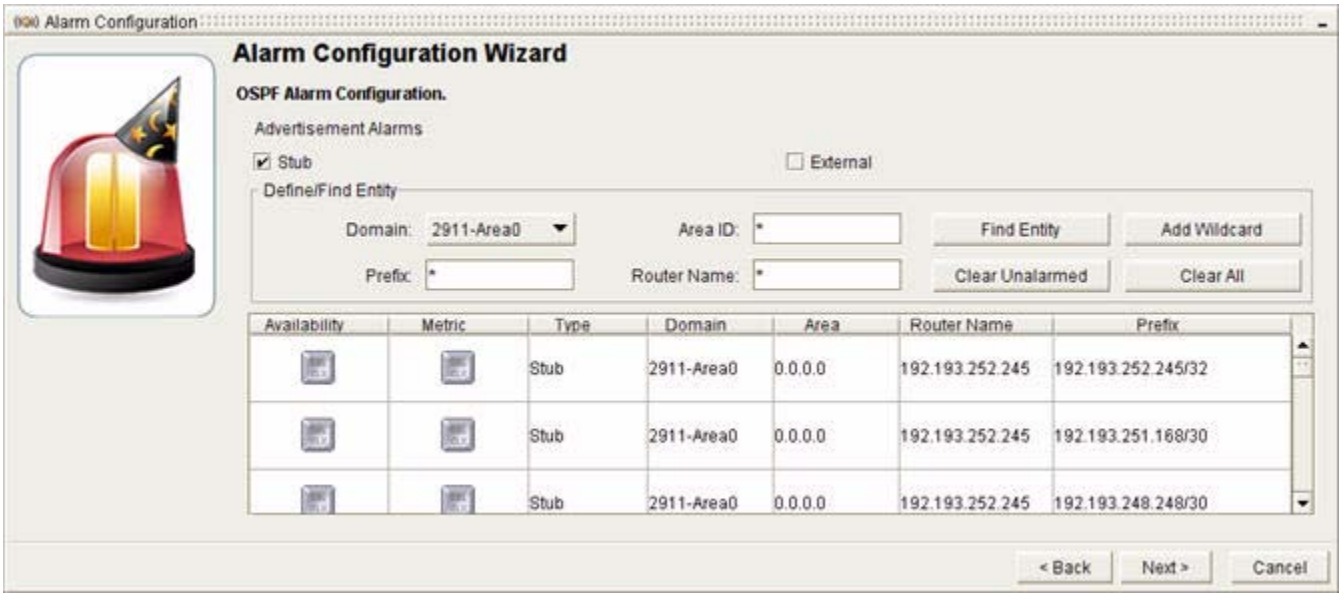
A narrower set of route advertisements is displayed.

Step 5 (Optional) Click **Add Wildcard** to add options for setting wildcard alarms on advertisements that match the configuration parameters you selected previously.

Note If you decide to set wildcard alarms on all advertisements within the selected domain (listed in the Domain field), manually delete settings you entered in the Prefix, Area ID, and Router Name fields, enter an asterisk (*) in each field, and click **Add Wildcard** to set wildcard alarms on all advertisements of selected type(s) (Stub or External or both) in the selected OSPF area.

Set the Alarm Type

Figure 8-24 Advertisement Alarm Screen Showing Alarm Options in OSPF Alarm Configuration Wizard

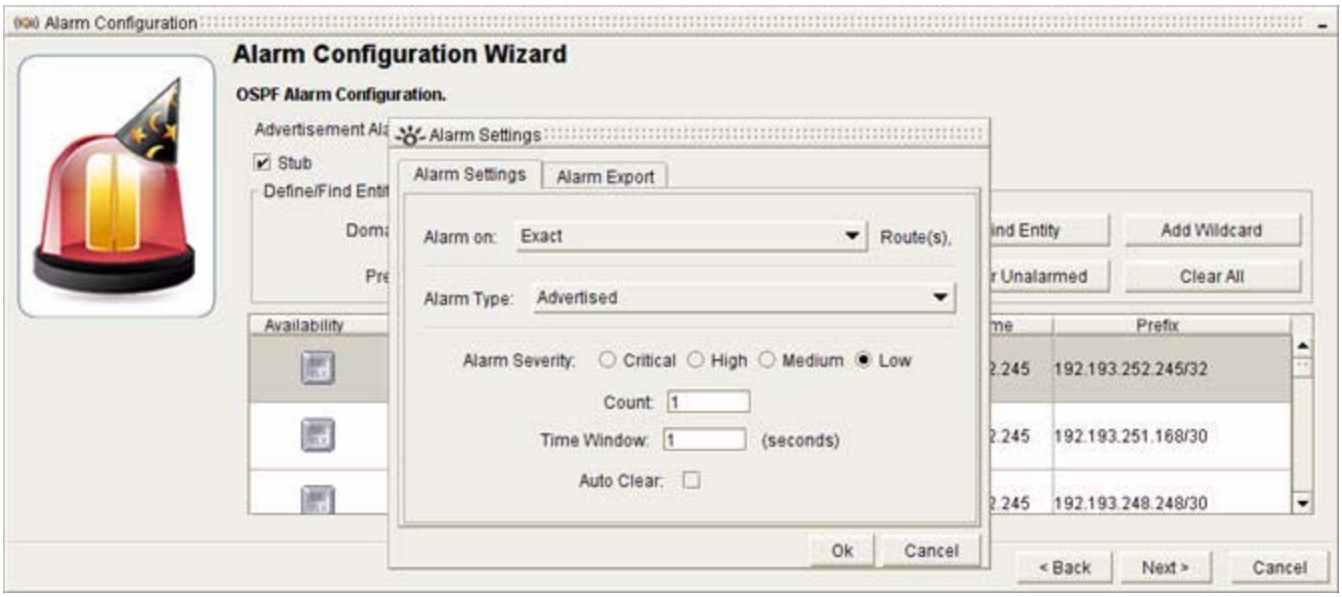


To set the alarm type, double-click any of the following buttons (see Figure 8-24):

- **Availability**
- **Metric**

Provide Alarm Settings

Figure 8-25 Alarm Settings Screen in Advertisement Alarms



To provide alarm settings (see Figure 8-25):

Step 1 Provide alarm settings. (The Metric Alarm does not support Steps a, b, and f, below.)

a. Select the degree of specificity to the route to cause the alarm to trigger. In the Alarm on drop-down menu, select one of the following options:

- **Exact**—Causes the alarm to trigger when there is a change in availability of the exact route prefix you entered in the Prefix field.
- **More Specific**—Causes the alarm to trigger when there is a change in availability of a more specific route prefix.
- **Less Specific**—Causes the alarm to trigger when there is a change in availability of a less specific route prefix.
- **Exact Mask Length**—Causes the alarm to trigger when there is a change in the availability of a prefix that has the same mask length as the value you entered.
- **Greater Mask Length**—Causes the alarm to trigger when there is a change in availability of a prefix with a greater mask length than the prefix you entered.
- **Lesser Mask Length**—Causes the alarm to trigger when there is a change in availability of a prefix with a lesser mask length than the prefix you entered.

b. Select one of the following in the Alarm Type drop-down menu:

- **Advertised**—Route is advertised.
- **Withdrawn**—Route is withdrawn.
- **Flap**—Route is intermittently advertised and withdrawn.

c. Select one of the following options for the Alarm Severity radio buttons:

- **Critical**
- **High**
- **Medium**
- **Low**

  See Severity Values of Alarms, page 8-61.

d. Enter the number of times the change must occur within a selected period of time (see Time Window below) to trigger the alarm in the Count field.

e. Enter the number of seconds for the Count in the Time Window field.

For information about setting the Count and Time Window, see Time Window for Alarm Triggering, page 8-63.

f. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the Availability Alarm (if selected), displays a triangle with a red star, indicating that the alarm has been configured.

The DBL CLK under the Metric Alarm (if selected), displays two triangles, each with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**. Alarms are displayed in the Alarm section of the Alarm Monitor window.

Configure an OSPF Route Alarm

Step 1 Use the procedure to Start the OSPF Alarm Configuration Wizard, page 8-19.

Step 2 Select the **Route** radio button and click **Next**.

- The Alarm Settings dialog box for Router Alarms wizard screen appears (see Figure 8-26).
- An asterisk (*) is displayed as a wildcard in the **Prefix** field, by default.

Figure 8-26 Route Alarm Screen in OSPF Alarm Configuration Wizard

Select the Route Type

To select the route type:

Step 1 Select one or both of the following route types by clicking the check box(es):

- **Core**—Sets alarms to detect changes to routes with destinations inside an autonomous system.
- **External—**Sets alarms to detect changes to routes with destinations in an external autonomous system.

Step 2 Click **Find Entity** to view all possible core or external routes in the domain.

or

a. Narrow down your option set by completing any of the following fields before clicking **Find Entity**:

- In the Domain field, the domain that contains the destination of the route appears by default.
- In the Prefix field, enter the prefix of the route in the form of an IP address and subnet mask. Example: `10.10.0.1/24`

b. Click **Find Entity**.

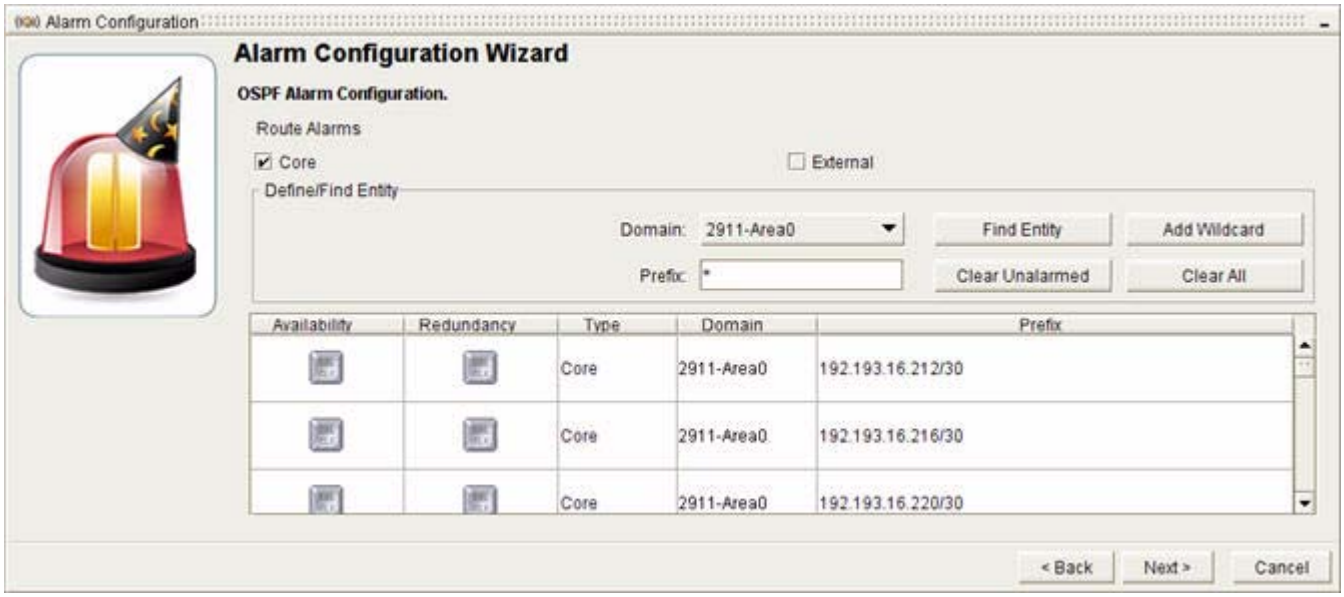
A narrower set of advertisements is displayed.

Step 3 (Optional) Click **Add Wildcard** to add options for setting wildcard alarms on routes that match the configuration parameters you selected previously.

Note If you decide to set wildcard alarms on all routes within the selected domain (listed in the Domain field), manually delete settings you entered in the Prefix field, enter an asterisk (*) in the field, and click **Add Wildcard** to set wildcard alarms on all routes in the selected OSPF area.

Set the Alarm Type

Figure 8-27 Route Alarm Screen Showing Alarm Options in OSPF Alarm Configuration Wizard

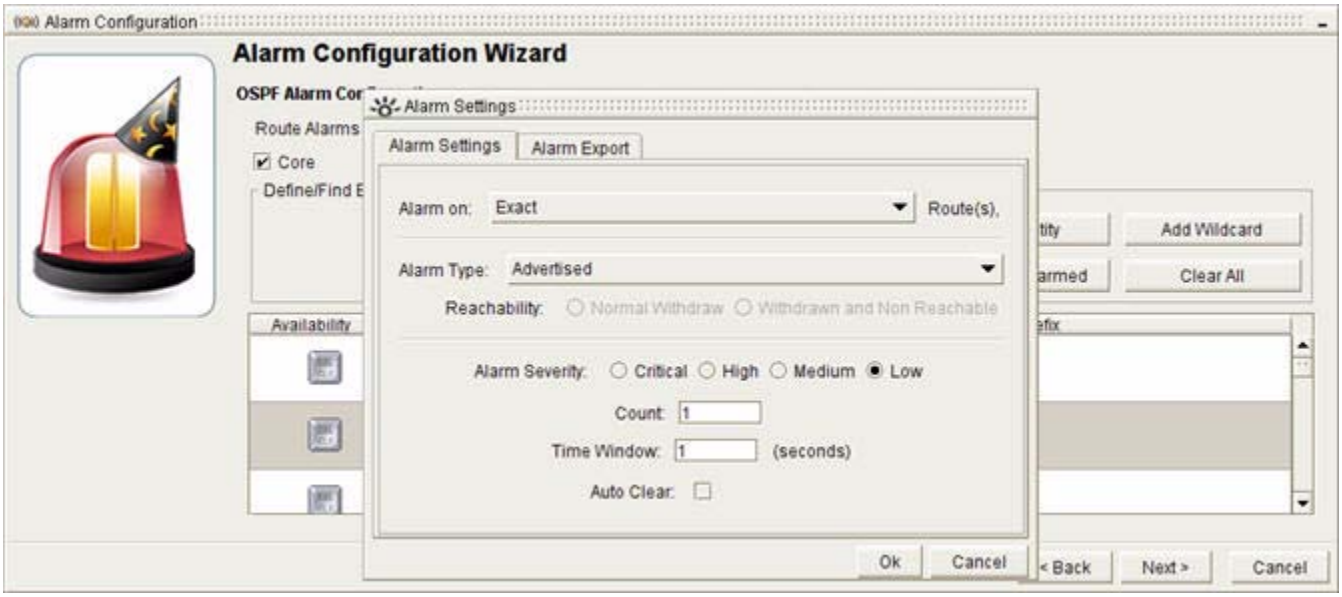


To set the alarm type, double-click any of the following buttons (see Figure 8-27):

- **Availability**
- **Redundancy**

Provide Alarm Settings

Figure 8-28 Alarm Settings Screen in Route Alarms



To provide alarm settings (see Figure 8-28):

Step 1 Provide alarm settings.

- **For an Availability Change Alarm:**

a. Select the degree of specificity to the route to cause the alarm to trigger. In the Alarm on drop-down menu, select one of the following options:

  - **Exact**—Causes the alarm to trigger when there is a change in availability of the exact route prefix you entered in the Prefix field.
  - **More Specific**—Causes the alarm to trigger when there is a change in availability of a more specific route prefix.
  - **Less Specific**—Causes the alarm to trigger when there is a change in availability of a less specific route prefix.
  - **Exact Mask Length**—Causes the alarm to trigger when there is a change in the availability of a prefix that has the same mask length as the value you entered.
  - **Greater Mask Length**—Causes the alarm to trigger when there is a change in availability of a prefix with a greater mask length than the prefix you entered.
  - **Lesser Mask Length**—Causes the alarm to trigger when there is a change in availability of a prefix with a lesser mask length than the prefix you entered.

b. Select one of the following in the Alarm Type drop-down menu:

  - **Advertised**—Is advertised.
  - **Withdrawn**—Is withdrawn.
  - **Flap**—Is intermittently advertised and withdrawn.

- **For a Redundancy Change Alarm only:**

a. Select one of the following from the Alarm Type drop-down menu:
   - **Become Redundant**—Is redundant.
   - **Becomes Non Redundant**—Is not redundant.
   - **Flap**—Changes intermittently from redundant to non-redundant.

- **For a Route Availability or Redundancy Change Alarm**

b. Select one of the following options from the Alarm Severity radio buttons:
   - **Critical**
   - **High**
   - **Medium**
   - **Low**

   See Severity Values of Alarms, page 8-61.

c. Enter the number of times for changes to occur in the time window before triggering the alarm in the Count field.

   By default, the Count value is set to 1 to indicate one change within the time window.

d. Enter the Time Window, the number of seconds for the count.

   By default, the Time Window value is set to 1 to indicate a one-second time window. For information about setting the Count and Time Window, see Time Window for Alarm Triggering, page 8-63.

e. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the Availability Change Alarm or Redundancy Change Alarm (if selected), displays a triangle with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

Configure a Threshold Alarm

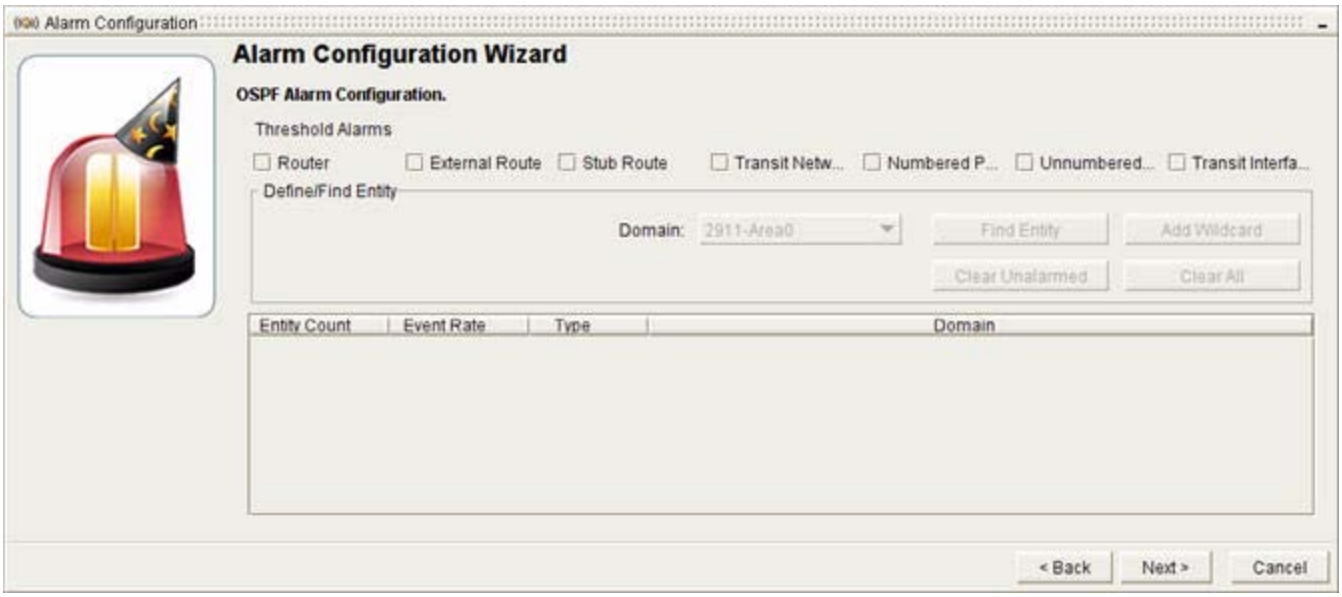
To configure a threshold alarm:

Step 1 Use the procedure to Start the OSPF Alarm Configuration Wizard, page 8-19.

Step 2 Select the **Threshold** radio button and click **Next**.

The Alarm Settings dialog box for Threshold Alarms wizard screen appears (see Figure 8-29).

Figure 8-29 Threshold Alarm Screen in OSPF Alarm Configuration Wizard



Select Alarm Object(s)

To select the alarm object(s):

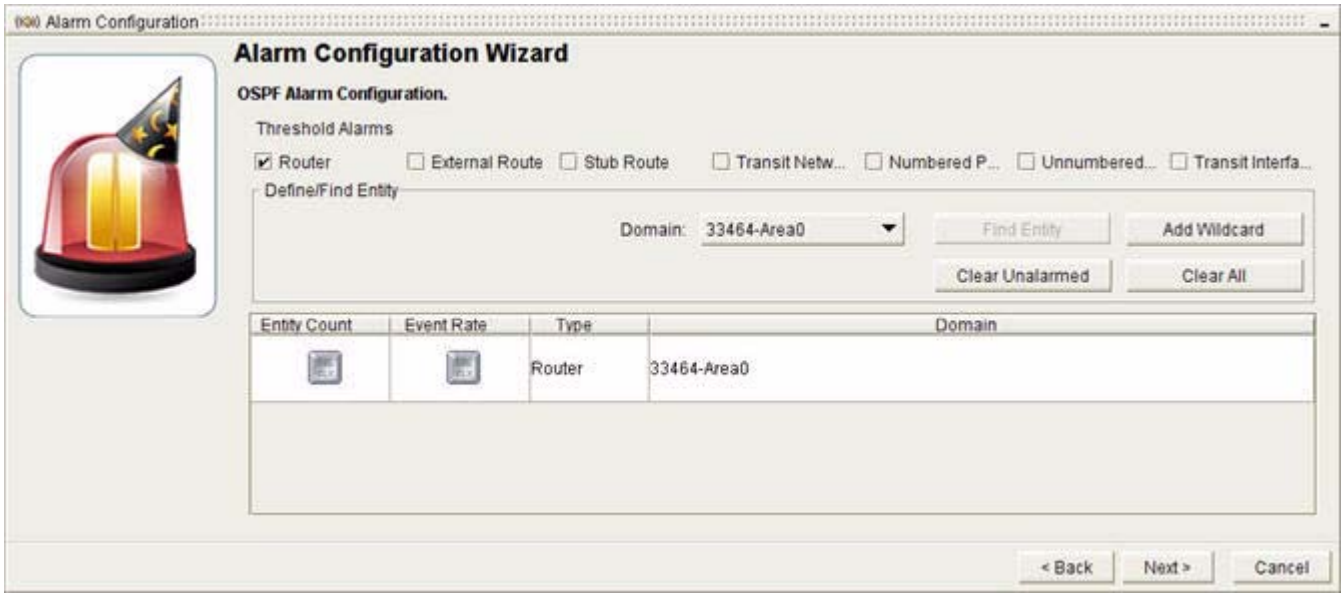
Step 1 Select one or more of the following options by selecting the check boxes:

- **Router**—Sets alarms to detect percentage deviation from normal values in the number of routers or the rate of router events.
- **External Route—**Sets alarms to detect percentage deviation from the normal values in the number of External routes or the rate of External route events.
- **Stub Route—**Sets alarms to detect percentage deviation from the normal values in the number of Stub routes or the rate of Stub route events.
- **Transit Network—**Sets alarms to detect percentage deviation from the normal values in the number of Transit networks or the rate of Transit network events.
- **Numbered Point-to-Point Interface—**Sets alarms to detect percentage deviation from the normal values in the number of Numbered Point-to-Point interfaces or the rate of Numbered Point-to-Point interface events.
- **Unnumbered Point-to-Point Interface—**Sets alarms to detect percentage deviation from the normal values in the number of Unnumbered Point-to-Point interfaces or the rate of Unnumbered Point-to-Point interface events.
- **Transit Interface—**Sets alarms to detect percentage deviation from the normal values in the number of Transit interfaces or the rate of Transit interface events.

Step 2 Click **Add Wildcard** to add an entity type. Multiple entity types can be added by checking the boxes corresponding to the entity types.

Set the Alarm Type

Figure 8-30 Threshold Alarm Screen Showing Alarm Options in OSPF Alarm Configuration Wizard

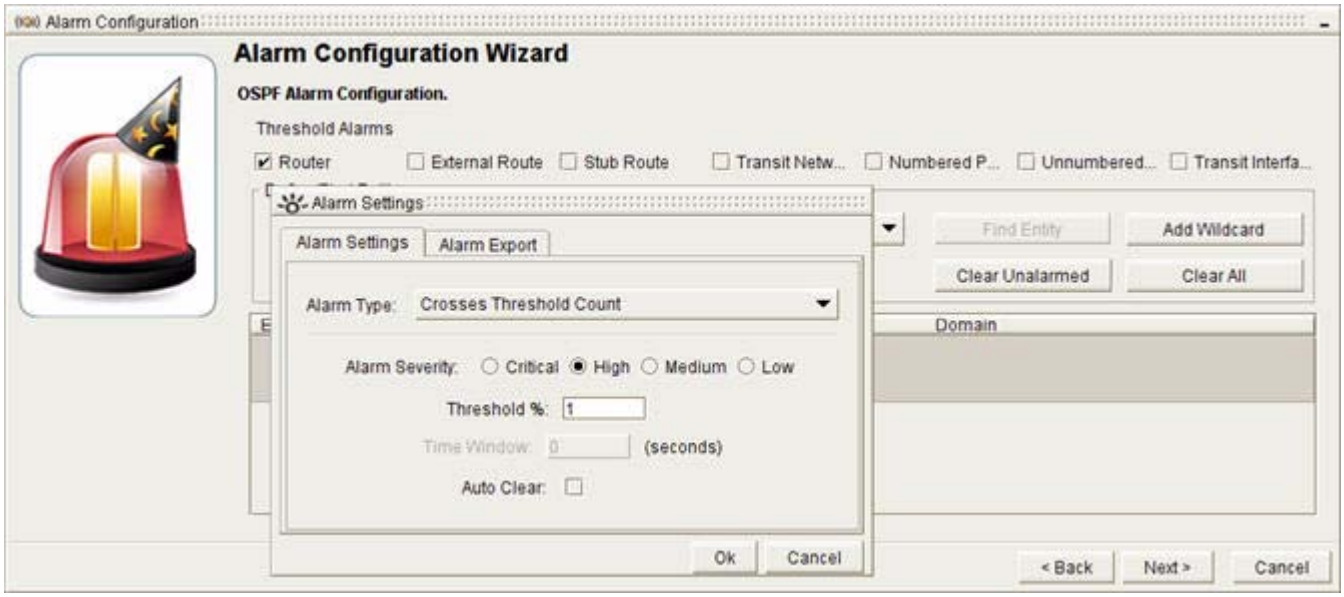


To set the alarm type, double-click any of the following buttons (see Figure 8-30):

- **Entity Count—**This alarm is triggered when the number of entities deviates from the average value by at least the defined percentage.
- **Event Rate—**This alarm is triggered when the rate of events exceeds the average value by more than the defined percentage.

Provide Alarm Settings

Figure 8-31 Alarm Settings Screen in Threshold Alarms



To provide alarm settings (see Figure 8-31):

Step 1 Provide alarm settings:

- **For both Threshold Entity Count Alarm and Threshold Event Rate Alarm**

a. From the Alarm Type drop-down menu, Crosses Threshold Rate appears by default.

b. Select one of the following options from the Alarm Severity radio buttons:

  - **Critical**
  - **High**
  - **Medium**
  - **Low**

  See Severity Values of Alarms, page 8-61.

c. Enter a percentage in the Threshold Percentage field.

  By default, the Threshold Percentage value is set to 1 to indicate 1 percent.

d. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the Threshold Entity Count Alarm (if selected), displays two buildings, each with a red star, indicating that the alarm has been configured.

The DBL CLK button under the Event Rate Alarm (if selected), displays two triangles, each with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

Configure an Error Alarm

To configure an error alarm:

Step 1 Use the procedure to Start the OSPF Alarm Configuration Wizard, page 8-19.

Step 2 Select the **Errors** radio button and click **Next**.

The OSPF Alarm Configuration, Error Alarms wizard screen appears (see Figure 8-32).

Interface Conflict Errors is selected, by default.

Figure 8-32 Error Alarms Screen in OSPF Alarm Configuration Wizard

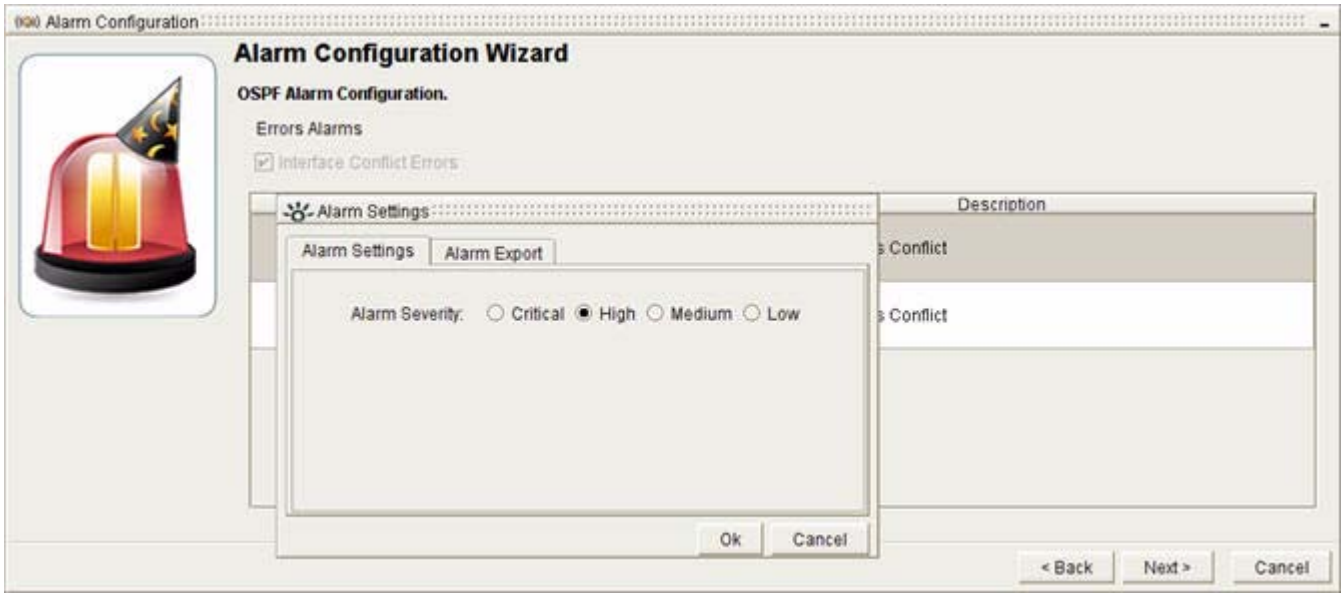
Set the Alarm Type

To set the alarm type:

Step 1 Double-click any of the following DBL CLK buttons:

- **Detection**
- **Resolution**

Figure 8-33 Alarm Settings Screen in Error Alarms



Step 2 Provide alarm settings (see Figure 8-33):

a. Select one of the following options for the Alarm Severity radio buttons:

- **Critical**
- **High**
- **Medium**
- **Low**

See Severity Values of Alarms, page 8-61.

Step 3 Click **OK**.

The DBL CLK button under the Detection Alarm or Resolution Alarm (if selected), displays a check mark with a red star, indicating that the alarm has been configured.

Step 4 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 5 Click **Finish**.

Alarms are displayed in the **Alarm** section of the Alarm Monitor window.

Configure a Service Alarm

To configure a service alarm:

Step 1 Select **Start > Alarm Monitor**.

The Alarm Monitor window appears in the Path Analyzer Management Console. By default, the Monitor tab is selected. If not, click the **Monitor** tab.

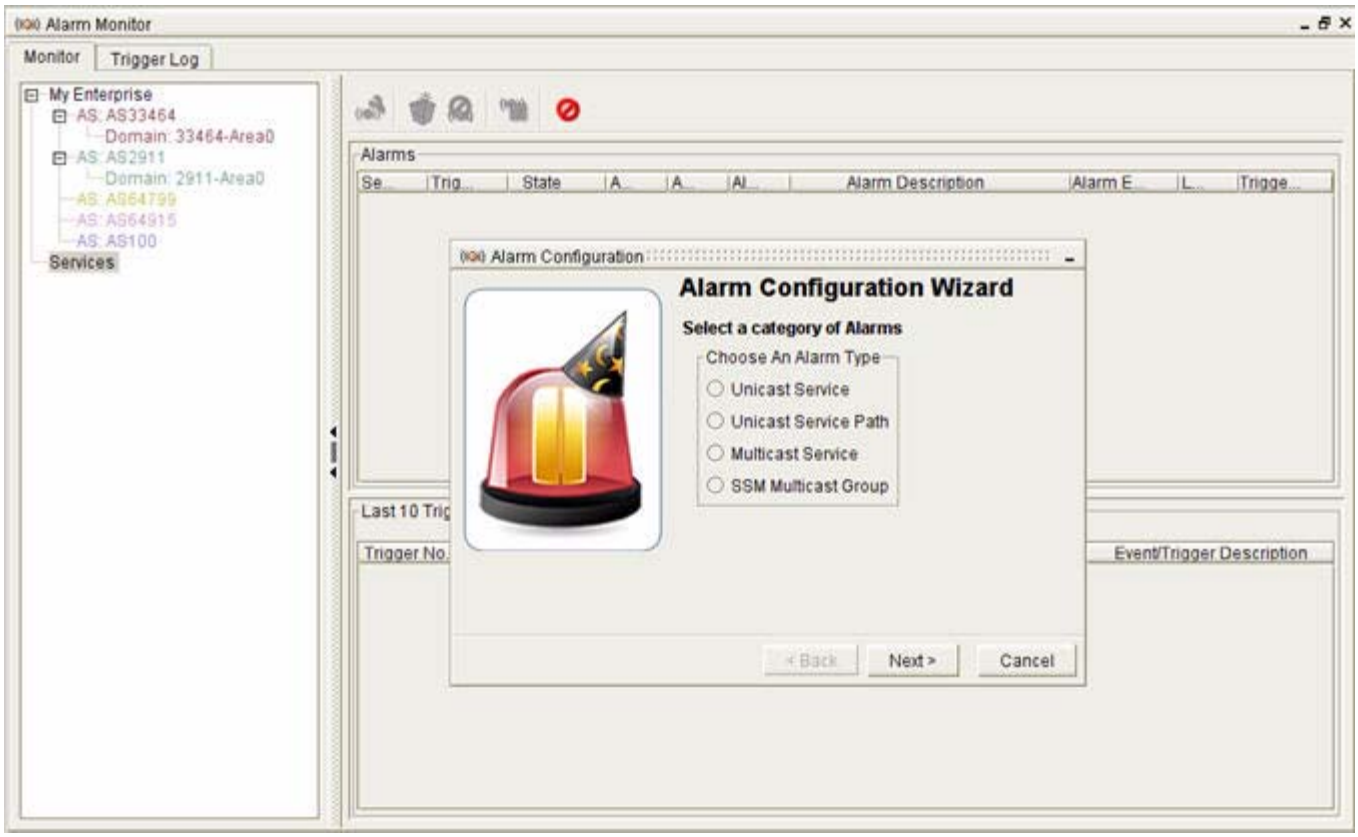
Step 2 Select **Services** from the Enterprise hierarchy on the left side.

Start the Service Alarm Configuration Wizard

To start the service alarm configuration wizard, click **Configure Alarms** in the Alarm Monitor toolbar.

The Alarm Configuration wizard appears, featuring options for Service alarms. (see Figure 8-34)

Figure 8-34 Service Alarms Configuration Wizard



Select a Category of Service Alarms

To select a category of service alarms:

Step 1 Select the radio button corresponding to the type of alarm you want to create:

- **Unicast Service**—Set alarms on changes to Path Analyzer unicast services. See Configure a Unicast Service Alarm, page 8-44.
- **Unicast Service Path—**Set alarms on changes to Path Analyzer unicast service paths. See Configure a Unicast Service Path Alarm, page 8-46.
- **Multicast Service**—Set alarms on changes to Path Analyzer multicast services. See Configure a Multicast Service Alarm, page 8-49.
- **SSM Multicast Group—**Set alarms on changes to Path Analyzer SSM Multicast Groups. See Configure a SSM Multicast Group Alarm, page 8-52.

Step 2 Click **Next**.

A configuration wizard will appear for the type of service alarm you have selected.

For more information about unicast and multicast services and service paths, see Monitoring Unicast and Multicast Services, page 3-1.

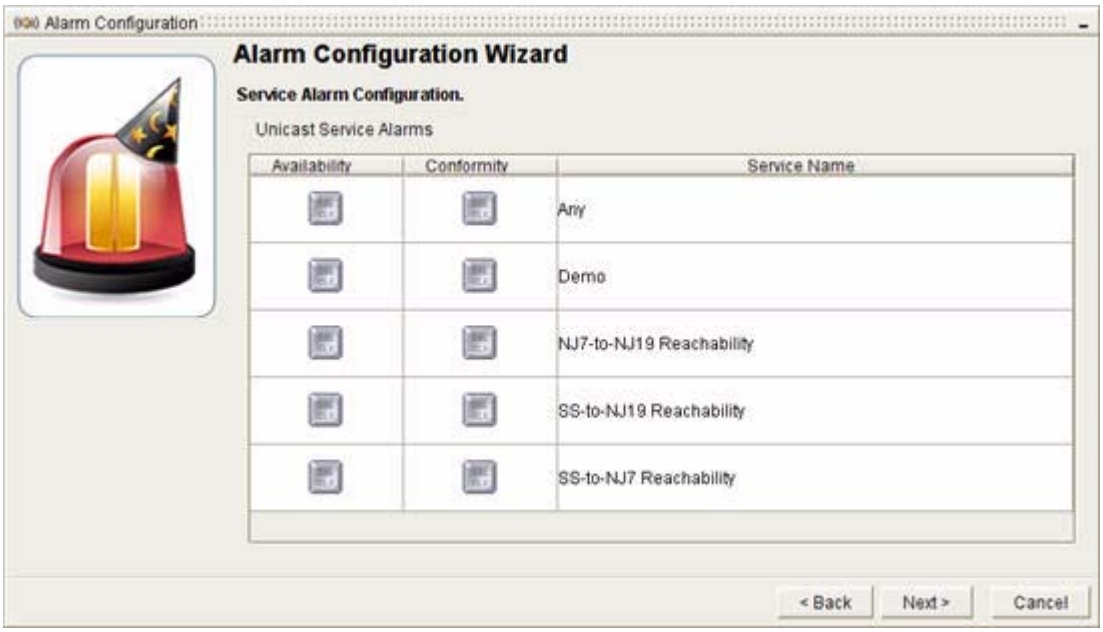
Configure a Unicast Service Alarm

Step 1 Use the procedure to Start the Service Alarm Configuration Wizard, page 8-42.

Step 2 Select the **Unicast Service** radio button and click **Next**.

The Service Alarm Configuration Wizard screen appears (see Figure 8-35).

Figure 8-35 Unicast Service Alarms in Service Alarm Configuration Wizard



Set the Alarm Type

To set the alarm type, double-click any of the following buttons for the service or services you wish to configure:

- **Availability**—Notifies of changes in the availability of a service or of intermittent availability (flap). Sets a Service Availability or Flap Alarm.
- **Conformity—**Notifies of changes in the conformity of a service to its configured baseline. A service is considered to conform to its baseline when all of its service paths conform to their configured baselines. Sets a Service Conformity Change alarm.

Provide Alarm Settings

Figure 8-36 Alarm Settings Screen in Unicast Service Alarms

To provide alarm settings (see Figure 8-36):

Step 1 Provide alarm settings:

- **For an Availability Alarm:**

a. Select the alarm trigger. In the Alarm Type drop-down menu, select one of the following options:

  - **Becomes Available**
  - **Becomes Unavailable**
  - **Flap**

- **For an Conformity Alarm:**

a. Select the alarm trigger. In the Alarm Type drop-down menu, select one of the following options:

  - **Becomes Conformant**—Conforms to its baseline.
  - **Becomes Deviant—**Deviates from its baseline.
  - **Flap—**Intermittently conforms to or deviates from its baseline.

- **For All Unicast Service Alarms:**

a. Select one of the following options for the Alarm Severity radio buttons:

  - **Critical**—Assigns highest importance to the alarm.
  - **High—**Assigns high importance to the alarm.
  - **Medium—**Assigns medium importance to the alarm.
  - **Low—**Assigns least importance to the alarm.

    See Severity Values of Alarms, page 8-61.

b. Enter the number of times for changes to occur in the time window before triggering the alarm in the Count field.

   By default, the Count value is set to 1 to indicate one change within the time window.

c. Enter the number of seconds for the count in the Time Window.

   By default, the Time Window value is set to 1 to indicate a one-second time window. For information about setting the Count and Time Window see, Time Window for Alarm Triggering, page 8-63.

d. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the Availability Alarm or Conformity Alarm (if selected), displays a triangle with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

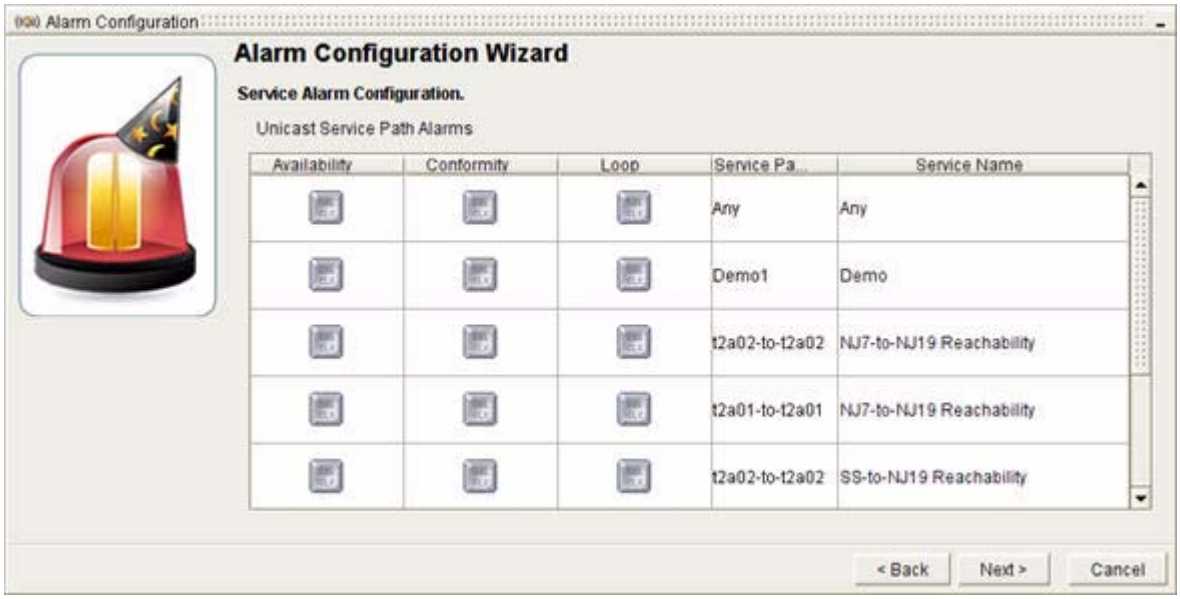
Configure a Unicast Service Path Alarm

Step 1 Use the procedure to Start the Service Alarm Configuration Wizard, page 8-42.

Step 2 Select the **Unicast Service Path** radio button and click **Next**.

The Unicast Service Alarm Configuration, Service Path Alarms screen appears (see Figure 8-37).

Figure 8-37 Unicast Service Path Alarms in Service Alarm Configuration Wizard



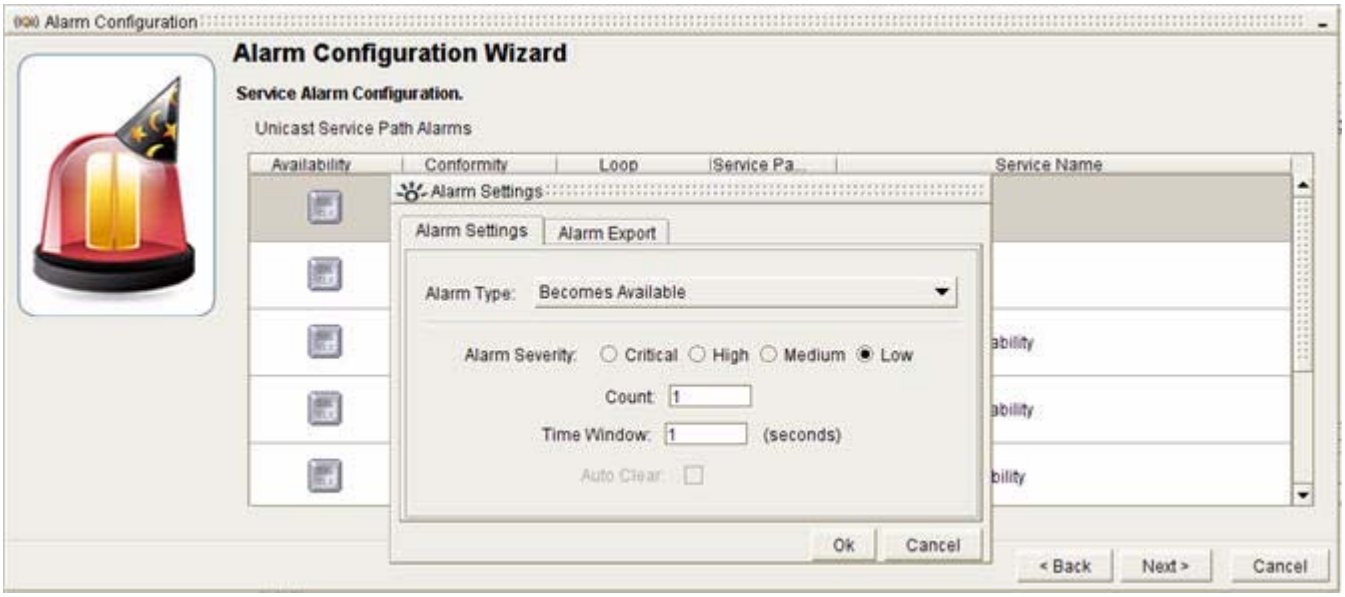
Set the Alarm Type

To set the alarm type, double-click any of the following buttons for the service path or service paths you wish to configure:

- **Availability**—Notifies of changes in the availability of a service path or of intermittent availability indicating flap. Sets a Service Path Availability or Flap Alarm.
- **Conformity—**Notifies of changes in the conformity of a service path to its configured baseline. A service path is considered conformant when it conforms to its configured baseline. Sets a Service Path Conformity Change alarm.
- **Loop**—Notifies if there is a detection of a loop in the service path. Sets a Service Path Loop Alarm.

Provide Alarm Settings

Figure 8-38 Alarm Settings Screen in Unicast Service Path Alarms



To provide alarm settings (see Figure 8-38):

Step 1 Provide alarm settings:

- **For an Availability Alarm**

a. Select the degree of availability to cause the alarm to trigger. In the Alarm Type drop-down menu, select one of the following options:

  - **Becomes Available**
  - **Becomes Unavailable**
  - **Flap**

- **For a Conformity Alarm**

a. Select the degree of availability to cause the alarm to trigger. In the Alarm Type drop-down menu, select one of the following options:

  - **Becomes Conformant**
  - **Becomes Deviant**
  - **Flap**

- **For All Service Path Alarms**

a. Select one of the following options for the Alarm Severity radio buttons:

  - **Critical**
  - **High**
  - **Medium**
  - **Low**

  See Severity Values of Alarms, page 8-61.

b. Enter the number of times for changes to occur in the time window before triggering the alarm in the Count field

   By default, the Count value is set to 1 to indicate one change within the time window.

c. Enter the number of seconds for the count in the Time Window.

   By default, the Time Window value is set to 1 to indicate a one-second time window. For information about setting the Count and Time Window, see Time Window for Alarm Triggering, page 8-63.

d. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Note For service path alarms, you can set the auto clear feature for Availability and Conformity alarms only.

Step 2 Click **OK**.

The DBL CLK button under the Availability Alarm and Conformity Alarm (if selected), displays a triangle with a red star, indicating that the alarm has been configured.

The DBL CLK buttons under the Loop Alarm (if selected), displays two triangles, each with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

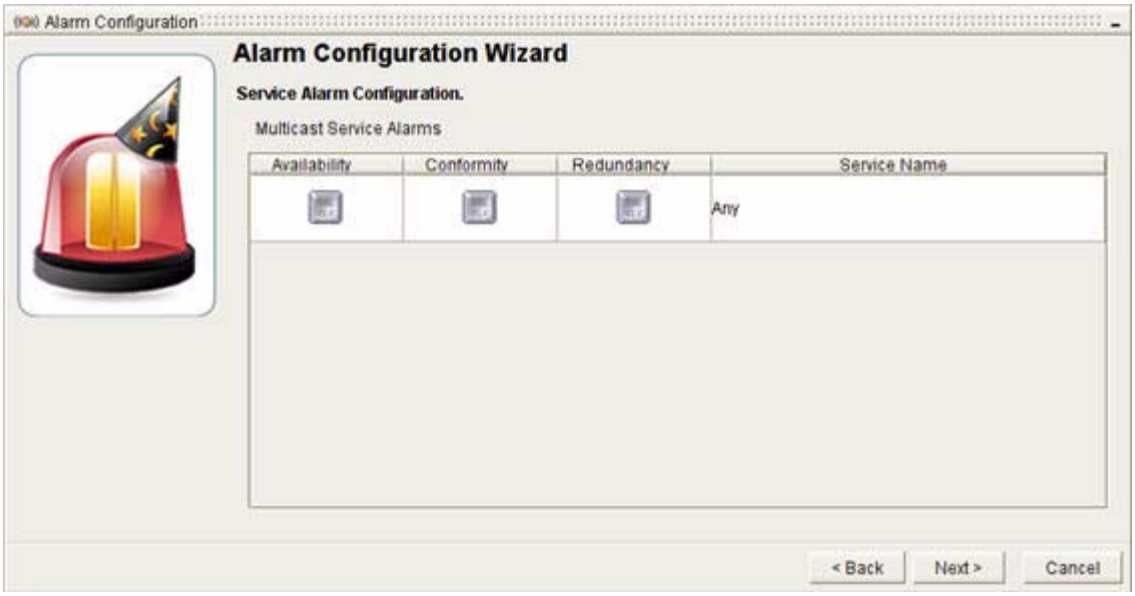
Configure a Multicast Service Alarm

Step 1 Use the procedure to Start the Service Alarm Configuration Wizard, page 8-42.

Step 2 Select the **Multicast Service** radio button and click **Next**.

The Multicast Service Alarm Configuration, Service Alarms screen appears (see Figure 8-39).

Figure 8-39 Multicast Service Alarms Screen in Alarm Configuration Wizard



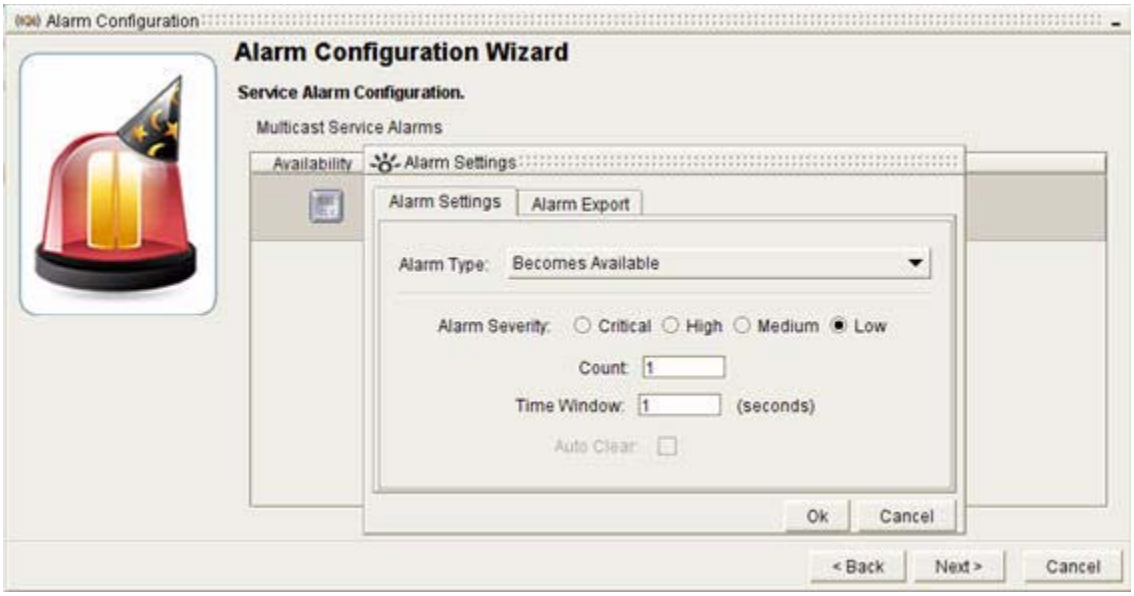
Set the Alarm Type

To set the alarm type, double-click any of the following buttons next to the service or services you wish to configure:

- **Availability**—Notifies of changes in the availability of a service or of intermittent availability (flap). Sets a Service Availability or Flap Alarm.
- **Conformity—**Notifies of changes in the conformity of a service to its configured baseline. A service is considered to conform to its baseline when all of its service paths conform to their configured baselines. Sets a Service Conformity Change alarm.
- **Redundancy—**Notifies of changes in the redundancy of a service or of intermittent availability (flap). A service is considered redundant when there is more than one way to reach the destination. Sets a Multicast Service Redundancy Change alarm.

Provide Alarm Settings

Figure 8-40 Alarm Settings Screen in Multicast Service Alarms



To provide alarm settings (see Figure 8-40):

Step 1 Provide alarm settings:

- **For an Availability Alarm**

a. Select the degree of availability to cause the alarm to trigger. In the Alarm Type drop-down menu, select one of the following options:

  - **Becomes Available**
  - **Becomes Unavailable**
  - **Flap**

- **For a Conformity Alarm**

a. Select the condition that will cause the alarm to trigger. In the Alarm Type drop-down menu, select one of the following options:

  - **Becomes Conformant**
  - **Becomes Deviant**
  - **Flap**

- **For a Redundancy Alarm**

a. Select the condition that will cause the alarm to trigger. In the Alarm Type drop-down menu, select one of the following options:

  - **Becomes Redundant**
  - **Becomes Non-Redundant**
  - **Flap**

- **For all Multicast Service Alarms**

a. Select one of the following options for the Alarm Severity radio buttons:
   - **Critical**
   - **High**
   - **Medium**
   - **Low**

   See Severity Values of Alarms, page 8-61.

b. Enter the number of times for changes to occur in the time window before triggering the alarm In the Count field.

   By default, the Count value is set to 1 to indicate one change within the time window.

c. Enter the number of seconds for the count in the Time Window.

   By default, the Time Window value is set to 1 to indicate a one-second time window. For information about setting the Count and Time Window, see Time Window for Alarm Triggering, page 8-63.

d. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the Availability Alarm, Conformity Alarm, and Redundancy Alarm (if selected), displays a triangle with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

Configure a SSM Multicast Group Alarm

Step 1 Use the procedure to Start the Service Alarm Configuration Wizard, page 8-42.

Step 2 Select the **SSM Multicast Group** radio button and click **Next**.

The Multicast Service Alarm Configuration, SSM Multicast Group Alarms screen appears (see Figure 8-41).

Figure 8-41 SSM Multicast Group Alarms Screen in Service Alarm Configuration Wizard

Set the Alarm Type

To set the alarm type, double-click any of the following buttons next to the SSM multicast group or groups you wish to configure:

- **Availability**—Notifies of changes in the availability of a SSM multicast group or of intermittent availability (flap). Sets an SSM Multicast Group Availability or Flap Alarm.
- **Conformity—**Notifies of changes in the conformity of a SSM multicast group to its configured baseline. An SSM multicast group is considered to conform to its baseline when all of its service paths conform to their configured baselines. Sets an SSM Multicast Group Conformity or Flap Alarm.

Provide Alarm Settings

To provide alarm settings:

Step 1 Provide alarm settings:

- **For an Availability Alarm**

a. Select the degree of availability to cause the alarm to trigger. In the Alarm Type drop-down menu, select one of the following options:

  – **Becomes Available**

  – **Becomes Unavailable**

  – **Flap**

- **For a Conformity Alarm**

a. Select the degree of availability to cause the alarm to trigger. In the Alarm Type drop-down menu, select one of the following options:

  - **Becomes Conformant**
  - **Becomes Deviant**
  - **Flap**

- **For All SSM Multicast Group Alarms**

a. Select one of the following options for the Alarm Severity radio buttons:
  - **Critical**
  - **High**
  - **Medium**
  - **Low**

  See Severity Values of Alarms, page 8-61.

b. Enter the number of times for changes to occur in the time window before triggering the alarm in the Count field.

   By default, the Count value is set to 1 to indicate one change within the time window.

c. Enter the Time Window, the number of seconds for the count.

   By default, the Time Window value is set to 1 to indicate a one-second time window. For information about setting the Count and Time Window, see Time Window for Alarm Triggering, page 8-63.

d. Select the **Auto Clear** check box to have the alarm cleared automatically after the trigger condition has been resolved.

Step 2 Click **OK**.

The DBL CLK button under the Availability Alarm and Conformity Alarm (if selected), displays a triangle with a red star, indicating that the alarm has been configured.

Step 3 Click **Next**.

You will receive a message: “Sending Alarm Request...” followed by, “The alarm request was successfully received by the Path Analyzer server.”

Step 4 Click **Finish**.

Alarms are displayed in the Alarm section of the Alarm Monitor window.

Set the Alarm Export Options

When network changes trigger an alarm, you receive a notification and a set of generated triggers with descriptions of the changes that occurred. All triggers are displayed in the Trigger Log.

After setting alarms and analyzing their triggers, you can export the triggers to a syslog host or a Simple Network Management Protocol (SNMP) agent to view them in your network management system.

For more information regarding how to set up export destinations, please see Chapter 8, Exporting Alarm Triggers in the *Cisco Service Path Analyzer System Administration Guide*. In Alarm Monitor, however, you can select the export destinations that were defined in the Alarm Export Administration module.

Note The Alarm Export destination selections that you make in Alarm Monitor override the selections made in the Alarm Export Administration module.

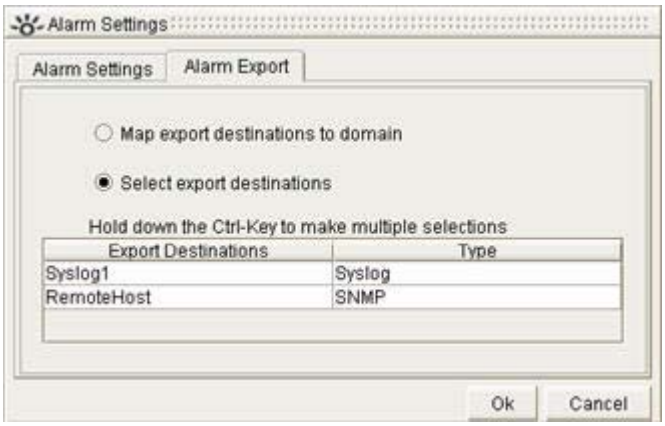
Set Export Options

To set alarm export options:

Step 1 Double-click any of the **DBL CLK** buttons. This applies to BGP, OSPF, and Service alarms.

Step 2 Click the **Alarm Export** tab (see Figure 8-42).

Figure 8-42 Alarm Export Screen in Alarm Wizard



Step 3 Select one of the following:

a. **Map export destination to domain**, or

a. **Select export destinations** and choose one or more export destinations from the table. (Hold down the Ctrl key to select multiple destinations.)

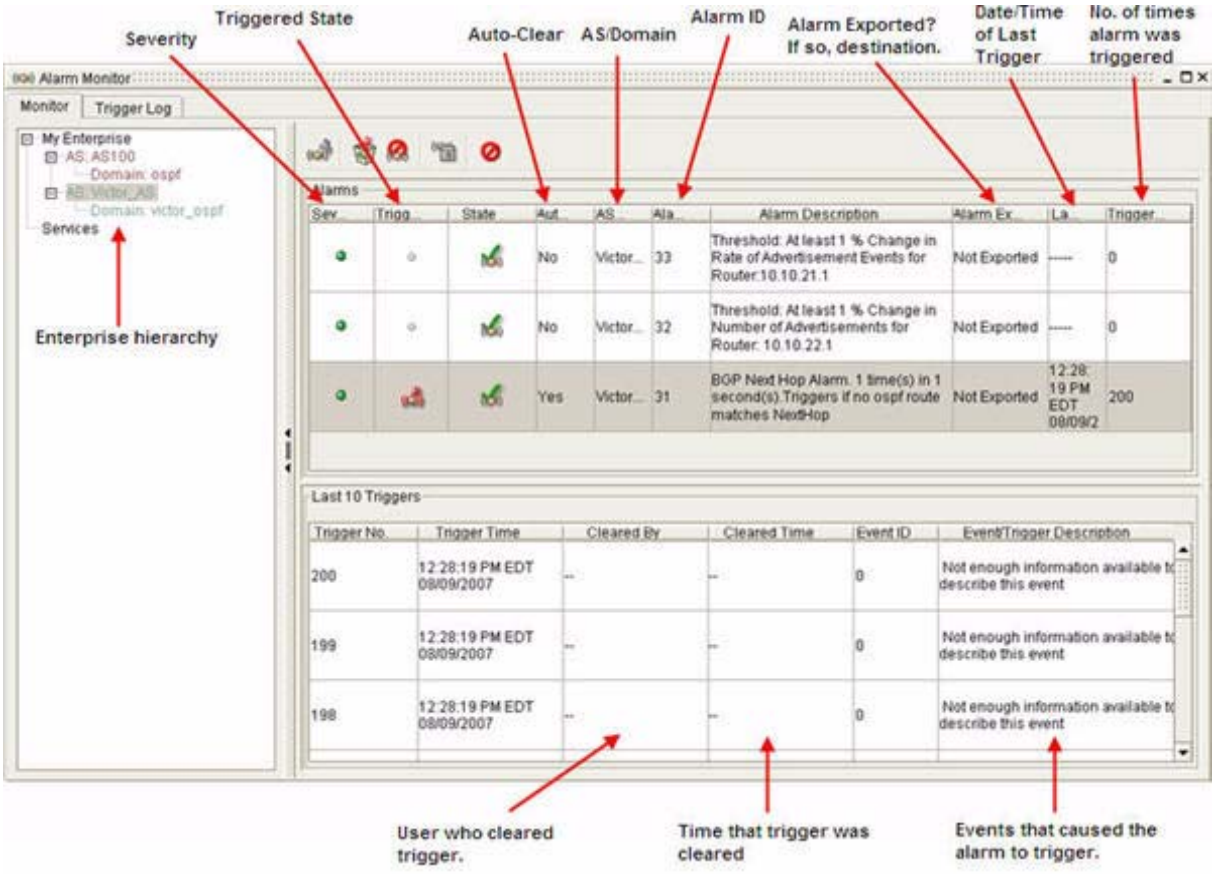
Step 4 Click **OK**.

To populate this screen with export destinations, select **Start** > **Administration** > **Alarm Export**.

Viewing and Managing Alarms

Setting an alarm on a network entity, such as a service, service path, router, router interface, or network enables the alarm. When changes occur on your network that activate or *trigger* the alarm, Alarm Monitor lists the information shown in Figure 8-43 with the alarm:

Figure 8-43 Set and Activated Alarms in Alarm Monitor



- **Severity—**Displays the severity of the alarm. See Severity Values of Alarms, page 8-61.
- **Trigger State—**Alerts you to view the alarm triggers, the changes to routing patterns that activate alarms. See Clear All Alarm Triggers, page 8-63.
- **State—**Displays whether the alarm is enabled or disabled.
- **Auto-Clear—**Allows you to view if the auto clear functionality is selected. If **Yes** appears in the column, then the alarm will clear automatically after its trigger condition has been detected and resolved. If **No** appears in the column, then you will have to clear the alarm manually.
- **AS/Domain—AS** shows the locations of routes and advertisements for BGP alarms; **Domain** shows the location of routers, interfaces, Transit networks, advertisements, and routes for OSPF alarms.
- **Alarm ID—**Shows the alarm ID.
- **Alarm Description—**Describes the alarm.
- **Alarm Export—**Shows the export destination of the alarms.
- **Last Trigger Time—**Displays the date and time the last alarm was triggered.
- **Trigger Count—**Shows the number of times the alarm was triggered.

For details about the fields, icons, and values that are displayed for alarms in Alarm Monitor, see Alarm Indicators in Alarm Monitor, page 8-61 and Alarm Monitor, page 8-72. Selecting a triggered alarm lists the most recent alarm triggers under the selected alarm. You can define the number of alarm triggers to display by resizing the Trigger Log. See Change the Number of Triggers Displayed, page 8-70 for more information.

Note The list of most recent triggers displayed in Alarm Monitor cannot be resized. Only the trigger log can be resized.

Icons indicate when an alarm is triggered and requires investigation and acknowledgement. See Indicators of Triggered Alarms, page 8-61 for information.

After investigating alarm triggers and fixing potential problems, you can clear the alarm to show that you have fixed the issue. When all triggers of an alarm are cleared, the **Cleared Trigger** icon appears. See Clear All Alarm Triggers, page 8-63 for information.

Differences Between SNMP Polls and Path Analyzer Alarms

Network management applications generally poll network devices using Simple Network Management Protocol (SNMP) to obtain status information. SNMP polling delivers a set of values for specific properties or attributes of your network devices to your NMS. When the values returned indicate that an alarm has occurred, your network management system sends you a notification.

Although SNMP polling is effective for identifying a large but finite set of physical issues with network devices, SNMP cannot identify routing issues, such as a failed link or a misconfigured router interface that transmits a packet to the wrong destination.

Additionally, because changes to routes and service paths occur faster than polling intervals, polling techniques incur a high level of latency in identifying IP-level issues.

The adjacency between an OSPF-enabled router and an IP Listener lets Path Analyzer capture all events generated from the Link State Advertisements (LSAs) of routers in an area. Each LSA generates at least one event that describes a change to your network.

Multi-area support enables the Path Analyzer Server to collect and persist in a database the detailed and dynamic set of events that occur throughout your network, without latency or gaps in the data. Issuing an alarm on an entity, such as a router or a Transit network in Alarm Monitor, ensures that you can obtain the full list of router events with detailed information to direct you to the root cause of an alarm.

Supported Alarms

Alarms are categorized by type: BGP, OSPF, and Services. The following section summarizes the alarms supported by Alarm Monitor.

BGP Alarms

The following BGP alarms can be configured:

- Advertisement alarms, page 8-58
- Threshold per Router alarms, page 8-58
- Route alarms, page 8-58
- Threshold per AS alarms, page 8-58
- BGP Next Hop alarms, page 8-58

Advertisement alarms

Set BGP advertisement alarms for notifications of changes to a BGP advertisement, such as changes to the advertised prefix. In setting the alarm, you are prompted to supply the autonomous system of the advertisement, the advertised prefix, and the router ID or DNS name of the advertising router.

For details about all BGP advertisement alarms, see BGP Route Advertisement Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Threshold per Router alarms

Set BGP threshold per router alarms for notification of when the system perceived (or baseline) behavior of BGP routes or BGP route updates for a router deviates by a certain percentage defined by the user.

For details about all BGP threshold per router alarms, see BGP Threshold per Router Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Route alarms

Set BGP route alarms for notifications of changes that affect a route, such as changes in the reachability of the route. In setting the alarm, you are prompted to supply autonomous system and prefix of the route.

For details about all BGP route alarms, see BGP Route alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Threshold per AS alarms

Set BGP threshold per AS alarms for notification of when the system perceived (or baseline) behavior of BGP routes or route updates in an autonomous system deviates by a certain percentage defined by the user.

For details about all BGP threshold per AS alarms, see BGP Threshold per AS Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

BGP Next Hop alarms

Set alarm to trigger when the next hop is no longer available using an OSPF route. You can also set the alarm to trigger when only the default OSPF route is matching the BGP next hop.

For details see BGP Next Hop Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

OSPF Alarms

The following OSPF alarms can be configured:

- Interface alarms, page 8-59
- Router alarms, page 8-59
- Transit network alarms, page 8-59
- Advertisement alarms, page 8-59
- Route alarms, page 8-59
- Threshold alarms, page 8-59
- Error detection and resolution alarms, page 8-60

Interface alarms

Set interface alarms on Numbered Point-to-Point (NP2P), Unnumbered Point-to-Point (UP2P), and Transit interfaces for notifications of changes to the availability or cost of the interface. In setting the alarm, you are prompted to supply the type of interface, interface identifier, router ID, area, OSPF area, and neighboring router.

- For details about Point-to-Point interface alarms, see Point-to-Point Interface Alarms in the *Cisco Service Path Analyzer Alarm Reference*. P2P interface alarms are part of interface alarms category.
- For details about Transit interface alarms, see Transit Interface Alarms in the *Cisco Service Path Analyzer Alarm Reference*. Transit interface alarms are part of interface alarms category.

Router alarms

Set router alarms for notifications of changes that affect a router, such as changes to the availability of a router or the number of areas in which it is configured. In setting the alarm, you are prompted to supply the router name and domain in which the router resides.

For details about all router alarms, see Router Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Transit network alarms

Set Transit network alarms for notifications of the changes that affect a selected Transit network, such as changes to the availability of a Transit network or the Designated Router (DR) assigned to the network. In setting the alarm, you are prompted to supply the autonomous system (domain) and area in which the Transit network is advertised, and the network prefix.

For details about Transit network alarms, see Transit Network Alarms in t*he Cisco Service Path Analyzer Alarm Reference*.

Advertisement alarms

Set advertisement alarms for notifications of the changes that affect a selected route advertisement, such as changes to the availability or cost of an advertised route, change to the cost metric of an Autonomous System Boundary Router (ASBR) interface, or a change in the type of External or Stub route.

- For details about Stub route alarms, see Stub Route Advertisement Alarms in the *Cisco Service Path Analyzer Alarm Reference*. Stub route advertisement alarms are part of advertisement alarms category.
- For details about External route alarms, see External Route Alarms in the *Cisco Service Path Analyzer Alarm Reference*. External route advertisement alarms are part of advertisement alarms category.

Route alarms

Set route alarms for notifications of changes to a route, including changes to the availability or redundancy of a core route, which has a destination within the local autonomous system, or an external route, which has a destination in an external autonomous system.

Threshold alarms

Set threshold alarms for notification when the system's perceived number of entities per domain or event rates deviate from the norm by a certain percentage defined by the user.

For details about threshold alarms, see OSPF Threshold Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Error detection and resolution alarms

Set error detection and resolution alarms for notifications when IP address conflicts occur or are resolved. Error detection and resolution alarms are a type of wildcard alarm.

For details about error detection and resolution alarms, see Error Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Service Alarms

The following service and service path alarms can be configured:

- Unicast Service alarms, page 8-60
- Multicast Service alarms, page 8-60
- Unicast Service Path alarms, page 8-60
- SSM Multicast Group alarms, page 8-60

Unicast Service alarms

Set alarms on unicast services for notifications of changes in the availability or conformity of a service.

For details about all service alarms, see Service and Service Path Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Multicast Service alarms

Set alarms on multicast services for notifications of changes in the availability, conformity, or redundancy of a service.

For details about all service alarms, see Service and Service Path Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Unicast Service Path alarms

Set service path alarms for notifications of changes that affect a service path, such as changes in availability, conformity, or loop in the path of a service path.

For details about all service alarms, see Service and Service Path Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

SSM Multicast Group alarms

Set service path alarms for notifications of changes that affect an SSM multicast group, such as changes in the availability or conformity of a specific service path.

For details about all service alarms, see Service and Service Path Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Wildcard alarms: Alarms on All Changes to All Selected Entities

Set wildcard alarms for notifications of all changes that affect any OSPF, BGP, or Service element. See Wildcard Alarms in the *Cisco Service Path Analyzer Alarm Reference*.

Severity Values of Alarms

When you set an alarm, you are required to specify a severity for the alarm. Severity values include:

- **Critical**—Select this option to show that the alarm is critical to your business and requires immediate attention, whether you are notified from Alarm Monitor, syslog, or your NMS. Displays as a red icon.
- **High**—Select this option to show that the alarm is important to investigate, but not as urgent as a Critical alarm. Displays as an orange icon.
- **Medium**—Select this option to show that the alarm has significant effects on a less critical service, service path, router, interface, route, or advertisement. Displays as a yellow icon.
- **Low**—Select this option to show that the alarm has a minimal impact on a less important service path or entity on the network. Displays as a green icon.

The icons in Figure 8-44 identify the severity of an alarm in Alarm Monitor:

Figure 8-44 Alarm Severities

Indicators of Triggered Alarms

The Path Analyzer Management Console and Alarm Monitor provide indicators to let you know when events set off an alarm.

Alarm Indicators in Alarm Monitor

Table 8-1 describes icons that indicate the state of alarms in Alarm Monitor. The table gives the meaning of the various icons when they appear in the Alarm Monitor against a particular alarm (Alarm Description column) and when they appear in the Path Analyzer taskbar (System Description column).

Table 8-1 Icons that Indicate the State of Alarms

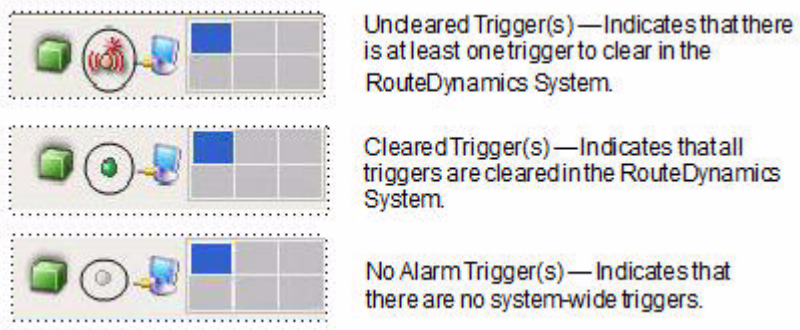
Icon	Alarm Description	System Description
Uncleared Trigger(s) 	There is at least one trigger to clear for an alarm.	There is at least one trigger to clear in the Path Analyzer system.
Cleared Trigger(s) 	All triggers are cleared per alarm.	All triggers are cleared in the Path Analyzer system.
No Trigger(s) 	No alarm triggers.	No systemwide alarm triggers.

Alarm Indicators in the Path Analyzer Taskbar

In the taskbar of the Path Analyzer Management Console, the same alarm states appear. See Alarm Indicators in Alarm Monitor, page 8-61 for more information.

After you investigate all uncleared triggers, the icon changes from **Uncleared Trigger** to **Cleared Trigger**. If there are no systemwide alarm triggers, then the **No Alarm Trigger** icon appears (see Figure 8-45).

Figure 8-45 Alarm Indicators



In the taskbar of the Path Analyzer Management Console, you can double-click on the Uncleared Trigger icon to launch the Alarm Monitor.

Figure 8-46 Location of Alarm State Icons in Alarm Monitor

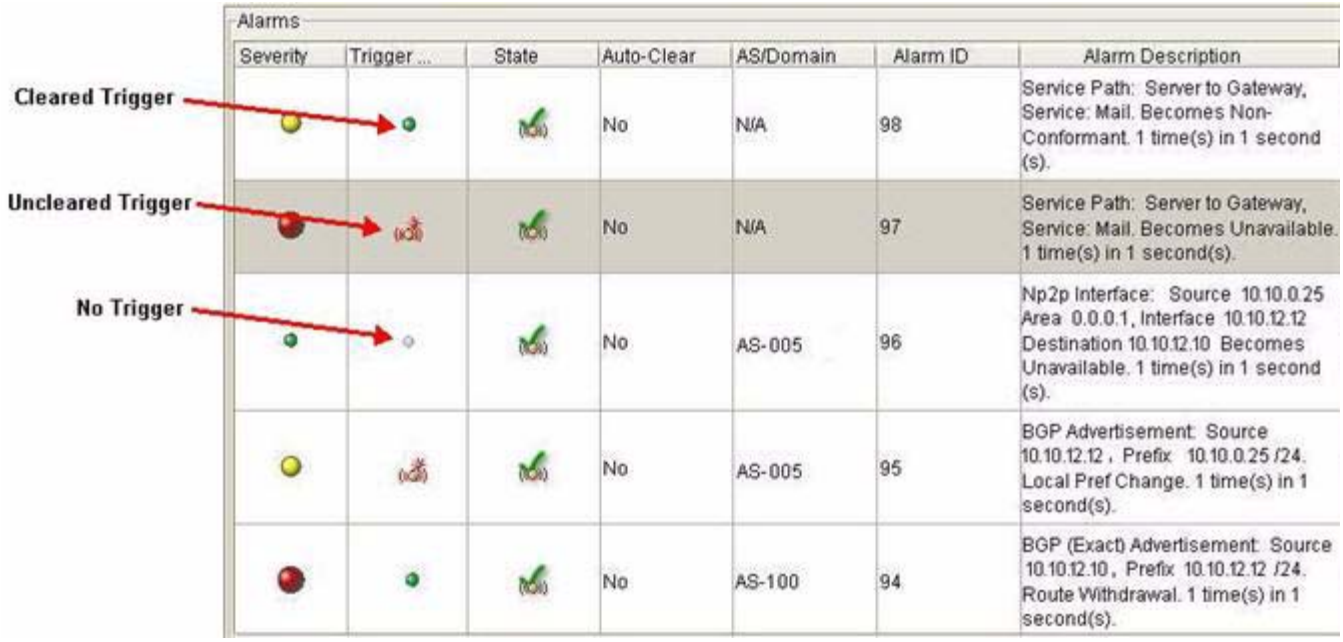


Figure 8-46 shows the different trigger state icons in Alarm Monitor.

Time Window for Alarm Triggering

In Alarm Monitor, you can set a finite or unlimited time window for alarm triggering. Alarms that are set with a finite time window trigger when the selected number of changes occurs within the time window. Between triggers, Path Analyzer refreshes the count and restarts the clock.

For example, you can set a Service Path Availability Flap alarm on a service to notify you if the service intermittently changes state from Unavailable to Available in the set time period.

Entering 5 in the Count field and 15 in the Time Window field causes Path Analyzer to track the first 5 changes in the 15-second interval, triggers the alarm, then resets the count to 0. It then tracks the next 5 changes in 15 seconds, and triggers the alarm again.

In this manner, Alarm Monitor provides you with a clear understanding of the events that occur on your network and their frequency.

Clear All Alarm Triggers

To clear all alarm triggers:

Step 1 Use the procedure to Start Alarm Monitor, page 8-3.

The alarm that appears with the **Uncleared Trigger** icon indicates that an alarm has been triggered.

Step 2 Select the alarm, right click on it, and select **Clear All Triggers**.

Step 3 The icon will change from the **Uncleared Trigger** icon to the **Cleared Trigger** icon.

To clear a single alarm trigger, see Clear A Trigger, page 8-67.

Globally Enable or Disable All Alarms

Once alarms have been configured, you can globally enable or disable them:

- Globally Disable All Alarms, page 8-64
- Globally Enable All Alarms, page 8-64

Globally Disable All Alarms

To globally disable all alarms:

Step 1 Use the procedure to Start Alarm Monitor, page 8-3.

Step 2 From the Alarm Monitor Toolbar, page 8-73, click the **Disable All Alarms** icon.

The State field of every alarm listed in Alarm Monitor is displayed with the **Alarm Disabled** icon, which indicates that all alarms are disabled. Disabled alarms cannot be triggered by events configured to set off the alarm.

The Alarm Monitor toolbar now shows the **Enable Alarm** icon, which indicates that all disabled alarms can be globally enabled if you decide to enable them. See also, Disable a Selected Alarm, page 8-65.

Note If you have not created any alarms, then all the Alarm Monitor toolbar buttons are grayed out except for the **Configure Alarms** button. For more information regarding the Alarm Monitor toolbar, see Alarm Monitor Toolbar, page 8-73.

Globally Enable All Alarms

To globally enable all alarms:

Step 1 Use the procedure to Start Alarm Monitor, page 8-3.

Step 2 From the Alarm Monitor Toolbar, page 8-73, click the **Enable All Alarms** icon.

The State field of each alarm listed in Alarm Monitor is displayed with the **Enable Alarm** icon, which indicates that all alarms are enabled. Enabled alarms can be triggered by events configured to set off the alarm.

The Alarm Monitor toolbar shows the **Alarm Disabled** icon, which indicates that all enabled alarms can be globally disabled if you decide to disable them. See also, Enable a Selected Alarm, page 8-65.

Disable a Selected Alarm

When you no longer require a specific alarm, you can disable the alarm. Once you have disabled the alarm, you can remove it, or you can keep it listed and enable it at a later date.

Step 1 Use the procedure to Start Alarm Monitor, page 8-3.

Step 2 Select the alarm you want to disable.

Step 3 Click **Disable Alarm** in the Alarm Monitor Toolbar, page 8-73.

or

Step 1 Right-click the alarm.

Step 2 Select **Disable Alarm**.

The alarm becomes disabled, indicated by the **Alarm Disabled** icon displayed in the State field.

When an alarm is disabled, it no longer sends notifications in response to events. See also, Globally Disable All Alarms, page 8-64.

Enable a Selected Alarm

When you want to re-enable an alarm that you previously disabled, you can enable the alarm. Once an alarm is enabled, notifications are displayed in Alarm Monitor every time events trigger the alarm.

In Alarm Monitor, the State field is displayed with the **Alarm Disabled** icon for any alarm that can be re-enabled.

Re-enable an Alarm

To re-enable an alarm:

Step 1 Use the procedure to Start Alarm Monitor, page 8-3.

Step 2 Select the alarm you want to re-enable.

Step 3 Click **Enable Alarm** in the Alarm Monitor Toolbar, page 8-73.

or

Step 1 Right-click the disabled alarm.

Step 2 Select **Enable Alarm**.

The State field of the alarm shows the **Alarm Enabled** icon, to indicate that the alarm is re-enabled. Notifications are displayed every time events trigger the alarm. See also, Disable a Selected Alarm, page 8-65.

Remove an Alarm

To remove an alarm:

Step 1 Use the procedure to Start Alarm Monitor, page 8-3.

Alarms you previously created are listed in the Alarm Monitor.

Step 2 Select the alarm you want to remove.

Step 3 From Alarm Monitor Toolbar**,** click **Remove Alarm.**

or

Right-click the alarm you want to remove and select **Remove Alarm**.

Start the Trigger Log

Selecting a triggered alarm in Alarm Monitor shows the top ten most recent events, or changes in your network, that triggered the alarm. You can also open the Alarm Trigger tab to view the chronological listing of alarm triggers.

For detailed information about using the Alarm Triggers window, see Working in the Trigger Log, page 8-68.

View the Trigger Log

To view the Trigger Log:

Step 1 Use the procedure to Start Alarm Monitor, page 8-3.

Step 2 Select an alarm from the Alarm Monitor table.

Step 3 Click the **Browse Alarm's Triggers in Trigger Log** icon in the Alarm Monitor Toolbar, page 8-73.

or

Step 1 Use the procedure to Start Alarm Monitor, page 8-3.

Step 2 Select an alarm from the Alarm Monitor table.

Step 3 Right-click and select **Browse Alarm's Triggers in Trigger Log**.

Note Using the **Browse Alarm's Triggers in Trigger Log** function enables you to view triggers per-alarm. If you want to view systemwide triggers, see Show Systemwide Triggers, page 8-70.

Clear A Trigger

To clear a trigger:

Step 1 Use the procedure to Start Alarm Monitor, page 8-3.

Step 2 Select the **Trigger Log** tab.

Step 3 From the Trigger Log, select a trigger.

Step 4 Right-click and select **Clear Trigger**.

Note When viewing previously cleared triggers in the Trigger Log, the name of the person who manually cleared the trigger(s) appears in the Cleared By column, and the time the trigger(s) was cleared appears in the Cleared Time column. If the trigger was automatically cleared by the Path Analyzer system, auto clear appears in the column.

If another user deletes an alarm while you are working in Alarm Monitor, you will be alerted by a pop-up box. The alarm and its triggers will be lost, and you will be taken to the Trigger Log with the System Wide Triggers View.

Working in the Trigger Log

In the Trigger Log, you can view the complete set of alarm triggers in chronological order.

Browse through the Trigger Log

Browsing through the Trigger Log, you can:

- Browse Backward, page 8-68
- Browse Forward, page 8-68

Browse Backward

Browsing backward through the list of alarm triggers interrupts the dynamic updating capabilities of Trigger Log, and allows you to view alarm triggers that occurred previously. See Trigger Log, page 8-96.

To browse backward in the Trigger Log:

Step 1 Use the procedure to View the Trigger Log, page 8-66.

Step 2 Click the **Step Back** icon in the Trigger Log Toolbar, page 8-96.

The previous set of alarm triggers are displayed.

Step 3 Continue to click **Step Back** to move backward through the list of alarm triggers at the rate of 20 alarm triggers per click.

Step 4 Click **Show Current** to move to the most recent 20 triggers and restore dynamic updating.

For information about changing the number of alarm triggers to display per click, see Change the Number of Triggers Displayed, page 8-70.

See Trigger Log, page 8-96.

Browse Forward

Browsing forward through the list of alarm triggers interrupts the dynamic updating capabilities of the Trigger Log, and allows you to browse through the static list of alarm triggers.

To browse forward in the Trigger Log:

Step 1 Use the procedure to View the Trigger Log, page 8-66.

Step 2 Click the **Step Forward** icon in the Trigger Log Toolbar, page 8-96.

The next set of alarm triggers appears.

Step 3 Continue to click **Step Forward** to move forward through the list of alarm triggers at the rate of 20 alarm triggers per click.

For information about changing the number of alarm triggers to display per click, see Change the Number of Triggers Displayed, page 8-70. See Trigger Log Toolbar, page 8-96.

Step 4 Click **Show Current** to restore dynamic updating or streaming.

See Refresh the List, page 8-69.

Refresh the List of Alarm Triggers

The Trigger Log dynamically updates the list of alarm triggers to ensure that you always have a current view of alarm triggers.

Browsing backward or forward through the list of alarm triggers interrupts dynamic updating, allowing you to browse backward or forward through the static list of alarm triggers.

Clicking **Show Current** restores dynamic updating in Current Mode, and updates the list of alarm triggers with the most recent list of alarm triggers.

Refresh the List

To refresh the Trigger Log list:

Step 1 Use the procedure to View the Trigger Log, page 8-66.

Step 2 Click the **Show Current** icon in the Trigger Log Toolbar, page 8-96.

Browse Mode is interrupted. The Trigger Log returns to the state of dynamically updating events as they occur. See Trigger Log Toolbar, page 8-96.

View the Earliest Set of Alarm Triggers

To view the earliest set of alarm triggers in the Trigger Log:

Step 1 Use the procedure to View the Trigger Log, page 8-66.

Step 2 Click the **Show Oldest** icon in the Trigger Log Toolbar, page 8-96.

The list of alarm triggers is redisplayed in the Trigger Log, starting with the beginning of the list.

Change the Number of Triggers Displayed in Trigger Log

By default, you can browse backward or forward at the rate of ten alarm triggers per click of the **Step Back** or **Step Forward** buttons.

You can increase the number of alarm triggers to display per click by resizing the alarm trigger buffer. You can display a minimum of 10 and a maximum of 100 triggers at a time.

Change the Number of Triggers Displayed

To change the number of triggers displayed in the Trigger Log:

Step 1 Use the procedure to View the Trigger Log, page 8-66.

Step 2 Click the **Enter Number of Alarm Triggers to Display** icon in the Trigger Log Toolbar, page 8-96.

The Enter Number of Alarm Triggers to Display dialog box appears.

Step 3 Enter the number of alarm triggers you want to display in the viewing area in the Enter Number of Alarm Triggers to Display field.

Step 4 Click **OK**.

The resize count is set to the value you entered.

Show Systemwide Triggers

To show system-wide triggers:

Step 1 Use the procedure to View the Trigger Log, page 8-66.

Step 2 Click **Show System-Wide Triggers** in the Trigger Log Toolbar, page 8-96.

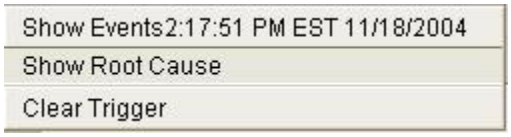
Browse Mode is interrupted. The Trigger Log returns to the state of dynamically updating triggers as they occur. See Trigger Log Toolbar, page 8-96.

Show the Root Cause of a Service Path Alarm Trigger

To show the root cause of a service path alarm trigger:

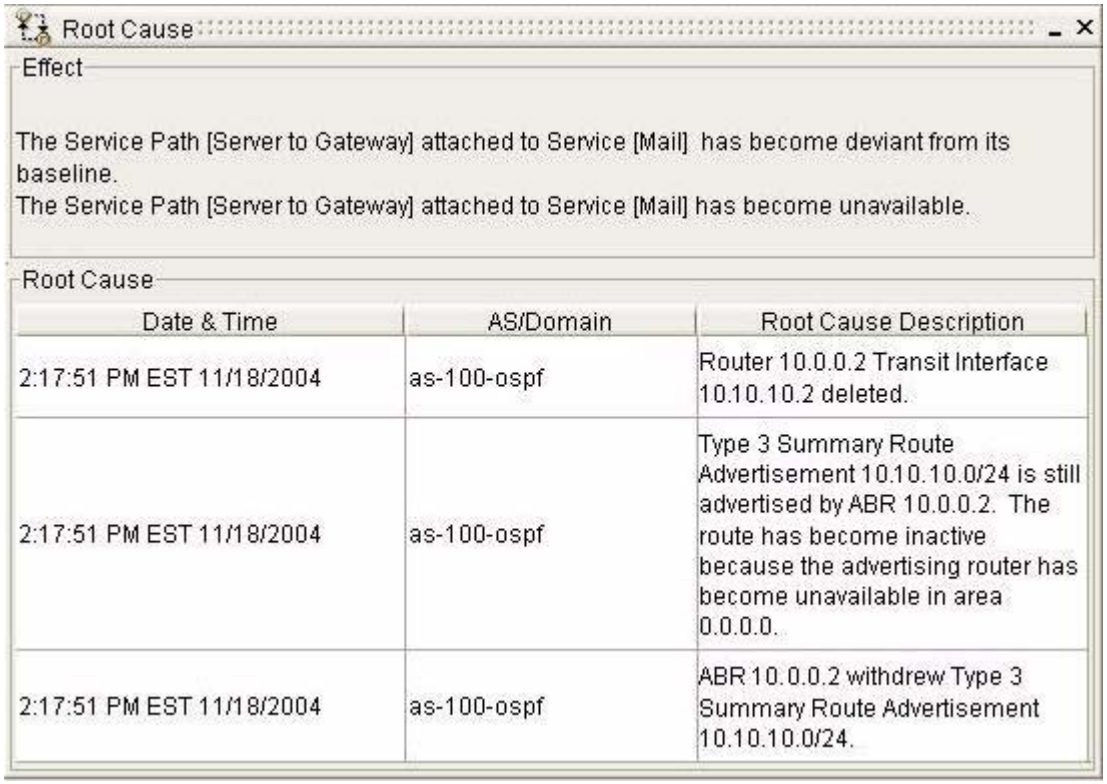
Step 1 In the Trigger Log, page 8-96 or Last 10 Triggers field, select a trigger for a service path alarm.

Step 2 Right-click and select **Show Root Cause**.



The Root Cause window appears (see Figure 8-47).

Figure 8-47 Root Cause Window for Service Path Alarm Trigger



Related Forms

The following tables detail various graphical elements and dialog boxes in the Alarm Monitor.

Alarm Monitor

From the Alarm Monitor, you can complete the following tasks:

- Configuring Alarms, page 8-4
- Viewing and Managing Alarms, page 8-55
- Working in the Trigger Log, page 8-68

Table 8-2 describes the fields and buttons of the Alarm Monitor.

Table 8-2 Alarm Monitor

Field	Description
Alarm Monitor Toolbar	See Alarm Monitor Toolbar, page 8-73.
Enterprise Hierarchy Tree	Allows you to view alarms by region, autonomous system, domain, or service.
Alarms	Provides fields and values that show details of listed alarms.
Severity	An indicator shows the severity of the alarm. For information about alarm severities and their uses, see Severity Values of Alarms, page 8-61.
Trigger State	An indicator shows the trigger state of an alarm. See Indicators of Triggered Alarms, page 8-61.
State	Indicates if a selected alarm is enabled or disabled. See Disable a Selected Alarm, page 8-65 and Re-enable an Alarm, page 8-65.
Auto-Clear	Informs you whether the auto clear functionality is selected. If **Yes** appears in the column, then the alarm will clear automatically after its trigger condition has been detected and resolved. If **No** appears in the column, then you will have to clear the alarm manually.
AS/Domain	Displays the AS or domain where the alarm resides.
Alarm ID	Displays the Alarm ID of an alarm.
Alarm Description	Describes the alarm.
Alarm Export	Displays the export destination of the alarm.
Last Trigger Time	Displays the most recent date and time that an alarm was triggered in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. Alarms that are active but have not triggered do not display a time stamp.
Trigger Count	Displays the number of times the alarm was triggered.
Last 10 Triggers	Provides fields and values that show details of the ten most recent events that triggered the alarm you selected in Alarms.
Trigger No. (Number)	Displays a number that identifies a trigger. Events, are displayed in Alarm Triggers in the order they occurred, from most recent to oldest.

Table 8-2 Alarm Monitor (continued)

Field	Description
Trigger Time	Displays the date and time that the event occurred that triggered the alarm. This information is displayed in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32.
Cleared By	Displays the name of the user who manually cleared an alarm. If the alarm was not manually cleared, **auto clear** appears in the column.
Cleared Time	Displays the time that the alarm was cleared.
Event ID	Displays the Event ID of the trigger.
Event/Trigger Description	Provides a description of the event that triggered the alarm.

Alarm Monitor Toolbar

The Alarm Monitor Toolbar provides a selection of buttons that allow you to complete the following tasks:

- Configure a BGP Alarm, page 8-4
- Configure an OSPF Alarm, page 8-19
- Globally Enable or Disable All Alarms, page 8-64
- Disable a Selected Alarm, page 8-65
- Enable a Selected Alarm, page 8-65
- Remove an Alarm, page 8-66
- Browse through the Trigger Log, page 8-68

Table 8-3 describes buttons available in the Alarm Monitor Toolbar for OSPF, BGP and Service Alarms.

z

Table 8-3 Alarm Monitor Toolbar

Button	Name	Description
	Configure Alarms	Opens the Alarm Configuration Wizard dialog box, in which you can create an alarm to notify you when a selected path changes.
	Remove Alarm	Removes a selected alarm from Alarm Monitor.
	Disable Alarm	Disables a selected alarm in Alarm Monitor.

Table 8-3 Alarm Monitor Toolbar (continued)

Button	Name	Description
	Enable Alarm	Enables a selected alarm in Alarm Monitor.
	Browse Alarm's Triggers in Trigger Log	View the set of events that triggered a selected alarm in the Trigger Log by selecting a specific alarm and clicking **Browse Alarm's Triggers in Trigger Log**. You can view the triggers of that alarm only. If you want to view all the triggers in the Trigger Log, you must click **Show Systemwide Triggers**. See Show Systemwide Triggers, page 8-70 for more information.
	Disable All Alarms	Globally disables all alarms in Alarm Monitor.
	Enable All Alarms	Globally enables all alarms in Alarm Monitor.

BGP Alarm Configuration Wizard

The BGP Alarm Configuration Wizard allows you to set alarms on BGP entities such as advertisements, threshold per routers, routes, and threshold per AS.

Table 8-4 describes the wizard pages of the BGP Alarm Configuration Wizard.

Table 8-4 BGP Alarm Configuration Wizard Pages

Wizard Page	Description
Select a Category of BGP Alarms, page 8-5	Provides options for setting BGP alarms on a variety of entities including advertisements and routes. The option you choose (Route or Advertisement) in this wizard page determines the next wizard page that appears.
BGP Alarm Configuration, Advertisement Alarms, page 8-75	Provides fields for setting alarms for notifications of changes to BGP advertisement alarms.
BGP Alarm Configuration, Threshold per Router Alarms, page 8-77	Provides fields for setting BGP threshold per router alarms for notification of when the behavior of an entity deviates from the system-perceived behavior.
BGP Alarm Configuration, Route Alarms, page 8-78	Provides fields for setting alarms for notifications of changes to BGP route alarms.

Table 8-4 BGP Alarm Configuration Wizard Pages (continued)

Wizard Page	Description
BGP Alarm Configuration, Threshold per AS Alarms, page 8-79	Provides fields for setting BGP threshold per AS alarms for notification when the behavior of an entity deviates from the system-perceived behavior.
BGP Alarm Configuration, Next Hop, page 8-80	Provides fields for setting BGP Next Hop alarms for notification when no OSPF route is available for the BGP next hop, and optionally, when only the default OSPF route is matching the BGP next hop.

BGP Alarm Configuration, Advertisement Alarms

The BGP Alarm Configuration, Advertisement Alarms wizard page provides options for setting alarms to notify you when there are any changes to advertisement alarms.

Table 8-5 describes the fields and buttons of the BGP Alarm Configuration, Advertisement Alarms wizard page.

Table 8-5 BGP Alarm Configuration, Advertisement Alarms

Field	Description
AS (drop-down menu)	Select the Autonomous System in which the route advertisements you want to alarm are advertised.
Prefix (text box)	Enter the prefix of the BGP advertisement in the form of an IP address and subnet mask. Example: `10.10.0.1/24`
Router Name (text box)	Enter the router ID, DNS name or user-defined name of the router.
Find Entity (button)	Searches for BGP route advertisements using your selections.
Add Wildcard (button)	Provides fields for setting a wildcard alarm on selected BGP advertisements.
Clear Unalarmed (button)	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear Unalarmed** removes all unset alarms.
Clear All (button)	Clears all alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear All** removes all alarm fields from the lower portion of the wizard page.

Table 8-5 BGP Alarm Configuration, Advertisement Alarms (continued)

Field	Description
Availability	Sets an availability change or flap alarm on one or more BGP Advertisements. Double-clicking the **Availability DBL CLK** button opens the Alarm Settings for BGP Advertisement Alarms dialog box and Alarm Export dialog box. The availability change alarm is triggered, by default, if the BGP advertisement changes availability once in one second. See the *Cisco Service Path Analyzer Alarm Reference* for information about all availability and flap alarms on BGP Advertisements.
AS Path	Double-click on the **AS Path DBL CLK** button to set a BGP Route Advertisement AS Path Change alarm. The AS Path attribute prevents routing loops by maintaining a list of the autonomous system numbers (ASNs) of autonomous systems the path traverses. The router can accept or reject the advertisement. If a router identifies its ASN in the advertisement sent from another router, it rejects the route.
Next Hop	Double-click on the **Next Hop DBL CLK** button to set a BGP Route Advertisement Next Hop Change alarm. The Next Hop attribute provides the IP address used to reach an advertising BGP peer.
Local Pref	Double-click on the **Local Pref DBL CLK** button to set a BGP Route Advertisement Local Pref Change alarm. The Local Pref attribute designates the preferred exit of a route from an autonomous system. Values are assigned to all exit points from an autonomous system. BGP speakers select to send data over the exit point configured with highest value.
MED	Double-click on the **MED DBL CLK** button to set a BGP Route Advertisement MED Change alarm. The Multi-Exit Discriminator (MED) attribute designates the preferred entrance of a route into the autonomous system. Values are assigned to all entry points from an autonomous system. BGP speakers identify and send data over the entry point configured with lowest value.
Community	Double-click on the **Community DBL CLK** button to set a BGP Route Advertisement Community Change alarm. The Community attribute informs a router whether to advertise a route to a community of BGP speakers.

Table 8-5 BGP Alarm Configuration, Advertisement Alarms (continued)

Field	Description
Other	Double-click on the **Other DBL CLK** button to set a BGP Route Advertisement Other Attribute Change alarm. The Other attribute notifies of changes to all other BGP attributes documented in RFC 1771 (http://www.ietf.org/rfc/rfc1771.txt) that are not listed in the BGP Alarm Configuration, Advertisement Alarms wizard page.
Any	Double-click on the **Any DBL CLK** button to set a BGP Route Advertisement Any Attribute Change alarm. The Any attribute notifies of any change to a selected BGP route advertisement.
AS	Displays the autonomous system on which the BGP advertisement resides.
Router Name	Displays the router ID, DNS name, or user defined name of the router that announces the BGP advertisement.
Prefix	Lists the IP Address and subnet mask on which the BGP Advertisement resides.

BGP Alarm Configuration, Threshold per Router Alarms

Threshold per router alarms notify you of when the system-perceived (or baseline) behavior of a particular BGP router on your network deviates by a certain percentage defined by the user.

Table 8-6 describes the fields and buttons of the BGP Alarm Configuration, Threshold per Router Alarms wizard page.

Table 8-6 BGP Alarm Configuration, Threshold per Router Alarms

Field	Description
Domain	Select the BGP domain that contains the entities for which you want to set threshold per router alarms.
Router	Enter the router name of the router that you want to associate with the threshold per router alarm.
Find Entity	Searches for BGP routers using your selections so that it can set threshold per router alarms on them.
Add Wildcard	This option is not available.
Clear Unalarmed	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear Unalarmed** removes all unset alarms.
Clear All	Clears all alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear All** removes all alarm fields from the lower portion of the wizard page.

Table 8-6 BGP Alarm Configuration, Threshold per Router Alarms (continued)

Field	Description
Advertisement Count	This alarm is triggered when the instantaneous number of route advertisements become more or less than the defined percentage of the threshold value. Double-clicking the **Advertisement Count DBL CLK** button opens the Alarm Settings dialog box for Threshold per Router Alarms and the Alarm Export dialog box. See the *Cisco Service Path Analyzer Alarm Reference* for information about BGP Threshold per Router Alarms.
Advertisement Event Rate	This alarm is triggered when the instantaneous rate of BGP advertisement events at a particular BGP router exceeds the threshold by more than the defined percentage. Double-clicking the **Advertisement Event Rate DBL CLK** button opens the Alarm Settings dialog box for Threshold per Router Alarms and the Alarm Export dialog box. See the *Cisco Service Path Analyzer Alarm Reference* for information about BGP Threshold per Router Alarms.
Router	Displays the router associated with the threshold per router alarm.
Type	Displays the type associated with the threshold per router alarm.
AS	Displays the autonomous system associated with the threshold per router alarm.

BGP Alarm Configuration, Route Alarms

The BGP Alarm Configuration, Route Alarms wizard page provides options for setting alarms to notify you when routes change in your network.

Table 8-7 describes the fields and buttons of the BGP Alarm Configuration, Route Alarms wizard page.

Table 8-7 BGP Alarm Configuration, Route Alarms

Field	Description
AS	Select the autonomous system in which the BGP routes that you want to alarm are advertised.
Prefix	Enter the prefix of the advertised route in the form of an IP address and subnet mask. Example: `10.10.0.1/24`
Find Entity	Searches for routes using your selections.
Add Wildcard	Provides fields for setting a wildcard alarm on selected routes.

Table 8-7 BGP Alarm Configuration, Route Alarms (continued)

Field	Description
Clear Unalarmed	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear Unalarmed** removes all unset alarms.
Clear All	Clears all alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear All** removes all alarm fields from the lower portion of the wizard page.
Availability	Sets an availability change or flap alarm on one or more BGP routes. Double-clicking the **Availability DBL CLK** button opens the Alarm Settings dialog box for BGP Route Alarms and the Alarm Export dialog box. The availability change alarm is triggered, by default, if the route changes availability once in one second. See the *Cisco Service Path Analyzer Alarm Reference* for information about all availability and flap alarms on routes.
Redundancy	Sets a redundancy alarm on one or more BGP routes. Double-clicking the **Redundancy DBL CLK** button opens the Alarm Settings dialog box for Interface Alarms. The redundancy change alarm is triggered, by default, if the route redundancy changes once in one second. A route is redundant when it has more than one way to reach the destination of the route. See the *Cisco Service Path Analyzer Alarm Reference* for information about all redundancy change alarms on routes.
AS	List the autonomous system on which the BGP route resides.
Prefix	List the IP Address and subnet mask on which the BGP route resides.

BGP Alarm Configuration, Threshold per AS Alarms

The BGP Alarm Configuration, Threshold per AS Alarms wizard page provides options for setting alarms to notify you when there are any changes to system perceived behavior of your entities.

Table 8-8 describes the fields and buttons of the BGP Alarm Configuration, Threshold per AS Alarms wizard page.

Table 8-8 BGP Alarm Configuration, Threshold per AS Alarms

Field	Description
Domain	Select the BGP domain that contains the entities for which you want to set threshold per AS alarms.
Find Entity	For BGP Threshold per AS alarms, the **Find Entity** button is grayed out. You can only set alarms using the **Add Wildcard** function.
Add Wildcard	Provides fields for setting a wildcard threshold per AS alarm on selected BGP routes.
Clear Unalarmed	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear Unalarmed** removes all unset alarms.
Clear All	Clears all alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear All** removes all alarm fields from the lower portion of the wizard page.
Route Count	This alarm is triggered when the number of routes in an autonomous system deviates from the defined percentage of the threshold value. Double-clicking the **Prefix Change DBL CLK** button opens the Alarm Settings dialog box for Threshold per AS Alarms and the Alarm Export dialog box. See the *Cisco Service Path Analyzer Alarm Reference* for information about BGP Threshold per AS Alarms.
Route Event Rate	This alarm is triggered when the rate of events in an autonomous system exceeds the threshold by more than the defined percentage. Double-clicking the **Route Event Rate DBL CLK** button opens the Alarm Settings dialog box for Threshold per AS Alarms and the Alarm Export dialog box See the *Cisco Service Path Analyzer Alarm Reference* for information about BGP Threshold per AS Alarms.
Type	Displays the type associated with the threshold per AS alarm.
Domain	Displays the domain associated with the threshold per AS alarm.

BGP Alarm Configuration, Next Hop

BGP Next Hop alarms notify you of the loss of next hop.

Table 8-9 describes the fields and buttons of the BGP Next Hop Alarms wizard page.

Table 8-9 BGP Alarm Settings, Next Hop Alarms

Field	Description
AS	List the autonomous system on which the advertising BGP/OSPF router resides.
Alarm Triggered If:	If the **Only the default OSPF Route is matching this BgpNextHop** check box is selected, alarm will trigger on this condition and on the **No OSPF Route available for this BgpNextHop** setting (default). If the **Only the default OSPF Route is matching this BgpNextHop** check box is not selected, alarm will trigger only on the default setting (**No OSPF Route available for this BgpNextHop**).
Alarm Cleared If:	**A non-default OSPF Route is matching this BgpNextHop** (default setting).
Alarm Settings	Click here to configure alarm settings.

OSPF Alarm Configuration Wizard

The OSPF Alarm Configuration Wizard allows you to set alarms on OSPF entities such as routers, interfaces, route advertisements, and routes.

Table 8-10 describes the wizard pages and categories of the OSPF Alarms.

Table 8-10 OSPF Alarm Configuration Wizard Pages

Wizard Page	Description
Select a Category of OSPF Alarms, page 8-19	Provides options for setting OSPF alarms on a variety of entities including interfaces, routers, Transit networks, advertisements, routes, and errors. The option you choose in this wizard page determines the next wizard page that appears.
OSPF Alarm Configuration, Interface Alarms, page 8-82	Provides fields for setting alarms for notifications of changes to Numbered Point-to-Point (NP2P), Unnumbered Point-to-Point (UP2P), and transit interfaces.
OSPF Alarm Configuration, Router Alarms, page 8-84	Provides fields for setting alarms for notifications of changes to routers.
OSPF Alarm Configuration, Transit Network Alarms, page 8-85	Provides fields for setting alarms for notifications of changes to Transit networks.
OSPF Alarm Configuration, Advertisement Alarms, page 8-87	Provides fields for setting alarms for notifications of changes to OSPF advertisements.

Table 8-10 OSPF Alarm Configuration Wizard Pages (continued)

Wizard Page	Description
OSPF Alarm Configuration, Route Alarms, page 8-88	Provides fields for setting alarms for notifications of changes to routes.
OSPF Alarm Configuration, Threshold Alarms, page 8-90	Provides fields for setting threshold alarms for notification of when the behavior of an entity deviates from the system-perceived behavior.
OSPF Alarm Configuration, Error Alarms, page 8-91	Provides fields for setting alarms for notifications of configuration errors, such as setting duplicate IP addresses.

OSPF Alarm Configuration, Interface Alarms

The OSPF Alarm Configuration, Interface Alarms wizard page provides options for setting alarms to notify you when Numbered Point-to-Point (NP2P), Unnumbered Point-to-Point (UP2P), and transit interfaces change in your network.

Table 8-11 describes the fields and buttons of the OSPF Alarm Configuration, Interface Alarms wizard page.

Table 8-11 OSPF Alarm Configuration, Interface Alarms

Field	Description
Numbered P2P	Click the check box to set an alarm on an NP2P interface.
Unnumbered P2P	Click the check box button to set an alarm on a UP2P interface.
Transit	Click the check box button to set an alarm on a transit interface.
Domain	Select the OSPF area that contains the interfaces for which you want to set alarms.
Interface or MIB	Keep the default asterisk (*), a wildcard, to search for all interfaces in the area. *or* Delete the asterisk and enter an Interface IP address of an NP2P interface or transit interface, or a MIB Index number of a UP2P interface.
Neighbor Name	Keep the default asterisk (*), a wildcard, to search for all neighbor IDs of an NP2P or UP2P interface. *or* Delete the asterisk and enter the Interface IP address or MIB Index number of the router that shares the NP2P or UP2P link.

Table 8-11 OSPF Alarm Configuration, Interface Alarms (continued)

Field	Description
Area	Keep the default asterisk (*), a wildcard, to search for interfaces in all areas. *or* Delete the asterisk and enter an area ID.
Router Name	Keep the default asterisk (*), a wildcard, to search for interfaces on all routers. *or* Delete the asterisk and enter a router name.
Find Entity	Searches for interfaces using your selections.
Add Wildcard	Provides fields for setting a wildcard alarm on selected interfaces.
Clear Unalarmed	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click Find Entity or Add Wildcards, and set some alarms, clicking Clear Unalarmed removes all unset alarms.
Clear All	Clears all alarms from the lower portion of the wizard page. For example, if you click Find Entity or Add Wildcards, and set some alarms, clicking Clear All removes all alarm fields from the lower portion of the wizard page.
Availability	Sets an availability change or flap alarm on one or more interfaces. Double-clicking the **Availability DBL CLK** button opens the Alarm Settings dialog box for Interface Alarms. The availability change alarm is triggered, by default, if the interface changes availability once in one second. See the *Cisco Service Path Analyzer Alarm Reference* for information about all availability and flap alarms on NP2P, UP2P, and Transit interfaces.
Metric	Sets a metric alarm on one or more interfaces. Double-clicking the **Metric DBL CLK** button opens the Alarm Settings dialog box for Interface Alarms. The metric change alarm is triggered, by default, if the interface metric changes once in one second. See the *Cisco Service Path Analyzer Alarm Reference* for information about all metric change alarms on NP2P, UP2P, and Transit interfaces.
Type	Displays the type of interface. Options include: • Numbered • Unnumbered • Transit

Table 8-11 OSPF Alarm Configuration, Interface Alarms (continued)

Field	Description
Domain	Displays the name of the OSPF area that contains the interface.
Area	Displays the area in which the interface resides.
Router Name	Displays the IP address or host name of the router on which the interface resides.
IF or MIB	Displays the unique identifier of the interface. • IP address for NP2P and transit interfaces. • Management Information Base (MIB) Index value for UP2P interfaces.
Neighbor Router Name	Displays the router name of the neighboring router that shares a point-to-point link. • For an NP2P link, the IP address of the neighbor interface is listed. • For a UP2P link, the MIB index of the neighbor interface is listed.

OSPF Alarm Configuration, Router Alarms

The OSPF Alarm Configuration, Router Alarms wizard page provides options for setting alarms to notify you when Routers change in your network.

Table 8-12 describes the fields and buttons of the OSPF Alarm Configuration, Router Alarms wizard page.

Table 8-12 OSPF Alarm Configuration, Router Alarms

Field	Description
Router	This check box is selected and grayed out if you selected Router from Select a Category of OSPF Alarms.
Domain	Select the OSPF area that contains the routers for which you want to set alarms.
Router Name	Keep the default asterisk (*), a wildcard, to search for interfaces on all routers. Delete the asterisk and enter the Router ID, DNS name, or user defined name of the router.
Find Entity	Searches for routers using your selections.
Add Wildcard	Provides fields for setting a wildcard alarm on selected routers.
Clear Unalarmed	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear Unalarmed** removes all unset alarms.

Table 8-12 OSPF Alarm Configuration, Router Alarms (continued)

Field	Description
Clear All	Clears all alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear All** removes all alarm fields from the lower portion of the wizard page.
Availability	Sets an availability change or flap alarm on one or more routers. Double-clicking the **Availability DBL CLK** button opens the Alarm Settings dialog box and the Alarm Export dialog box. The availability change alarm is triggered, by default, if the router changes availability once in one second. See the *Cisco Service Path Analyzer Alarm Reference* for information about all availability and flap alarms on routers.
ABR Status	Allows you to set an availability change or flap alarm on one or more ABRs. The availability change alarm is triggered if the ABR intermittently changes availability in the selected timeframe. See Configuring Alarms, page 8-4.
ASBR Status	Allows you to set an availability change or flap alarm on one or more ASBRs. The availability change alarm is triggered if the ASBR intermittently changes availability in the selected timeframe. See Configuring Alarms, page 8-4.
Area Count	Allows you to set an area count change alarm on one or more selected routers. The alarm is triggered if changes occur to the number of areas in which the router is configured.
Domain	Displays the name of the OSPF area that contains the interface.
Router Name	Displays the IP address, DNS name, or user defined name of the router on which the interface resides.

OSPF Alarm Configuration, Transit Network Alarms

The OSPF Alarm Configuration, Transit Network Alarms wizard page provides options for setting alarms to notify you when Transit networks change in your network.

Table 8-13 describes the fields and buttons of the OSPF Alarm Configuration, Transit Network Alarms wizard page.

Table 8-13 OSPF Alarm Configuration, Transit Network Alarms

Field	Description
Transit Network	This check box is selected and grayed out if you selected Transit networks from Select a category of OSPF Alarms.
Domain	Select the OSPF area that contains the Transit networks for which you want to set alarms.
Prefix	Keep the default asterisk (*), a wildcard, to search for all prefixes in the area. *or* Delete the asterisk and enter a prefix of a Transit network.
Area ID	Keep the default asterisk (*), a wildcard, to search for Transit networks in all areas. *or* Delete the asterisk and enter an area ID.
Find Entity	Searches for Transit networks using your selections.
Add Wildcard	Provides fields for setting a wildcard alarm on selected Transit networks.
Clear Unalarmed	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear Unalarmed** removes all unset alarms.
Clear All	Clears all alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear All** removes all alarm fields from the lower portion of the wizard page.
Availability	Sets an availability change or flap alarm on one or more Transit networks. Double-clicking the **Availability DBL CLK** button opens the Alarm Settings dialog box for Transit Network Alarms and the Alarm Export dialog box. The availability change alarm is triggered, by default, if the Transit network changes availability once in one second.
DR Change	Allows you to set a Designated Router (DR) change alarm on one or more Transit networks. The DR change alarm is triggered if any change occurs to the DR assigned to the Transit network.
Router Count	Allows you to set a router count change alarm on one or more Transit networks. The router count change alarm is triggered if changes occur to the number of routers that form an adjacency with the Transit network.
DR IF Change	Allows you to set a Designated Router (DR) Interface change alarm on one or more Transit networks. The DR Interface change alarm is triggered if any change occurs to the availability or number of DR Interfaces assigned to the Transit network.

Table 8-13 OSPF Alarm Configuration, Transit Network Alarms (continued)

Field	Description
Domain	Displays the name of the OSPF area that contains the Transit network.
Area	Displays the area in which the Transit network resides.
Route	Displays the IP address or host name of the route on which the Transit network resides.

OSPF Alarm Configuration, Advertisement Alarms

The OSPF Alarm Configuration, Advertisement Alarms wizard page provides options for setting alarms to notify you when Stub Advertisements and External Advertisements change in your network.

Table 8-14 describes the fields and buttons of the OSPF Alarm Configuration, Advertisement Alarms wizard page.

Table 8-14 OSPF Alarm Configuration, Advertisement Alarms

Field	Description
Stub	Click the **Stub** check box to set an alarm on a stub advertisement.
External	Click the **External** check box to set an alarm on an external advertisement.
Domain	Select the OSPF area that contains the advertisements for which you want to set alarms.
Prefix	Keep the default asterisk (*), a wildcard, to search for advertisements with any prefix. Delete the asterisk and enter an IP address/subnet mask of an advertisement.
Area ID	Keep the default asterisk (*), a wildcard, to search for advertisements in all areas. Delete the asterisk and enter an area ID.
Router Name	Keep the default asterisk (*), a wildcard, to search for advertisements on all routers. Delete the asterisk and enter a router name.
Find Entity	Searches for advertisements using your selections.
Add Wildcard	Provides fields for setting a wildcard alarm on selected advertisements.

Table 8-14 OSPF Alarm Configuration, Advertisement Alarms (continued)

Field	Description
Clear Unalarmed	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear Unalarmed** removes all unset alarms.
Clear All	Clears all alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcards**, and set some alarms, clicking **Clear All** removes all alarm fields from the lower portion of the wizard page.
Availability	Sets an availability change or flap alarm on one or more interfaces. Double-clicking the **Availability DBL CLK** button opens the Alarm Settings dialog box for Advertisement Alarms and the Alarm Export dialog box. See the *Cisco Service Path Analyzer Alarm Reference* for information about all availability and flap alarms on Stub and External advertisement alarms.
Metric	Sets a metric alarm on one or more interfaces. Double-clicking the **Metric DBL CLK** button opens the Alarm Settings dialog box for Interface Alarms. The metric change alarm is triggered, by default, if the interface metric changes once in one second. See the *Cisco Service Path Analyzer Alarm Reference* for information about all metric change alarms on Stub and External advertisements.
Type	Displays the type of interface. Options include: Stub External
Domain	Displays the name of the OSPF area that contains the advertisement.
Area	Displays the area in which the advertisement resides.
Router Name	Displays the router ID, DNS name, or user-defined name of the router on which the advertisement resides.
Prefix	Displays the prefix (IP address and subnet mask) on which the advertisement resides.

OSPF Alarm Configuration, Route Alarms

The OSPF Alarm Configuration, Route Alarms wizard page provides options for setting alarms to notify you when Core Routes and External Routes change in your network.

Table 8-15 describes the fields and buttons of the OSPF Alarm Configuration, Route Alarms wizard page.

Table 8-15 OSPF Alarm Configuration, Route Alarms

Field	Description
Core	Select the check box next to core to set an alarm on a core route.
External	Select the check box next to external to set an alarm on an external route.
Domain	Select the OSPF area that contains the routes for which you want to set alarms.
Prefix	Keep the default asterisk (*), a wildcard, to search for. *or* Delete the asterisk and enter a prefix.
Find Entity	Searches for routes using your selections.
Add Wildcard	Provides fields for setting a wildcard alarm on selected routes.
Clear Unalarmed	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcard**, and set some alarms, clicking **Clear Unalarmed** removes all unset alarms.
Clear All	Clears all alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcard**, and set some alarms, clicking **Clear All** removes all alarm fields from the lower portion of the wizard page.
Availability	Sets an availability change or flap alarm on one or more routes. Double-clicking the **Availability DBL CLK** button opens the Alarm Setting dialog box for Route Alarms and the Alarm Export dialog box. The availability change alarm is triggered, by default, if the route changes availability once in one second. See the *Cisco Service Path Analyzer Alarm Reference* for information about all availability and flap alarms on routes.
Redundancy	Sets a redundancy alarm on one or more routes. Double-clicking the **Redundancy DBL CLK** button opens the Alarm Settings dialog box for Interface Alarms. The redundancy change alarm is triggered, by default, if the route redundancy changes once in one second. See the *Cisco Service Path Analyzer Alarm Reference* for information about all redundancy change alarms on routes.
Type	Displays the type of interface. Options include: • Core • External
Domain	Displays the name of the OSPF area that contains the route.
Prefix	Displays the prefix of a route.

OSPF Alarm Configuration, Threshold Alarms

The OSPF Alarm Configuration, Threshold Alarms wizard page provides options for setting threshold alarms to notify you when the entity's behavior deviates from the system-perceived behavior by an established percentage.

Table 8-16 describes the fields and buttons of the OSPF Alarm Configuration, Threshold Alarms wizard page.

Table 8-16 OSPF Alarm Configuration, Threshold Alarms

Field	Description
Router	Select this check box to set alarms to detect percentage deviations in the number of routers or the rate of routers events from the normal values.
External Route	Select this check box to set alarms to detect percentage deviations in the number of External routes or the rate of External route events from the normal values.
Stub Route	Select this check box to set alarms to detect percentage deviations in the number of Stub routes or the rate of Stub route events from the normal values.
Transit Network	Select this check box to set alarms to detect percentage deviations in the number of Transit networks or the rate of Transit network events from the normal values.
Numbered P2P Interface	Select this check box to set alarms to detect percentage deviations in the number of numbered P2P interfaces or the rate of numbered P2P interface events from the normal values.
Unnumbered P2P Interface	Select this check box to set alarms to detect percentage deviations in the number of unnumbered P2P interfaces or the rate of unnumbered P2P interface events from the normal values.
Transit Interface	Select this check box to set alarms to detect percentage deviations in the number of Transit interfaces or the rate of Transit interface events from the normal values.
Domain	Select the OSPF area that contains the entities for which you want to set threshold alarms.
Find Entity	Searches for the entities using your selections. This button is inactive for OSPF Threshold Alarms.
Add Wildcard	Provides fields for setting a wildcard alarm on selected entities.
Clear Unalarmed	Clears all unset, unalarmed alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcard**, and set some alarms, clicking **Clear Unalarmed** removes all unset alarms.

Table 8-16 OSPF Alarm Configuration, Threshold Alarms

Field	Description
Clear All	Clears all alarms from the lower portion of the wizard page. For example, if you click **Find Entity** or **Add Wildcard**, and set some alarms, clicking **Clear All** removes all alarm fields from the lower portion of the wizard page.
Entity Count	The entity count threshold alarm is triggered when the number of entities becomes more than the defined percentage of the threshold value. Double-clicking the **Entity Rate DBL CLK** button opens the Alarm Settings dialog box for Threshold Alarms and the Alarm Export dialog box. See the *Cisco Service Path Analyzer Alarm Reference* for information about OSPF threshold alarms.
Event Rate	The event rate threshold alarm is triggered when the rate of events exceeds the threshold by more than the defined percentage. Double-clicking the **Event Rate DBL CLK** button opens the Alarm Settings and Alarm Export dialog box. See the *Cisco Service Path Analyzer Alarm Reference* for information about OSPF threshold alarms.
Type	Displays the type of threshold alarm.
Domain	Displays the domain where the threshold alarm is located.

OSPF Alarm Configuration, Error Alarms

The OSPF Alarm Configuration, Error Alarms wizard page provides options for setting alarms to notify you when interface address conflict errors occur in your network.

Table 8-17 describes the fields and buttons of the OSPF Alarm Configuration, Error Alarms wizard page.

Table 8-17 OSPF Alarm Configuration, Error Alarms

Field	Description
Interface Conflict Errors	This check box is selected and grayed out if you selected Errors from **Select a Category of OSPF Alarms**.
Detection	Allows you to set an alarm that notifies you of interface address conflicts in your network.
Resolution	Allows you to set an alarm that notifies you when an interface address conflict is resolved in your network.
Domain	Select the OSPF area that contains the interfaces for which you want to set alarms.
Description	Any interface address conflict.

Service Alarm Configuration Wizard

The Service Alarm Configuration Wizard allows you to set alarms on unicast and multicast Service and Service Path entities.

Table 8-18 describes the wizard pages of the Unicast Service Alarm Configuration Wizard.

Table 8-18 Service Alarm Configuration Wizard Pages

Wizard Page	Description
Select a category of Unicast Service Alarms	Provides options for setting Service alarms on a variety of entities including Service and Service Paths. The option you choose in this wizard page determines the next wizard page that appears.
Unicast Service Alarm Configuration, Service Alarms, page 8-92	Provides fields for setting alarms for notifications of changes to Unicast Service alarms.
Unicast Service Alarm Configuration, Service Path Alarms, page 8-93	Provides fields for setting alarms for notifications of changes to Unicast Service Path alarms.
Multicast Service Alarm Configuration, Service Alarms, page 8-94	Provides fields for setting alarms for notifications of changes to Multicast Service alarms.
Multicast Service Alarm Configuration, SSM Multicast Group Alarms, page 8-95	Provides fields for setting alarms for notifications of changes to SSM Multicast Service Group alarms.

Unicast Service Alarm Configuration, Service Alarms

In the Service Alarm Configuration Wizard, you can set alarms on services. See Configure a Unicast Service Alarm, page 8-44. For detailed information about service alarms, see *Service Alarms* in the *Cisco Service Path Analyzer Alarm Reference*.

Table 8-19 describes the fields and buttons of the Service Alarm Configuration Wizard.

Table 8-19 Unicast Service Alarm Configuration Wizard, Service Alarms

Field	Description
Availability	Allows you to set an availability or flap alarm on one or more unicast services. The availability alarm is triggered if the service varies between availability and unavailability on the network. The flap alarm is triggered if the unicast service changes availability from Down to Up twice in 180 seconds (3 minutes), or changes a specified number of times in a specified timeframe. See the *Cisco Service Path Analyzer Alarm Reference Guide* for more information on Service Alarms.
Conformity	Allows you to set a conformity alarm on a unicast service. The alarm is triggered if the service deviates from the set measure of conformity specified in Service Monitor when you created the service.
Service Name	Displays the name of the service.

Unicast Service Alarm Configuration, Service Path Alarms

In the Service Alarm Configuration Wizard, you can set alarms on unicast service paths. See Configure a Unicast Service Path Alarm, page 8-46. For detailed information about service path alarms, see *Service Path Alarms* in the *Cisco Service Path Analyzer Alarm Reference*.

Table 8-20 describes the fields and buttons of the Unicast Service Path.

Table 8-20 Unicast Service Alarm Configuration Wizard, Service Path Alarms

Field	Description
Availability	Allows you to set an availability or flap alarm on one or more unicast service paths. The availability alarm is triggered if the service path varies between availability and unavailability on the network. The flap alarm is triggered if the service path changes availability from Down to Up twice in 180 seconds (3 minutes), or changes a specified number of times in a specified timeframe. See Configure a Unicast Service Path Alarm, page 8-46 for more information.
Conformity	Allows you to set a conformity alarm on a unicast service path. The alarm is triggered if the service path deviates from the set measure of conformity specified in *Service Monitor* when you created the service path.
Loop	Allows you to set a loop alarm on a unicast service path. The alarm is triggered if there is a detection of a loop in the service path.

Table 8-20 Unicast Service Alarm Configuration Wizard, Service Path Alarms

Field	Description
Service Path Name	Displays the name of the service path.
Service Name	Displays the service name.

Multicast Service Alarm Configuration, Service Alarms

In the Service Alarm Configuration Wizard, you can set alarms on multicast services. See Configure a Multicast Service Alarm, page 8-49. For detailed information about service alarms, see *Service Alarms* in the *Cisco Service Path Analyzer Alarm Reference*.

Table 8-21 describes the fields and buttons of the Multicast Service Alarm Configuration Wizard.

Table 8-21 Multicast Service Alarm Configuration Wizard, Service Alarms

Field	Description
Availability	Allows you to set an availability or flap alarm on one or more services. The availability alarm is triggered if the service varies between availability and unavailability on the network. The flap alarm is triggered if the service changes availability from Down to Up twice in 180 seconds (3 minutes), or changes a specified number of times in a specified time period. See Service Alarms in the *Cisco Service Path Analyzer Alarm Reference*.
Conformity	Allows you to set a conformity alarm on a multicast service. The alarm is triggered if the service deviates from the set measure of conformity specified in Service Monitor when you created the service. The flap alarm is triggered when any service path of a multicast service intermittently deviates from the set baseline a specified number of times within a set interval of time.
Redundancy	Allows you to set redundancy or flap alarm on one or more multicast services. The redundancy alarm is triggered if the service becomes redundant or non-redundant. A multicast service is considered redundant when there is more than one path to a given leaf. The flap alarm is triggered if the multicast service intermittently changes from redundant to non-redundant within the specified time period.
Service Name	Displays the name of the multicast service.

Multicast Service Alarm Configuration, SSM Multicast Group Alarms

In the Service Alarm Configuration Wizard, you can set alarms on multicast service groups. See Configure a SSM Multicast Group Alarm, page 8-52. For detailed information about service alarms, see *Service Alarms* in the *Cisco Service Path Analyzer Alarm Reference*.

Table 8-22 describes the fields and buttons of the Service Alarm Configuration Wizard.

Table 8-22 Multicast Service Alarm Configuration Wizard, SSM Multicast Group Alarms

Field	Description
Availability	Allows you to set an availability or flap alarm on an SSM Multicast Group. The availability alarm is triggered if the multicast service group varies between availability and unavailability on the network. The flap alarm is triggered if the multicast service group changes availability from Down to Up twice in 180 seconds (3 minutes), or changes a specified number of times in a specified time period. See Service Alarms in the *Cisco Service Path Analyzer Alarm Reference*.
Conformity	Allows you to set a conformity alarm on a multicast service group The alarm is triggered if a group deviates from the set baseline specified in Service Monitor at least once in the set time period. The flap alarm is triggered if any SSM Multicast Group intermittently deviates from the set baseline a specified number of times within the set time period.
SSM Multicast Group Name	Displays the name of the SSM multicast service group.
Service Name	Displays the name of the multicast service.

Last 10 Triggers Dialog Box

In the Last 10 Triggers dialog box, you Clear All Alarm Triggers, page 8-63.

Table 8-23 describes the fields and buttons of the Alarm Trigger dialog box.

Table 8-23 Alarm Trigger(s)

Field	Description
Trigger Number	Displays the number of times the alarm was triggered.
Trigger Time	Displays the most recent date and time the alarm was triggered. Uses the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32.

Table 8-23 Alarm Trigger(s) (continued)

Field	Description
Cleared By	Displays the name of the user who manually cleared the alarm. If the alarm was not manually cleared, **auto clear** appears in the column.
Cleared Time	Displays the time that the alarm was cleared.
Event ID	Provides the unique identifier of the alarm trigger.
Event/Trigger Description	Describes the event that triggered the alarm.

Trigger Log

In the Trigger Log, you can complete the following tasks:

- Browse Backward, page 8-68
- Browse Forward, page 8-68
- Refresh the List of Alarm Triggers, page 8-69
- View the Earliest Set of Alarm Triggers, page 8-69
- Change the Number of Triggers Displayed, page 8-70
- Show Systemwide Triggers, page 8-70

Trigger Log Toolbar

Table 8-24 describes buttons on the toolbar of the Trigger Log.

Table 8-24 Trigger Log Toolbar Buttons

Button	Name	Description
	Show Oldest	Returns the Trigger Log to the beginning of the set of alarm triggers. See View the Earliest Set of Alarm Triggers, page 8-69.
	Step Back	Interrupts dynamic updating and sets the Trigger Log to Browse Mode, allowing you to browse backward through the list of alarm triggers. See Browse Backward, page 8-68.

Table 8-24 Trigger Log Toolbar Buttons (continued)

Button	Name	Description
	Step Forward	Enables you to browse forward through the list of alarm triggers when the Trigger Log is set in Browse Mode. This icon is unavailable when the Trigger Log dynamically updates alarm triggers. See Browse Forward, page 8-68.
	Show Current	Interrupts Browse Mode and restores dynamic updating. Updates the list of events to show the most recent set of alarm triggers. This icon becomes available in Browse Mode. It is unavailable when the Trigger Log dynamically updates events. **Note:** The Trigger Log dynamically receives updates as alarms are triggered. See Refresh the List of Alarm Triggers, page 8-69.
	Number of Alarm Triggers to Display	Opens the **Enter Number of Alarm Triggers to Display** dialog box, in which you can change the size of the viewing area for alarm triggers from 10 to 100. See Change the Number of Triggers Displayed, page 8-70.
	Show System Wide Triggers	Interrupts Browse Mode and restores dynamic updating. Updates the list of events to show system wide triggers. This icon becomes available in Browse Mode. It is unavailable when the Trigger Log dynamically updates events. **Note:** The Trigger Log dynamically receives updates as alarms are triggered. See Show Systemwide Triggers, page 8-70.

Trigger Log

Table 8-25 describes the fields and buttons of the Trigger Log.

Table 8-25 Trigger Log Fields and Buttons

Field	Description
Severity	Presents a sphere-shaped indicator that represents the severity of the alarm trigger. For information about alarm severities, see Severity Values of Alarms, page 8-61.
Alarm ID	Displays the Alarm ID of the alarm associated with the trigger.
Alarm Description	Describes the alarm associated with the trigger.

Table 8-25 Trigger Log Fields and Buttons (continued)

Field	Description
Trigger Number	Displays the number of times the alarm was triggered.
AS/Domain	Displays the autonomous system or domain associated with the trigger.
Trigger Time	Displays the time and date when the alarm was triggered, in the format defined in your user preferences. See Set the Formatting of Dates and Times, page 1-32. **Note:** If the Date and Time of an alarm trigger is not displayed in the Date/Time field, refer to the date and time of the next alarm trigger in the list for this information.
Cleared By	Displays the name of the user who manually cleared the alarm. If the alarm was not manually cleared, **auto clear** appears in the column.
Cleared Time	Displays the time that the alarm was cleared.
Event ID	Provides the unique identifier of the alarm trigger.
Event/Trigger Description	Describes the event that triggered the alarm.
Event Time	Displays the time of the event.

Root Cause

Table 8-26 describes the fields and buttons of the Root Cause window. You can access the root cause window only if a service path alarm is triggered.

Table 8-26 Trigger Log Root Cause

Field	Description
Date & Time	Displays the date and time of the event that triggered a service path alarm.
AS/Domain	Displays the AS or domain of the event that triggered the service path alarm.
Root Cause Description	Displays the description of the event that triggered the services path alarm trigger.

CHAPTER 9

Generating Reports

Generating Reports Showing Network Changes and Trends over Time

The Report Manager in RouteDynamics contains standard reports, and lets you customize reports as well.

Reports and Charts

Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) Report Manager allows you to collect important information about your Path Analyzer system in an easy-to-comprehend, printable format.

Each Path Analyzer report contains a set of predetermined charts that tells the complete story of your changing network at a glance. These charts are packaged in a way that enables you to detect key activity and trends in your network. For example, you can identify multi-domain OSPF and BGP trends, or view data on key speakers in the network.

Customized Reports

You can also customize reports by creating charts to identify specific network conditions such as:

- Router activity
- Type 3 summary route updates by each ABR router
- Noisiest routers on your network

The charts included in reports, when accompanied by selected routing information derived from your Path Analyzer system, provide the macro and micro viewpoints of your network in a readable and printable form.

For information about creating specific, individual charts in Chart Manager, see Chapter 10, “Generating Charts”. For information about creating reports in Report Manager, see Creating Reports, page 9-2.

Report Manager Tasks

- Starting Report Manager, page 9-2
- Creating Reports, page 9-2
- Managing Reports, page 9-6
- Managing Charts from Report Manager, page 9-9
- Types of Reports, page 9-15

Starting Report Manager

To run and view reports, you must first start the Report Manager.

Start Report Manager

To start Report Manager, click **Start > Report Manager**.

The Report Manager opens in Path Analyzer.

Creating Reports

To create a report, complete the following steps:

- Start the Report Wizard, page 9-2
- Select a Report, page 9-2
- Select an Autonomous System, page 9-3
- Select Time Period, page 9-5

Start the Report Wizard

To start the report wizard:

Step 1 Use the procedure to Start Report Manager, page 9-2.

The Report Manager Window appears.

Step 2 Click the **Create New Report** icon in the Report Manager Toolbar, page 9-31.

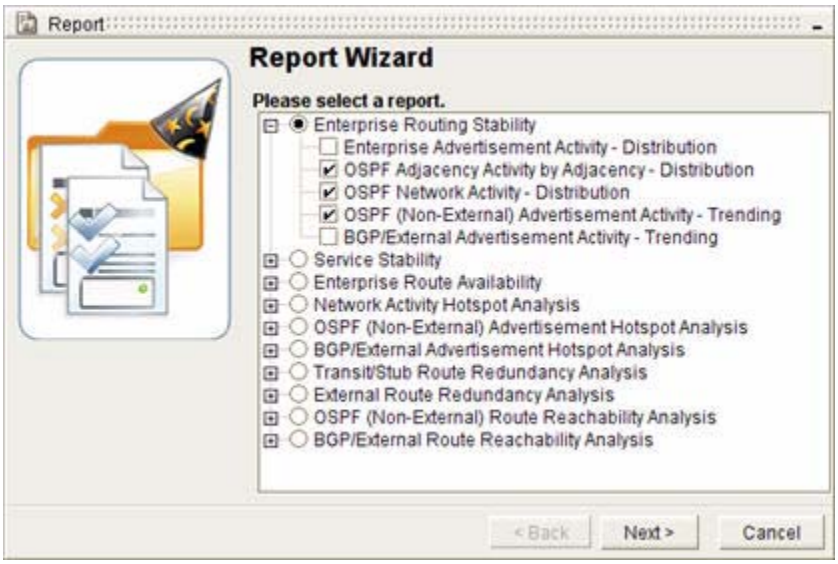
The Report Wizard opens (see Figure 9-1). If this is your first time using the Report Wizard, click the **Do not show this screen again** checkbox, and click Next.

Select a Report

To select a report in the report wizard:

Step 1 Select a report from the list of the reports that is displayed (see Figure 9-1). See Types of Reports, page 9-15 for information about the types of reports available. You can only select one report at a time.

Figure 9-1 Select a Report Screen in Report Wizard



Step 2 Click the plus (+) sign of a report to display the charts it contains. From the list, select the individual charts to include in the report, or select the radio button next to a report to include all of the report's charts.

A check mark is displayed in the check box of each selected chart.

Step 3 Click **Next**.

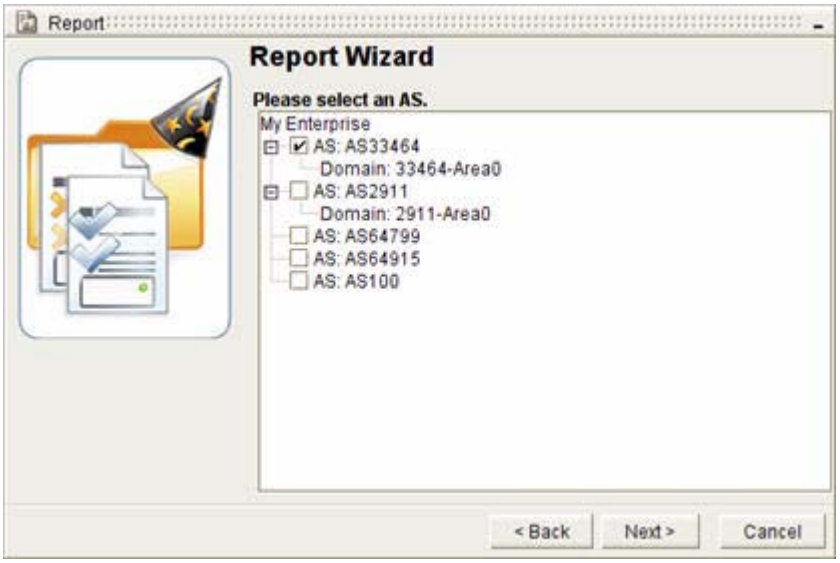
The Select AS screen appears (see Figure 9-2).

Select an Autonomous System

To select an autonomous system in the report wizard:

Step 1 Select one or more autonomous systems listed in the enterprise hierarchy to include information about in the report.

Figure 9-2 Select an Autonomous System Screen in Report Wizard



A check mark is displayed in the check box of each selected autonomous system.

Step 2 Click the plus (+) sign of an autonomous system to view the routing domains it contains. If there are routing domains associated with the autonomous system, they are automatically included with your autonomous system selection.

A check mark is displayed in the check box of each selected autonomous system.

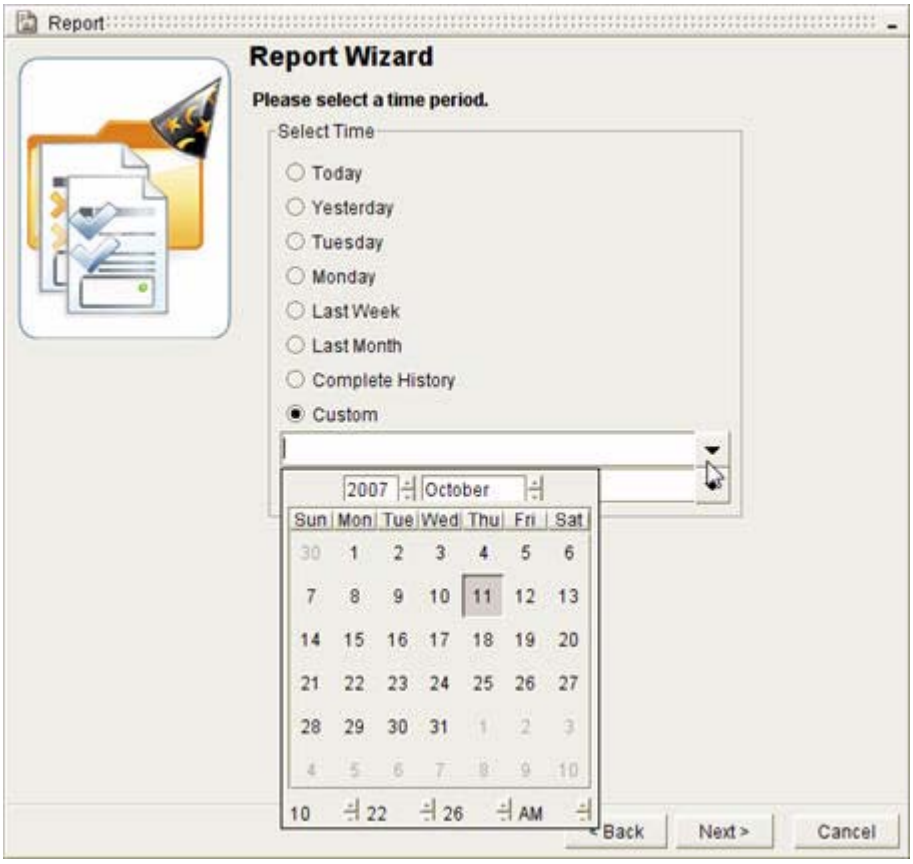
Note Selecting autonomous systems and routing domains narrows the amount of data the Path Analyzer Server returns. Limiting the scope of the data reduces the amount of bandwidth and processing power required by the Path Analyzer Server to retrieve the requested data, and by the Management Console to present it. The fixed set of data returned allows you to view and analyze a smaller and more specific set of information.

Step 3 Click **Next**.

The Select a Time Period screen appears (see Figure 9-3).

Select Time Period

Figure 9-3 Select a Time Period Screen in Report Wizard



In the Select Time Period window, you can:

Set a Predefined Period of Time, page 9-5

or

Customize a Period of Time, page 9-6

Set a Predefined Period of Time

To set a predefined period of time in the report wizard, from the Select Time section of the wizard screen, select one of the following predefined periods of time:

- **Today**
- **Yesterday**
- **Last Week**
- **Last Month**
- **Complete History**
- **Custom**

In addition, you will see all previous business days in the current week as options.

Customize a Period of Time

To customize a period of time to report on in the report wizard:

Step 1 Click **Custom** in the Select Time section of the wizard screen.

Step 2 Enter a start date and time.

a. Click the Start Time arrow in the Date dialog box.

b. Select the year and month of the start date from the calendar.

c. Select the hour, minute, second, and AM or PM options for the start time under the calendar.

d. Click the start date to complete the start of the period of time and close the calendar.

Step 3 Set an end date and time.

a. Click the End Time arrow in the Date dialog box.

b. Select the year and month of the end date from the calendar.

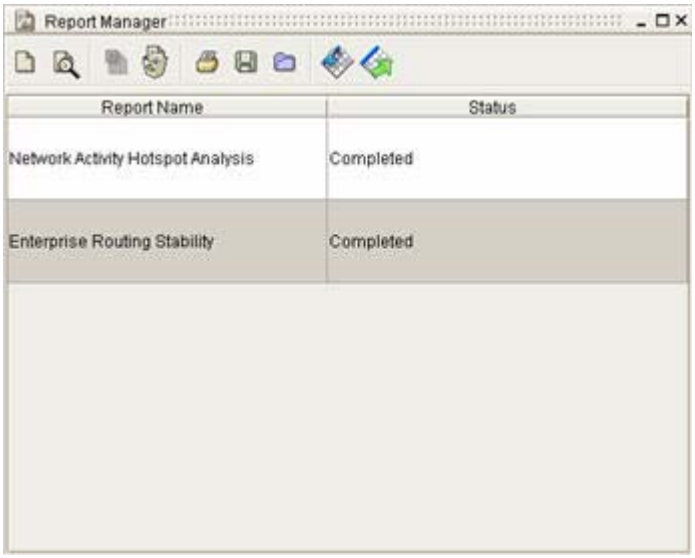
c. Select the hour, minute, second, and AM or PM options for the end time under the calendar.

d. Click the end date to complete the end of the period of time and close the calendar.

Step 4 Click **Finish**.

The Status field of the Report Manager window indicates the status of the report as it is generated (see Figure 9-4).

Figure 9-4 Report Manager Status Screen



Managing Reports

In Report Manager, you can perform the following tasks:

- View a Report, page 9-7

- Cancel a Report, page 9-7
- Delete a Report, page 9-8
- Print a Report, page 9-8
- Save a Report, page 9-8
- Load a Report, page 9-9

View a Report

To view a report:

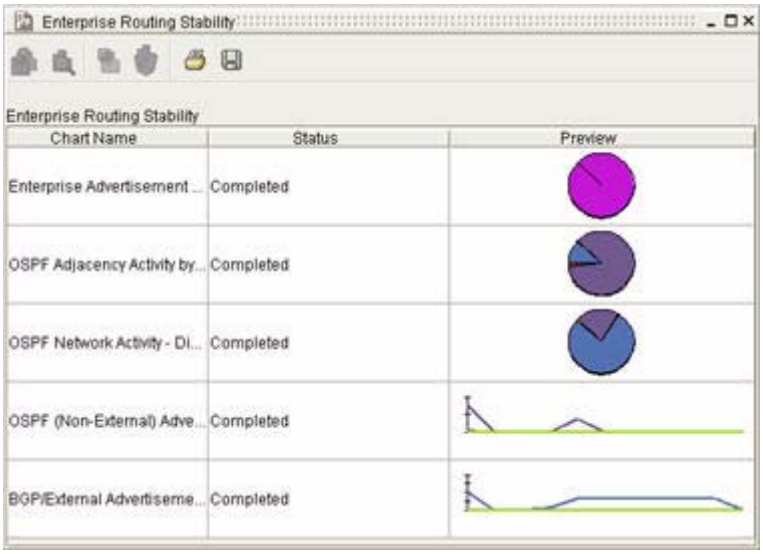
Step 1 Use the procedure to Start Report Manager, page 9-2.

Step 2 Select a report to open from the list of reports displayed.

Step 3 Click the **View Report** icon in the Report Manager Toolbar, page 9-31, or double click on the report name.

The report opens, presenting the list of charts it contains (see Figure 9-5).

Figure 9-5 View a Report window



Cancel a Report

To cancel a report:

Step 1 Use the procedure to Start Report Manager, page 9-2.

Step 2 Select a report to cancel from the list of reports displayed. You can only cancel a report if Processing appears in the Status column.

Step 3 Click the **Cancel Report** icon in the Report Manager Toolbar, page 9-31.

The Status column displays that the report is Cancelled.

Delete a Report

To delete a completed report:

Step 1 Use the procedure to Start Report Manager, page 9-2.

Step 2 Select a report to delete from the list of reports displayed.

Step 3 Click the **Delete Report** icon in the Report Manager Toolbar, page 9-31.

The report is removed from the list reports in the Report Manager window. Please note that the report is deleted without asking for confirmation.

Note You can select and deselect more than one report by using the Ctrl and Shift keys with your mouse.

Print a Report

To print a report:

Step 1 Use the procedure to Start Report Manager, page 9-2.

Step 2 Select a report to print from the list of reports displayed.

Step 3 Click the **Print Report** icon in the Report Manager Toolbar, page 9-31.

Step 4 Click **OK** in the Print window of your system.

The report is sent to the printer.

Save a Report

To save a report:

Step 1 Use the procedure to Start Report Manager, page 9-2.

Step 2 Select a report to save from the list of reports displayed.

Step 3 Click the **Save Report** icon in the Report Manager Toolbar, page 9-31.

Step 4 Select a location for the report in the Choose File dialog box, then click OK.

The report is saved in the location you specify.

Load a Report

To load a report:

Step 1 Use the procedure to Start Report Manager, page 9-2.

Step 2 Click the **Load Report** icon in the Report Manager Toolbar, page 9-31.

The Choose File dialog box appears (see Figure 9-6).

Figure 9-6 Choose File Window to Load Report

Step 3 Navigate to (browse and select) the report you want to view in the Choose File dialog box, then click **Open**.

The report now appears in the list of reports in the Report Manager window.

Managing Charts from Report Manager

For information about managing individual charts in Chart Manager, see Generating Reports, page 9-1. You can perform the following tasks on charts in Report manager:

- Derive a Chart, page 9-10
- View a Chart, page 9-10
- Cancel a Chart, page 9-11
- Delete a Chart, page 9-12
- Scheduling a Report, page 9-12
- Pick Up Reports, page 9-15

Derive a Chart

To derive a chart from a report:

Step 1 Use the procedure to Start Report Manager, page 9-2.

Step 2 Use the procedure to View a Report, page 9-7.

Step 3 Select a chart in the Report Window, and click the **View Chart** icon, or double click on the chart name.

Step 4 Click the **Derive Chart** icon in the Chart Toolbar, page 9-32.

The Derive a Chart Wizard appears. For more information on deriving a chart, see Generating a Derived Chart, page 10-23. Once finished being generated, the derived chart is displayed in Chart Manager.

View a Chart

To view a chart:

Step 1 Use the procedure to Start Report Manager, page 9-2.

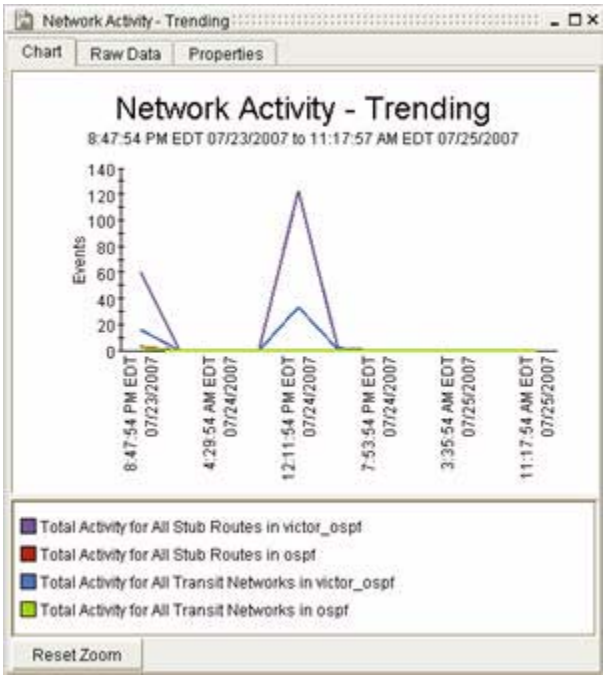
Step 2 Use the procedure to View a Report, page 9-7.

Step 3 Select a chart to view in the Report Window.

Step 4 Click the **View Chart** icon in the Chart Toolbar, page 9-32.

The chart appears in the Chart Detail dialog box (see Figure 9-7).

Figure 9-7 View a Chart Window



Step 5 Click a tab to view a break down of data:

- Select the **Chart** tab to view the chart data in tabulated form.
- Select the **Raw Data** tab to view the data used to generate the chart.
- Select the **Properties** tab to view details about how the chart was created.

Cancel a Chart

To cancel a chart:

Step 1 Use the procedure to Start Report Manager, page 9-2.

Step 2 Use the procedure to View a Report, page 9-7.

Step 3 Select a chart to cancel from the list of charts displayed. You can only cancel a chart if it's status in the Status column is Processing.

Step 4 Click the **Cancel Chart** icon in the Chart Toolbar, page 9-32.

The Status column displays the report's status as Cancelled.

Delete a Chart

To delete a chart:

Step 1 Use the procedure to Start Report Manager, page 9-2.

Step 2 Use the procedure to View a Report, page 9-7.

Step 3 In the Report Window, select a chart to delete.

Step 4 Click the **Delete Chart** icon in the Chart Toolbar, page 9-32.

The chart is removed from the list of charts.

Please note that clicking the **Delete Chart** icon deletes the chart immediately, without requesting additional confirmation.

Note From the Report window, you can print and save reports. You can also select and deselect more than one report or chart by using the **Ctrl** and **Shift** keys with your mouse.

Scheduling a Report

To schedule a report to run again, or repeatedly:

Step 1 Use the procedure to Start Report Manager, page 9-2.

The Report Manager Window appears.

Step 2 Select a report from Report Manager.

Step 3 Click the **Schedule Report** icon in the Report Manager Toolbar, page 9-31.

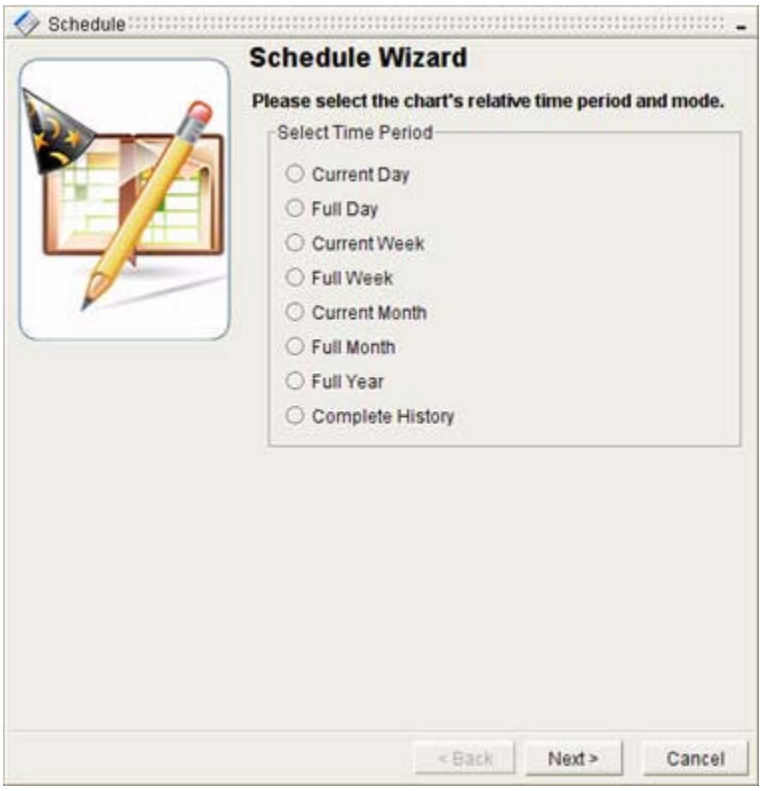
The Schedule Wizard appears. If this is your first time using the Schedule Wizard, click the **Do not show this screen again** checkbox, and click **Next**.

Step 4 Select one of the following in the Time Period screen (see Figure 9-8):

- **Current Day**—Covers from Midnight to Run Time
- **Full Day**—Covers the 24 Hours prior to Run Time
- **Current Week**—Covers from Sunday Midnight to Run Time
- **Full Week**—Covers the 7 Days prior to Run Time
- **Current Month**—Covers from First of Month to Run Time
- **Full Month**—Covers the 1 Month prior to Run Time
- **Full Year**—Covers from First of Year to Run Time

- **Complete History**—Covers from Last Database Purge to Run Time

Figure 9-8 Select Time Period Screen in Schedule Report Wizard

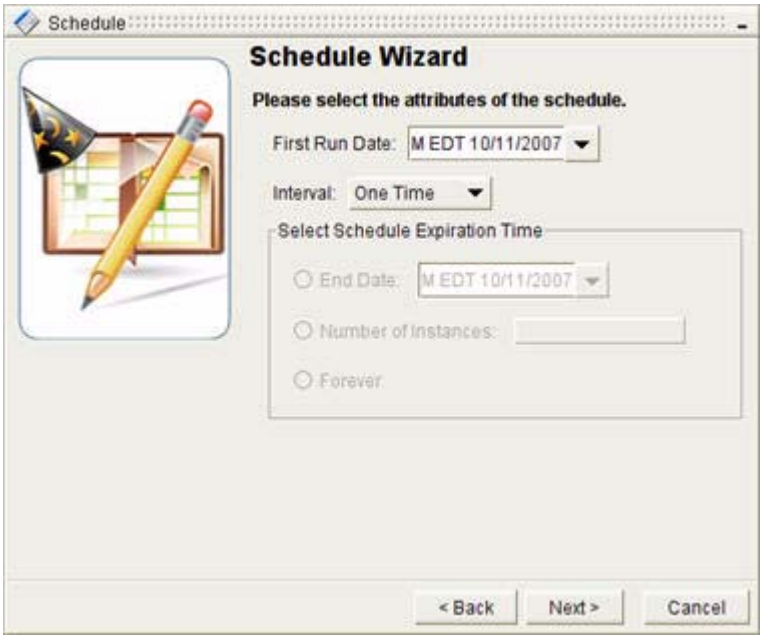


Please note that you will also be able to select any previous days of the current business week as options.

Step 5 Click **Next**.

The Select Schedule Attributes wizard screen appears (see Figure 9-9).

Figure 9-9 Select Schedule Attributes Screen in Report Wizard



Step 6 Select the First Run Date and Interval of the task from the Select Schedule Attributes wizard screen.

a. Select the date, year, month, hour, minute, second, and AM or PM options from the First Run Date drop-down box.

b. Select one of the following from the Interval drop-down box:

- **One Time**
- **Daily**
- **Weekly**
- **Monthly**
- **End of Month**
- **Yearly**

c. If you have selected an interval other than "One Time," select one of the following radio buttons from the Schedule Expiration Time field:

- **End Date**—Select an end date by selecting the **End Date** radio button, clicking the **End Date** drop-down box, and selecting the date, year, month, hour, minute, second, and AM or PM options. If you select this option, you will enter an end date for the schedule and its corresponding tasks to stop running.
- **Number of Instances**—Select how many times you want to run a schedule and its corresponding tasks by selecting the **Number of Instances** radio button, and entering the number of times the task should be repeated.
- **Forever**—Select the **Forever** radio button to run the schedule and its tasks perpetually.

Step 7 Click **Next**. A message appears to indicate that the Path Analyzer Server successfully received the schedule request.

Step 8 Click **Finish**. The new scheduled report can now be viewed in the Schedule Manager. For more information, see Chapter 11, "Scheduling Reports and Charts".

Once a report has been scheduled, you can also access its schedule and results from the Path Analyzer Web Schedule Manager. For more information, see Chapter 12, "Web-Based Report Management".

Pick Up Reports

To pick up a completed report:

Step 1 Use the procedure to Start Report Manager, page 9-2.

The Report Manager Window appears.

Step 2 Click the **Pickup my Reports** icon from the Report Manager Toolbar, page 9-31.

You can now pick up any completed scheduled reports, which causes them to appear in the Report Manager window.

Types of Reports

Path Analyzer Report Manager provides the following predefined reports for information about concurrent trends and top performers in your network.

- Enterprise Routing Stability, page 9-15
- Service Stability, page 9-17
- Enterprise Route Availability, page 9-19
- Network Activity Hotspot Analysis, page 9-21
- OSPF (Non-External) Advertisement Hotspot Analysis, page 9-22
- BGP/External Advertisement Hotspot Analysis, page 9-24
- Transit/Stub Route Redundancy Analysis, page 9-25
- External Route Redundancy Analysis, page 9-27
- OSPF (Non-External) Route Reachability Analysis, page 9-28
- BGP/External Route Reachability Analysis, page 9-29

Enterprise Routing Stability

The Enterprise Routing Stability report contains general levels of routing activity and trends for the entire enterprise network.

The following charts are included in this report:

- Enterprise Advertisement Activity—Distribution, page 9-16
- OSPF Adjacency Activity by Adjacency—Distribution, page 9-16

- OSPF Network Activity—Distribution, page 9-17
- OSPF (Non-External) Advertisement Activity—Trending, page 9-17
- BGP/External Advertisement Activity—Trending

The first three charts divide the level of routing activity into time intervals to help you identify areas of instability.

The last two charts drill down on the data presented in Enterprise Advertisement Activity chart by plotting the activity levels over time for both intra-domain (OSPF Interface and External Advertisements) and inter-domain (OSPF external and BGP routes).

Questions Answered

The following questions are addressed by this report:

- What is the overall health of the enterprise network?
- What is the general level of IP activity in the enterprise?
- What aspects of the enterprise are most or least stable?
- When was the enterprise unstable?
- Is the network currently more or less stable than it was previously?

Inputs

- List of AS and Domains: select or omit specific autonomous systems and domains
- Time Period
- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

Enterprise Advertisement Activity—Distribution

A pie chart with the total number of OSPF Interfaces, External advertisements, T3 and T4 advertisements, and BGP activity. The pie chart also displays the total number of events in addition to the distribution by protocol.

Data shown in this chart can be used to determine which aspect of the Enterprise network had the most number of updates, OSPF or BGP. OSPF activity is further partitioned into type of activity. Interface activity indicates instability of a router or interface. The ripple effect of changes to the interface is captured by the External Advertisements metric. Finally, T3 and T4 Advertisements show instability at the edges of the OSPF network. This metric can be correlated to the level of BGP activity.

OSPF Adjacency Activity by Adjacency—Distribution

A pie chart with the total amount of OSPF Interface (NP2P, UP2P, Transit Interface) activity. A pie chart also displays the total number of events in addition to distribution by network element.

The data shown in this chart can be used to determine the number of routing updates per network element. You can determine which type of network element has the most adjacency instability or greatest number of configuration changes.

OSPF Network Activity—Distribution

A pie chart showing the total amount of Transit Network and Stub Routes activity. The pie chart also displays the total number of events in addition to distribution by network type.

The data shown in this chart can be used to determine the level of subnet (stub) and Transit network instability and the number of configuration changes.

OSPF (Non-External) Advertisement Activity—Trending

The trending chart shows the amount of OSPF Interface and External Advertisements activity over time, partitioned at the specified granularity and displayed as a stacked bar graph. This chart shows when OSPF routing updates were generated and propagated through domains. The relative difference between Interfaces and T3 and T4 Advertisements activity gives an indication of the amount of ripple-effect from Interface network changes.

BGP/External Advertisement Activity—Trending

The trending chart shows the amount of OSPF External Advertisement and BGP Route activity over time and displayed at the specified granularity. This chart shows when inter-domain routing updates were generated and propagated through the Enterprise.

Service Stability

The Service Stability report gives an indication of how the IP network is affecting business critical applications and departments that use the network. A base activity level is shown both over time and partitioned by service. This allows you to determine how many routing updates affected services, which services were most or least affected, and when they were affected. The report also breaks the data down by level of impact and by service path, helping you ascertain if the service had total availability loss or degraded performance.

The following charts are included in this report:

- Service Activity—Classification, page 9-18
- Service Activity—Trending, page 9-18
- Availability and Baseline Activity—Classification, page 9-18
- Service Path Activity—Classification, page 9-18
- Service Stability—Classification, page 9-18
- Duration of Service Availability for Service—Trending, page 9-19

Questions Answered

The following questions are addressed by this report:

- How much impact did the IP network have on my services?
- When were my services impacted?
- To what degree were my services impacted?
- How long were my services affected?
- Which service paths were affected?

Inputs

- Time Period
- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

Service Activity—Classification

A stacked bar with the total amount of service activity. A pie chart also displays the total number of events in addition to the distribution by service. The data shown in this chart can be used to determine the number of service-affecting routing updates, and which services were affected the most.

Service Activity—Trending

A trending chart shows the amount of service activity over time, displayed at the specified granularity. This chart shows when service activity was generated. Service activity includes all events that are service and service path affecting, including availability and baseline changes. Distribution is shown by service.

Availability and Baseline Activity—Classification

A classification chart ranks services by the amount of activity generated, including availability and baseline changes within the specified time period, and is displayed as a stacked bar graph. Each activity value is subdivided into the amount of changes to availability and baseline activity. This chart shows the type of activity categorized by service characteristic. Service activity is caused by changes to service paths.

Service Path Activity—Classification

A classification chart ranks services by the amount of activity generated by each member service path within the specified time period, and is displayed as a stacked bar graph. Each activity value is subdivided into the amount of activity caused by each service path. For example, service e-commerce has an activity level of 20. Eighteen events are caused by changes to the service path originating from the Web server and destined for the order processing server. Two are caused by the reverse path. This gives you a distribution by service path for the most active services during that time period.

Service Stability—Classification

A classification chart ranks services by the number of times the stability of the service changed to one of the following states over the specified time period:

- Available and conformant to the set baseline
- Available but deviant from the baseline
- Unavailable

The chart data is displayed as a stacked bar graph. For each service, the total number of changes is subdivided into the number of times the service changed to the specific state. This chart shows the total number of changes and the distribution by stability state.

Duration of Service Availability for Service—Trending

Each classification chart ranks services by the amount of time the service was in one of the following states over the specified time period:

- Amount of time all services were available and conformant to the set baseline
- Amount of time all services were available but deviant from baseline
- Amount of time all services were unavailable

The state is displayed as a stacked bar graph. For each service, the total amount of time is subdivided into the amount of time the service was in a specific state. The chart shows the total amount of time and the amount of time spent in each state.

Please note that a separate chart for Service Availability is generated for each service.

Enterprise Route Availability

The Enterprise Route Availability report contains trending activity for both OSPF and BGP prefixes, as well as redundancy and reachability levels. Data is divided by protocol. OSPF prefixes are further subdivided into Transit/Stub and External Routes. Transit/Stub Routes are routeable addresses that reside within a domain. External Routes are routeable addresses that reside outside a domain. BGP prefixes are scoped at the level of autonomous systems.

This report includes the following charts:

- Network Activity—Trending, page 9-20
- BGP Route Activity—Trending, page 9-20
- Transit/Stub Route Redundancy—Trending, page 9-20
- External Route Redundancy—Trending, page 9-20

The Transit/Stub Route Redundancy chart maps the intra-domain routing activity shown in the Network Activity – Trending chart over time. It shows the type of network routing activity, as well as when the activity occurred at a user-defined time granularity. Similarly, the BGP Route Activity – Trending chart also maps route activity over time. The next two charts show redundancy levels for all BGP and OSPF prefixes. Redundancy level gives an indication of the degree of fault tolerance built into the routing configuration.

Questions Answered

The following questions are addressed by this report:

- What is the overall health of prefixes advertised into the enterprise network?
- What is the general level of routing activity affecting OSPF prefixes in a domain?
- What is the general level of routing activity affecting BGP prefixes in an AS?
- How much redundancy is configured into the OSPF and BGP routing configuration?
- How many OSPF/BGP prefixes were unreachable in the domain/AS?

Inputs

- List of Domains: can either select or omit certain domains
- Time Period

- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

Network Activity—Trending

The trending chart shows the amount of Transit and Stub Network activity over time, displayed at your specified granularity of time. Network activity includes changes in reachability as well as configuration changes such as advertised metric. Transit Network activity also includes all designated router changes. This chart shows when network updates were generated.

BGP Route Activity—Trending

The trending chart shows the amount of BGP route activity over time, displayed at your specified granularity of time. Prefix activity includes available and withdrawn advertisements. This chart shows when prefix updates were generated.

Transit/Stub Route Redundancy—Trending

The trending chart shows the number of redundancy changes for all Interface Routes displayed as a stacked bar. The Interface includes prefixes configured as Transit and Stub networks. A redundancy change occurs when the number of Interface routers that advertise a route to a prefix increase or decrease. Redundancy level has the following three possible values:

- **0—**No routers are advertising a route for the prefix within the domain
- **1—**One router is advertising a route for the prefix within the domain
- **1+**—More than one router is advertising a route for the prefix within the domain

This chart shows the number of redundancy changes distributed over the time period at the specified granularity. Each bar shows the total number of changes as well as how many changes increased and decreased the amount of redundancy. (Increased redundancy is moving from a 0 or 1 state to a 1+ state. Decreased redundancy is moving from a 1+ state to a 1 or 0 state.)

External Route Redundancy—Trending

The trending chart shows the number of redundancy changes for all OSPF external routes displayed as a stacked bar chart. “External” includes prefixes advertised into the OSPF network from other domains. A redundancy change occurs when the number of ASBRs that advertise a route to a prefix increase or decrease.

Redundancy level has the following three possible values:

- **0—**No routers are advertising a route, specific or less specific, for the prefix within the domain
- **1—**One router is advertising a route, specific or less specific, for the prefix within the domain
- **1+—**More than one router is advertising a route, specific or less specific, for the prefix within the domain

This chart shows the number of redundancy changes distributed over the time period at the specified granularity. Each bar shows the total number of changes, as well as how many changes increased and decreased the amount of redundancy. (Increased redundancy is moving from a 0 or 1 state to a 1+ state. Decreased redundancy is moving from a 1+ state to a 1 or 0 state.)

Network Activity Hotspot Analysis

The Network Activity Hotspot Analysis report helps you drill down and investigate general Transit and Stub Network activity, as well as Designated Router stability. Network Activity includes reachability and configuration changes for all networks in a domain. This report allows you to further narrow down the specific type of activity, when the activity occurred and which specific networks are responsible for the high level of activity.

This report contains the following charts:

- Transit Network Activity—Trending, page 9-21
- Transit Network Activity—Classification, page 9-22
- Transit Network Loss—Classification, page 9-22
- Designated Router Stability—Classification, page 9-22
- Stub Network Activity—Trending, page 9-22
- Stub Network Activity—Classification, page 9-22
- Stub Network Loss/Metric—Classification, page 9-22

Questions Answered

The following questions are addressed by this report:

- What is the overall health of transit and Stub networks?
- What is the general level of routing activity due to transit and Stub networks?
- What kind of changes are causing the high level of activity?
- When do the changes occur?
- Which networks are changing?

Inputs

- List of Domains: can either select or omit certain domains
- Time Period
- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

Transit Network Activity—Trending

The trending chart shows the amount of Transit Network activity over time, is displayed at the specified granularity. Transit Network activity includes both changes to reachability as well as configuration changes such as designated router changes. This chart shows when Transit network updates were generated.

Transit Network Activity—Classification

The classification chart shows the Transit Networks that generated the most activity within the specified time period. Activity level includes both changes to reachability as well as configuration changes such as designated router changes. This chart gives a ranking of the most active Transit Networks.

Transit Network Loss—Classification

The classification chart shows the Transit Networks that are reported as down or not reachable most often within the specified time period. This chart gives a ranking of the most unstable Transit networks as determined by reachability.

Designated Router Stability—Classification

The classification chart shows the Transit Networks that have gone through the designated router election process most often. This chart gives a ranking of the most unstable Transit networks as determined by the number of designated router changes.

Stub Network Activity—Trending

The trending chart shows the amount of Stub Network activity over time, and is displayed at the specified granularity. Stub Network activity includes both changes to reachability as well as configuration changes such as metric cost. This chart shows when Stub network updates were generated.

Stub Network Activity—Classification

The classification chart shows Stub Networks that generated the most amount of activity within the specified time period. Activity level includes both changes to reachability as well as configuration changes, such as metric cost. This chart gives a ranking of the most active Stub networks.

Stub Network Loss/Metric—Classification

The classification chart shows Stub Networks that have the most loss and most metric changes over the specified time, displayed as a stacked bar graph. This chart gives a ranking of the most active Stub networks. Each activity level is further divided by unavailability and metric changes.

OSPF (Non-External) Advertisement Hotspot Analysis

The OSPF (Non-External) Advertisement Hotspot Analysis report helps you drill down and investigate general routing activity within a domain. Intra-domain routing activity includes advertisements, withdrawn advertisements, and metric changes to prefixes within the domain. The report also displays information on interface adjacency changes, as well as the ripple effect caused by those changes. This report allows you to further narrow down the specific type of activity, the time when the activity occurred, and which specific routers and ABRs are responsible for the high level of activity.

This report contains the following charts:

- OSPF (Non-External) Advertisement Activity—Trending, page 9-23
- Adjacency Activity—Classification, page 9-23
- Adjacency Activity by Router—Classification, page 9-23
- T3 and T4 Advertisement Activity—Classification, page 9-24
- ABR Activity by Advertisement Type—Classification, page 9-24

Questions Answered

The following questions are addressed by this report:

- What is the overall health of the intra-domain routing?
- What is the ratio between Interface routing changes and the ripple effect into other OSPF areas?
- What kind of changes are causing the high level of activity?
- When do the changes occur?
- Which routers and ABRs are changing?

Inputs

- List of Domains: can either select or omit certain domains
- Time Period
- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

OSPF (Non-External) Advertisement Activity—Trending

The trending chart shows the amount of Interface and External Advertisement activity over time, displayed at the specified granularity. Interface activity includes all adjacency and configuration changes to routers and interfaces. External Advertisement activity is a measure of the ripple affect due to Interface routing changes. It includes all Type 3 and Type 4 LSAs. This chart shows the amount of each activity type and when the activity occurred.

Adjacency Activity—Classification

The classification chart ranks Interface routers by the amount of activity generated, including adjacency and metric changes within the specified time period. It is displayed as a stacked bar graph. Each activity value is subdivided into the amount of adjacency availability/ unavailability and metric changes. This chart shows the type of activity categorized by router. Activity levels for each router include changes to the interfaces on the router.

Adjacency Activity by Router—Classification

The classification chart ranks Interface routers by the amount of activity generated by type of device within the specified time period, displayed as a stacked bar graph. Each activity value is subdivided into the amount of activity generated by interface type. For example, Router 10.10.10.0 has an activity level of 20. Five of those events were generated because of changes to transit interfaces, ten can be attributed to NP2P interfaces, and the remaining five are changes to UP2P interfaces. This tells you how much activity was generated by the router and the distribution by adjacency type during the specified time period.

T3 and T4 Advertisement Activity—Classification

The classification chart ranks ABRs by the amount of activity generated, including advertisements, withdrawn advertisements, and metric changes within the specified time period. It is displayed as a stacked bar graph. Each activity value is subdivided into the amount of available/unavailable routes and metric changes. This chart shows the type of activity categorized by ABR. Activity levels for each ABR include both type 3 and type 4 advertisements.

ABR Activity by Advertisement Type—Classification

The classification chart ranks ABRs by the amount of activity generated by the type of advertisement within the specified time period, displayed as a stacked bar graph. Each activity value is subdivided into the amount of activity as a given type of LSA. For example, ABR 12.1.1.1 has an activity level of 20. 19 are type 3 advertisements and the remaining 1 is a type 4 advertisement. This tells you how much activity was generated by an ABR, distribution by advertisement type, and when the activity occurred.

BGP/External Advertisement Hotspot Analysis

The BGP/External Advertisement Hotspot Analysis report helps you drill down and investigate general routing activity within an AS and between OSPF domains. BGP/External routing activity includes advertisements, withdrawn advertisements, metric changes to prefixes outside the domain but advertised within the domain (OSPF external), and BGP prefixes. This report allows you to further narrow down the specific type of activity, when the activity occurred, and which specific BGP routers and ASBRs are responsible for the high level of activity.

Note Depending on the size of your database, this report can take a long time to run, and can delay additional Path Analyzer reporting capacity until it is finished. If you have a large database, consider scheduling this report for a time when your system is less active. For more information on scheduling reports, please see Scheduling Reports, page 11-2.

The following charts are contained in this report:

- BGP/External Advertisement Activity—Trending, page 9-25
- External Advertisement Activity by ASBR—Classification, page 9-25
- BGP Advertisement Activity—Classification, page 9-25

Questions Answered

The following questions are addressed by this report:

- What is the overall health of the BGP/External routing?
- What is the ratio between OSPF external activity and BGP activity?
- What kind of changes are causing the high level of activity?
- When do the changes occur?
- Which ASBRs are changing?

Inputs

- List of AS's: can either select or omit certain autonomous systems (AS)
- Time Period
- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

BGP/External Advertisement Activity—Trending

This chart shows the amount of OSPF external activity and BGP activity over time, and is displayed at the specified granularity. OSPF external activity includes all adjacency and configuration changes to routes originating outside the domain, but advertised into the OSPF domain. BGP activity includes all BGP routes. This chart shows the amount of each activity type and when the activity occurred.

External Advertisement Activity by ASBR—Classification

The classification chart ranks ASBRs by the amount of activity generated including available and unavailable advertisements and metric changes within the specified time period. It is displayed as a stacked bar graph. Each activity value is subdivided into the amount of available/unavailable routes and metric changes. This chart shows the type of activity categorized by ASBR. Activity levels for each ASBR include external (type 5) LSAs.

BGP Advertisement Activity—Classification

The classification chart ranks BGP routers by the amount of activity generated, including adjacency and metric/attribute changes within the specified time period. It is displayed as a stacked bar graph. Each activity value is subdivided into the amount of available/unavailable routes and metric and attribute changes. This chart shows the type of activity categorized by BGP router.

Transit/Stub Route Redundancy Analysis

The Transit/Stub Route Redundancy Analysis report helps you drill down and investigate general redundancy activity within an AS and between OSPF domains. Transit/Stub redundancy activity includes redundancy increases and decreases within the OSPF domain (Transit and Stub routes). This report allows you to further narrow down the specific type of redundancy change, when the activity occurred and which specific routes are responsible for the high level of activity.

This report contains the following charts:

- Route Redundancy – Trending, page 9-26
- Stub and Transit Network Redundancy—Classification, page 9-26
- Duration of Redundancy Route—Trending, page 9-26

Questions Answered

The following questions are addressed by this report:

- What is the redundancy health of Transit/Stub routing?
- What routes are causing the high level of activity?

- When do the changes occur?
- Which routes are the least healthy, and are redundant for the shortest period of time?

Inputs

- List of AS's: can either select or omit certain autonomous systems (AS)
- Time Period
- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

Route Redundancy – Trending

The trending chart shows the number of redundancy changes for all Interface Routes displayed as a stacked bar. Interface Routes include prefixes configured as Transit and Stub networks. External includes prefixes advertised into the OSPF network from other domains. A redundancy change occurs when the number of routers, Interface routers for Interface prefixes, and ASBRs for external prefixes that advertise a route to a prefix increase or decrease. The level of redundancy has the following three possible values:

- **0**—No routers are advertising a route for the prefix within the domain.
- **1**—One router is advertising a route for the prefix within the domain.
- **1+**—More than one router is advertising a route for the prefix within the domain.

This chart shows the number of redundancy changes distributed over the time period at the specified granularity.

Stub and Transit Network Redundancy—Classification

The classification chart ranks Interface prefixes by the number of redundancy changes generated, including redundancy loss, gain, and no redundancy within the specified time period. It is displayed as a stacked bar graph. A route can be in three states: redundant (reachable), non-redundant-reachable, non-redundant-non-reachable. Each redundancy change is subdivided into the number of times redundancy increased, decreased and was absent (i.e. No reachability). This chart shows the amount of redundancy changes categorized by prefix. A Interface prefix is not reachable if no routers advertise a route (specific or less specific) for it.

Duration of Redundancy Route—Trending

The trending chart displays the average amount of time all prefixes didn't have redundancy. This chart is best used for a specific prefix rather than for graphing the average of all prefixes.

Please note that a separate chart for Duration is generated for each Redundancy Route.

External Route Redundancy Analysis

The External Route Redundancy Analysis report helps you drill down to investigate general redundancy activity within an AS, and between OSPF domains. External Route redundancy activity includes redundancy increases and decreases for external routes advertised within the OSPF domain. This report allows you to further narrow down the specific type of redundancy change, when the activity occurred, and which specific routes are responsible for the high level of activity.

This report contains the following charts:

- Route Redundancy—Trending, page 9-27
- External Route Redundancy—Classification, page 9-27
- Duration of Redundancy Route—Trending, page 9-28

Questions Answered

The following questions are addressed by this report:

- What is the redundancy health of the intra-AS routing?
- What routes are causing the high level of activity?
- When do the changes occur?
- Which external routes are the least healthy, and redundant for the shortest period of time?

Inputs

- List of AS's: can either select or omit certain autonomous systems (AS)
- Time Period
- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

Route Redundancy—Trending

The trending chart shows the number of redundancy changes for all OSPF external routes displayed as a bar chart. A redundancy change occurs when the number of ASBRs that advertise a route to a prefix increase or decrease. Redundancy level has the following three possible values:

- **0**—No routers are advertising a route for the prefix within the domain.
- **1**—One router is advertising a route for the prefix within the domain.
- **1+**—More than one router is advertising a route for the prefix within the domain.

This chart shows the number of redundancy changes distributed over the time period at the specified granularity.

External Route Redundancy—Classification

The classification chart ranks External routes by the amount of redundancy changes generated, including loss, gain, and no redundancy within the specified time period. It is displayed as a stacked bar graph. Each redundancy change is subdivided into the number of times redundancy increased, decreased, and was absent (no reachability). This chart shows the amount of redundancy changes categorized by prefix.

Duration of Redundancy Route—Trending

The trending chart displays the average amount of time all prefixes didn't have redundancy, while ranking the prefixes by least amount of time with redundancy. This chart is best used for a specific external prefix, instead of showing the average time for all prefixes.

Please note that a separate chart for Duration is generated for each Redundancy Route.

OSPF (Non-External) Route Reachability Analysis

The OSPF (Non-External) Reachability Analysis report helps you drill down to investigate general reachability activity within an AS, and between OSPF domains. OSPF (Non-External) reachability activity includes reachability gain and loss for transit and stub routes advertised within the OSPF domain. This report allows you to further narrow down the specific type of reachability change, when the activity occurred, and which specific routes are responsible for the high level of activity.

The following charts are contained in this report:

- Transit and Stub Route Reachability—Trending, page 9-28
- Transit and Stub Route Reachability—Classification, page 9-29
- Duration of Reachability Route—Trending, page 9-29
- Duration of Availability Route—Trending, page 9-29

Questions Answered

The following questions are addressed by this report:

- What is the redundancy health of the OSPF (Non-External) routing?
- What routes are causing the high level of activity?
- When do the changes occur?
- Which transit and stub routes are the least healthy, and reachable for the shortest period of time?

Inputs

- List of AS’s: can either select or omit certain autonomous systems (AS)
- Time Period
- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

Transit and Stub Route Reachability—Trending

The trending chart shows the number of reachability changes for all OSPF Transit and Stub routes, displayed as a bar chart. A reachability change occurs when the number of OSPF routers that advertise a route or a matching, less specific route to a prefix changes from 1 to 0 or 0 to 1. This chart shows the number of reachability changes distributed over a time period at the specified granularity.

Transit and Stub Route Reachability—Classification

The classification chart ranks Transit and Stub routes by the number of times that route became unreachable within the specified time period, displayed as a bar graph. A route becomes unreachable when there are no specific or less specific advertisements available for that route. This chart shows the amount of activity categorized by route.

Duration of Reachability Route—Trending

Three charts are generated, one for each of the top Transit and Stub routes, ranked by the least amount of time spent in a state of being reachable. Each of the charts shows when the least healthy Transit and Stub routes were reachable, and for how long.

Duration of Availability Route—Trending

Three charts are generated, one for each of the top Transit and Stub routes ranked by the least amount of time spent in a state of being available. A route is available if there is a specific advertisement for that route. Each of the charts shows when the least healthy Transit and Stub routes were available, and for how long.

BGP/External Route Reachability Analysis

The BGP/External Route Reachability Analysis report helps you drill down to investigate general reachability activity within an AS and between OSPF domains. BGP/External reachability activity includes reachability gain and loss for External and BGP routes advertised within the OSPF domain. This report allows you to further narrow down the specific type of reachability change, when the activity occurred, and which specific routes are responsible for the high level of activity.

This report helps to narrow down the specific type of activity, when the activity occurred, and which specific BGP routers and ASBRs are responsible for the high level of activity.

The following charts are contained in this report:

- BGP Route Reachability—Trending, page 9-30
- BGP Route Reachability—Classification, page 9-30
- BGP Route Availability—Trending, page 9-30
- BGP Route Availability—Classification, page 9-30
- External Route Reachability—Trending, page 9-30
- External Route Reachability—Classification, page 9-31
- External Route Availability—Trending, page 9-31
- External Route Availability—Classification, page 9-31
- Duration of Reachability for External Route, page 9-31
- Duration of Availability for External Route, page 9-31
- Duration of Reachability for BGP Route, page 9-31
- Duration of Availability for BGP Route, page 9-31

Questions Answered

The following questions are addressed by this report:

- What is the reachability health of the BGP/External routing?
- What routes are causing the high level of activity?
- When do the changes occur?
- Which BGP and external routes are the least healthy, and reachable for the shortest period of time?
- Which BGP and external routes are the least healthy, and available for the shortest period of time?

Inputs

- List of AS's: can either select or omit certain autonomous systems (AS)
- Time Period
- Granularity: Minutes/Hours/Days/Weeks/Months

Chart Descriptions

BGP Route Reachability—Trending

The trending chart shows the number of reachability decreases for all BGP routes displayed as a bar chart. Reachability loss occurs when the number of routers that advertise a route or a matching less specific route to a prefix becomes 0. This chart shows the number of reachability changes distributed over a time period at the specified granularity.

BGP Route Reachability—Classification

The classification chart ranks BGP routes by the number of times that route became unreachable within the specified time period, and is displayed as a bar graph. A route becomes unreachable when there are no specific or less specific advertisements available for that route. This chart shows the amount of activity categorized by route.

BGP Route Availability—Trending

The trending chart shows the amount of unavailable activity for all BGP routes displayed as a bar chart. Availability loss occurs when the number of routers that advertise a specific route to a prefix becomes 0. This chart shows the number of availability changes distributed over a time period at the specified granularity.

BGP Route Availability—Classification

The classification chart ranks BGP routes by the number of times each route became unavailable within the specified time period. It is displayed as a bar graph. A route becomes unavailable when there are no specific advertisements available for that route. This chart shows the amount of activity categorized by route.

External Route Reachability—Trending

The trending chart shows the number of reachability decreases for all external routes, displayed as a bar chart. Reachability loss occurs when the number of routers that advertise a route or a matching less specific route to a prefix becomes 0. This chart shows the number of reachability changes distributed over the time period at specified granularity.

External Route Reachability—Classification

The classification chart ranks external routes by the number of times that route became unreachable within the specified time period, displayed as a bar graph. A route becomes unreachable when there are no specific or less specific advertisements available for that route. This chart shows the amount of activity categorized by route.

External Route Availability—Trending

The trending chart shows the number of availability decreases for all external routes, displayed as a bar chart. Availability loss occurs when the number of routers that advertise a specific route to a prefix becomes 0. This chart shows the number of availability changes distributed over a time period at the specified granularity.

External Route Availability—Classification

The classification chart ranks external routes by the number of times that route became unavailable within the specified time period, displayed as a bar graph. A route becomes unavailable when there are no specific advertisements available for that route. This chart shows the amount of activity categorized by route.

Duration of Reachability for External Route

Three charts are generated, one for each of the top external routes, ranked by the least amount of time spent in a state of being reachable. Each of the charts shows when the least healthy external routes were reachable, and for how long.

Duration of Availability for External Route

Three charts are generated, one for each of the top external routes, ranked by the least amount of time spent in a state of being available. Each of the charts shows when the least healthy external routes were available, and for how long.

Duration of Reachability for BGP Route

Three charts are generated, one for each of the top BGP routes, ranked by the least amount of time spent in a state of being reachable. Each of the charts shows when the least healthy BGP routes were reachable, and for how long.

Duration of Availability for BGP Route

Three charts are generated, one for each of the top BGP routes, ranked by the least amount of time spent in a state of being available. Each of the charts shows when the least healthy BGP routes were available, and for how long.

Related Forms

Report Manager Toolbar

Table 9-1 describes Report Manager Toolbar buttons.

Table 9-1 Report Manager Toolbar Buttons

Button	Description
	Opens the Report Wizard, in which you select a report to generate and the charts to include. For information about report types, see Types of Reports, page 9-15.
	Opens a selected report, allowing you to derive, view, or delete a chart, or save or print a report.
	Cancels a selected report.
	Deletes a selected report.
	Prints a selected report.
	Saves a selected report.
	Allows you to load a saved report.
	Allows you to schedule a report.
	Allows you to pick up your scheduled report.

Chart Toolbar

Table 9-2 describes the Chart Toolbar buttons.

Table 9-2 Report Manager Toolbar Buttons

Button	Description
	Derives charts based on the generated charts.
	Opens a selected chart, allowing you to view the chart properties, raw data, and details about the chart in tabular format.
	Cancels a selected chart.
	Deletes a selected chart.
	Prints a selected report.
	Saves a selected report.

Chart Detail Window

In the Chart Detail window, you can view properties of a chart.

Table 9-3 describes the fields and buttons of the Chart Detail window.

Table 9-3 Chart Detail Window

Field	Description
Chart tab	Allows you to view a chart in either the stacked bar or pie chart format. It also describes the total activity, route redundancy and reachability of a particular chart.
Reset Zoom (button)	Allows you to refresh your view of the chart after zooming in on a region.
Raw Data tab	Allows you to view detailed tabular raw data for the chart. The tabular heading fields will depend on the report and chart you are viewing.

Table 9-3 Chart Detail Window (continued)

Field	Description
Properties tab	Allows you to view the time period, time division length, entity types, data sets, and graph mode of a chart.
Time Period (field in Properties tab)	Shows the start and end date of the period of time you selected.
Time Division (field in Properties tab)	Shows the unit of time into which the period of time is divided.
Entities (field in Properties tab)	Shows the network elements, such as routers and routes, displayed in the chart.
Data Sets (field in Properties tab)	List the type of data sets such as Interface, T3 and T4, External, and All.
Graph Mode (field in Properties tab)	Shows the mode of the chart such as Trending, Distribution or Classification.

CHAPTER 10

Generating Charts

Using Charts to Investigate Network Changes

Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) Chart Manager lets you create bar charts, pie charts, and tables of formatted data to identify trends in OSPF and BGP routing, or to identify network entities most affected by routing changes.

Chart Manager contains wizards for creating both basic and advanced charts. For more information on the differences between basic and advanced charts, see Select a Basic or Advanced Chart, page 10-3.

By plotting data returned from a selected time period, you can discover the entities or services that had the greatest positive or negative impact on your network.

Chart Manager Tasks

- Starting Chart Manager, page 10-1
- Determining the Type of Chart to Generate, page 10-2
- Generating a Basic Chart, page 10-6
- Generating an Advanced Chart, page 10-11
- Viewing Generated Charts, page 10-24
- Managing Charts, page 10-27

Chart Manager Details

- Descriptions of Charts, page 10-29
- Related Forms, page 10-48

Starting Chart Manager

This section details the process of starting the Chart Manager.

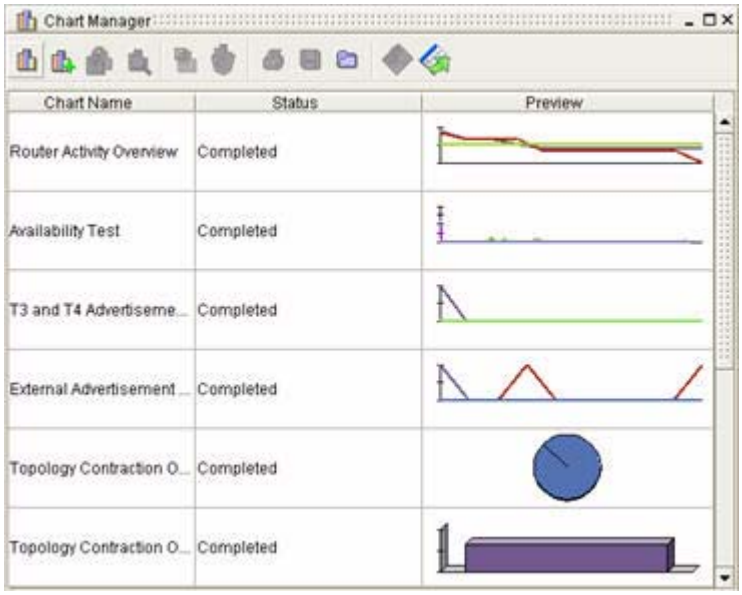
Start Chart Manager

To start the Chart Manager, click **Start > Chart Manager**.

The Chart Manager window opens in the Path Analyzer Management Console.

If you have not generated any charts, the Chart Manager window is unpopulated. Figure 10-1 shows the Chart Manager window populated with completed charts.

Figure 10-1 Chart Manager Window



Determining the Type of Chart to Generate

Before you generate a chart, you should determine the type of data you want to display. The following questions will help you decide:

- Do you want to generate a chart from a predefined template, or do you want to create a chart that provides precise, relevant information in response to a specific question?
- Do you want to view a graph that shows a general, high-level trend?
- Do you want to identify entities that have the most impact on your network?
- Do you want to view a distribution of events across your network?
- Do you want to generate a chart about a specific network entity?

The data you want to display and the way you want to format it affect your selections when you generate a chart.

The charts you generate may raise questions that can be answered by creating sets of related charts, using the Report Manager. For information about generating reports, see Chapter 9, “Generating Reports”.

Select a Basic or Advanced Chart

In Chart Manager, you can generate Basic Charts from a set of predefined chart templates, or customize Advanced Charts by providing specific details for a chart.

Note Basic Charts raise questions that can be answered by generating a set of Advanced Charts. Advanced Charts provide detailed information about a trend discovered in a Basic Chart.

Basic Charts

The Chart Wizard for Basic Charts provides a set of predefined templates from which you can create a chart. After selecting a chart template, you provide the following information to return the appropriate set of data for the chart:

- The autonomous system and routing domain.
- The period of time in which routing events occurred.
- The mode of the chart. (See Select the Mode of the Chart, page 10-4 for information about possible ways of presenting data in a chart.)

See Generating a Basic Chart, page 10-6.

Advanced Charts

Advanced Charts allow you to closely analyze specific data for a network entity or service, enabling you to identify the reasons for trends and top performers.

Advanced Charting allows you to:

- Query and derive data for specific entities—Use the Entity Filter to select specific entities of a given type. For example, you can query for a specific service path or all service paths.
- Control the period of time by:
  - Customizing the time period.
  - Dividing the period of time into intervals, called “time divisions.”
  - Show selected groupings of data—Compare more than one state, such as Available or Unavailable, of selected network entities in the same graph.
  - Customize the name of the chart.

See Generating an Advanced Chart, page 10-11.

Select the Type of Chart to Generate

For a detailed description of each chart, see Descriptions of Charts, page 10-29.

You can generate any of the following types of charts:

Enterprise Chart

Generates charts that show changes to your enterprise network, including:

- Routing activity.

- Increase or decrease in the number of routing updates passing through your network.
- Increase or decrease in the number of services that traverse your network.

Topology Chart

A subset of the Enterprise reports. Generates charts that show change within and across autonomous systems of your network, including:

- Growth or contraction of your network topology.
- Increases and decreases in the number of OSPF External Routes and BGP routes that traverse your network.
- Increases and decreases in the amount of activity and flaps of network elements, such as routers, Transit Networks, Designated Routers (DR), and Stub Routes, within OSPF areas of your network.

Routing Updates Chart

A subset of the Enterprise reports. Generates charts that show changes in the number of routes and route advertisements in your network, including:

- Increases and decreases in the amount of BGP and external route activity, flaps and redundancy on external routes, Transit and Stub Route redundancy, and Type 3 and Type 4 Summary Route activity.
- Increases and decreases in BGP, Stub, external, Type 3 Summary, and Type 4 Summary Route activity in your network.

Services Chart

A subset of the Enterprise reports. Generates charts that show changes in the amount of Service and Service path activity in your network, including:

- Increases and decreases in the amount of service activity on your network.
- Increases and decreases in the amount of service path activity on your network.

Select the Mode of the Chart

You can create charts in one of the following modes:

Trending Mode

Trending charts provide a high-level view of trends in routing events that occurred during a selected period of time. In addition, they allow you to control the granularity of the data presented. For example, you can divide a two-month period of time into eight weeks with a data point for each week, or into 60 days with a data point for each day.

Trending charts show the following data:

- X-axis shows a breakdown of the selected period of time into discrete units of time, called time divisions. Depending on the chart, time divisions may be measured in seconds, minutes, hours, days, or weeks.

- Y-axis shows selected chart data, such as the number of status flaps on a router, the number of new Type 3 Summary routes, or the amount of time services were available or conformed to the set baseline.

Classification Mode

Classification charts provide rankings of the network entities that were most affected by changes in routing during the selected period of time. When accompanying a trend chart, a classification chart shows the entities that had the most influence in creating trends on your network.

Classification charts show the following data:

- X-axis shows the unique identifier of each entity.
- Y-axis shows the number of changes or action of the entity, or the duration of time in which an entity changed.

Distribution Mode

Distribution charts provide further classification of the data, in pie chart format. For example, the Service Path Distribution chart gives both the level of service activity (i.e., total number of service events), as well as how much of the activity level affected each member service path.

Tracking Mode

Tracking charts, which are only available with Advanced Charts, provide a high-level view of network activity that occurred during an exact point in time (date/time).

Tracking charts display the following data:

- X-axis shows the date/time.
- Y-axis shows the actual measure of activity that occurred in the selected period of time.

Note You can select tracking mode for advanced charts only when you select the Choose Specific Entities option on the Select Entity Types, page 10-16 screen for the following advanced charts:

- Availability
- Reachability
- Redundancy
- Baseline Conformity
- Service Health

For more information about advanced charts, see Generating an Advanced Chart, page 10-11.

Normalized Mode

Normalized charts provide a high-level view of network activity that occurred during a selected period of time using T-Score values. For more information about T-Score values, see T-Score Normalization, page 5-4.

Note This option is only available for the Routing Activity Overview, page 10-30 basic chart. This is a canned, basic chart. For more information about basic charts, see Generating a Basic Chart, page 10-6.

Normalized charts display the following data:

- X-axis shows the divisions in the selected period of time.
- Y-axis shows the T-Score measure of activity that occurred in the selected period of time.

Generating a Basic Chart

From Chart Manager, you can create a Basic Chart from the set of predefined charts listed in the Chart Wizard.

Start the Wizard

To start the chart wizard:

Step 1 Use the procedure to Start Chart Manager, page 10-2.

Step 2 Click the **Create New Chart** icon from the Chart Manager Toolbar, page 10-48.

The Chart Wizard opens, showing the Select the Chart, page 10-6 wizard screen.

Select the Chart

To select the chart:

Step 1 Select a chart from the Select the Chart field (see Figure 10-2).

Figure 10-2 Select a Chart to Run Screen in Chart Wizard

For information about each chart selection provided, see Descriptions of Charts on page 10-29.

Step 2 Click **Next**.

The Select an Autonomous System and Domain, page 10-7 wizard screen appears.

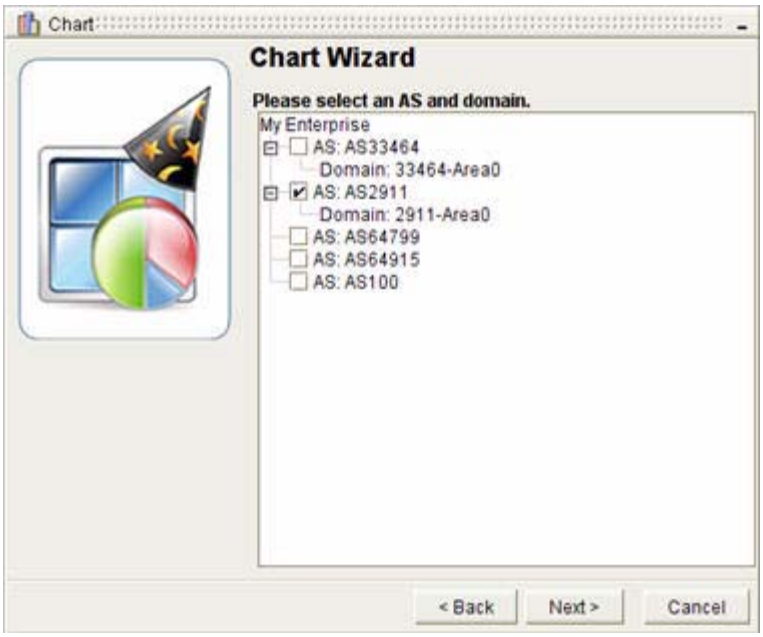
Select an Autonomous System and Domain

To select an AS and domain in the chart wizard (see Figure 10-3):

Step 1 Click the check box of at least one autonomous system from the Select AS and Domain field.

A check mark is displayed in the check box to indicate that the option is selected.

Figure 10-3 Select an Autonomous System and Domain Screen in Chart Wizard



Step 2 Click **Next**.

The Select the Period of Time wizard screen appears (see Figure 10-4).

Note Selecting autonomous systems narrows the amount of data the Path Analyzer Server returns, which in turn, reduces the amount of bandwidth and processing power required by the Path Analyzer Server to retrieve the requested data and by the Management Console to present it. In addition, the fixed set of data returned allows you to view and analyze a smaller and more specific set of information.

Select the Period of Time

In the Select Time section of the wizard screen, you can either:

- Set a Predefined Period of Time, page 10-9.

or

- Customize a Period of Time, page 10-10.

Figure 10-4 Select a Time Period and Mode Screen in Chart Wizard

Set a Predefined Period of Time

To set a predefined period of time in the chart wizard:

Step 1 Select one of the following predefined timeframes in the Select Time section of the wizard screen, s:

- **Today**
- **Yesterday**
- **Last Week**
- **Last Month**
- **Complete History**
- **Custom**

In addition, you can choose any previous business day of the current week.

Step 2 After setting the predefined period of time, Select the Mode, page 10-10 of the chart.

Customize a Period of Time

To set a customized period of time in the chart wizard:

Step 1 Click **Custom** from the Select Time section of the wizard screen.

Step 2 Enter a start date and time.

a. Click the Start Time arrow in the Date dialog box.

b. Select the year and month of the start date from the calendar.

c. Select the hour, minute, second, and AM or PM options for the start time under the calendar.

d. Click the start date to complete the start of the period of time and close the calendar.

Step 3 Set an end date and time.

a. Click the End Time arrow in the Date dialog box.

b. Select the year and month of the end date from the calendar.

c. Select the hour, minute, second, and AM or PM options for the end time under the calendar.

d. Click the end date to complete the end of the period of time and close the calendar.

Step 4 After setting the predefined period of time, Select the Mode, page 10-10 of the chart.

Select the Mode

To select the mode of the chart:

Step 1 Select one of the following options from the Select Mode field:

- **Trending Mode (Display over time)**—Shows trends by graphing changes that occur on your network during the selected time period.
- **Classification Mode (Display 10 top entities)—**Shows the top ten network entities that experienced the most change in the selected time period.
- **Distribution (Display in a pie chart)**—Shows the distribution of change across routing domains and autonomous systems.
- **Normalized—**Shows a high-level view of network activity that occurred during a selected period of time using T-Score values. (This option is only available for the Routing Activity Overview, page 10-30 basic chart.)

Step 2 Click **Next**.

A message appears indicating that the Path Analyzer Server successfully received the chart.

Note If you decide during processing that you do not want to create the chart, or that you want to create a chart with a different set of criteria, you can Cancel a Chart, page 10-11.

Step 3 Click **Finish**.

The new chart appears in Chart Manager.

Cancel a Chart During Processing

Charts can only be cancelled while they are being processed.

Cancel a Chart

To cancel a chart while it's being processed:

Step 1 Select the chart you want to cancel in the Chart Manager.

Step 2 Click the **Cancel Chart** icon in the Chart Manager Toolbar, page 10-48.

The chart request is withdrawn.

Generating an Advanced Chart

From the Chart Manager, you can create an Advanced Chart by using the Advanced Chart Wizard.

Start the Wizard

To start the advanced chart wizard:

Step 1 Use the procedure to Start Chart Manager, page 10-2.

Step 2 Click the **Create Advanced Chart** icon in the Chart Manager Toolbar, page 10-48.

The Chart Wizard opens, showing the Select Data Set, page 10-12 screen (see Figure 10-5).

Figure 10-5 Select Data Sets Screen in Advanced Chart Wizard

View Charts

To view the types of advanced charts you can generate in the advanced chart wizard:

Step 1 From the Select Data Set, page 10-12 screen, you can view following charts:

- Activity
- Availability
- Reachability
- Redundancy
- Growth
- Baseline Conformity
- Service Health

For more information about chart types and data sets, see Chart Types Associated with Data Sets, page 10-45.

Step 2 To view the data sets associated with each chart type, expand the tree by clicking on the (**+**) symbol. To collapse the tree, click on the (**–**) symbol.

Select Data Set

To select a data set in the advanced chart wizard:

Step 1 Select a data set in the Select a Data Set field by selecting the check box. You may only select one Data Set per advanced chart.

See the following sections for more information:

- Select a Data Set for an Activity Chart, page 10-13
- Select a Data Set for an Availability Chart, page 10-13
- Select a Data Set for a Reachability Chart, page 10-13
- Select a Data Set for a Redundancy Chart, page 10-13
- Select a Data Set for a Growth Chart, page 10-14
- Select a Data Set for a Baseline Conformity Chart, page 10-14
- Select a Data Set for a Service Health Chart, page 10-14

Select a Data Set for an Activity Chart

From the Select a data set field, select one of the following options:

- **Total Activity—**Returns data about all changes to the network for the entity you select on the following wizard screen.
- **Metric Changes**—Returns data about metric changes affecting the cost of traversing links and the total route cost.
- **Designated Router Activity—**Returns data about changes to the designated router.

Select a Data Set for an Availability Chart

From the Select a data set field, select one of the following options:

- **Available**—Returns data about the availability of entities you selected from the following wizard screen.
- **Unavailable**—Returns data about the unavailability of entities you selected from the following wizard screen.

Select a Data Set for a Reachability Chart

From the Select a data set field, select one of the following options:

- **Route Reachable**—Returns data bout the reachability of routes.
- **Route Unreachable—**Returns data about the unreachability of routes.

Select a Data Set for a Redundancy Chart

From the Select a data set field, select one of the following options:

- **Route Redundant—**Returns data about the redundancy of a route.
- **Route Not Redundant—**Returns data about the non-redundancy of a route.

Select a Data Set for a Growth Chart

From the Select a data set field, select one of the following options:

- **New Entities**—Returns data about all new entities in your network. A new entity is one just added to your enterprise.
- **Contracted Entities—**Returns data about all entities removed from your network.

Select a Data Set for a Baseline Conformity Chart

From the Select a data set field, select one of the following options:

- **Baseline Conformance**—Returns data about the baseline conformity of your network.
- **Baseline Deviance**—Returns data about the deviation of your network from the configured baseline of services.

Select a Data Set for a Service Health Chart

From the Select a data set field, select one of the following options:

- **Available and Conformant Activity (Service)**—Returns data about the availability and conformity of services in an autonomous system.
- **Available and Deviant Activity (Service)**—Returns data about the availability and deviation from the configured baseline of services in an autonomous system.

Step 2 Click **Next**.

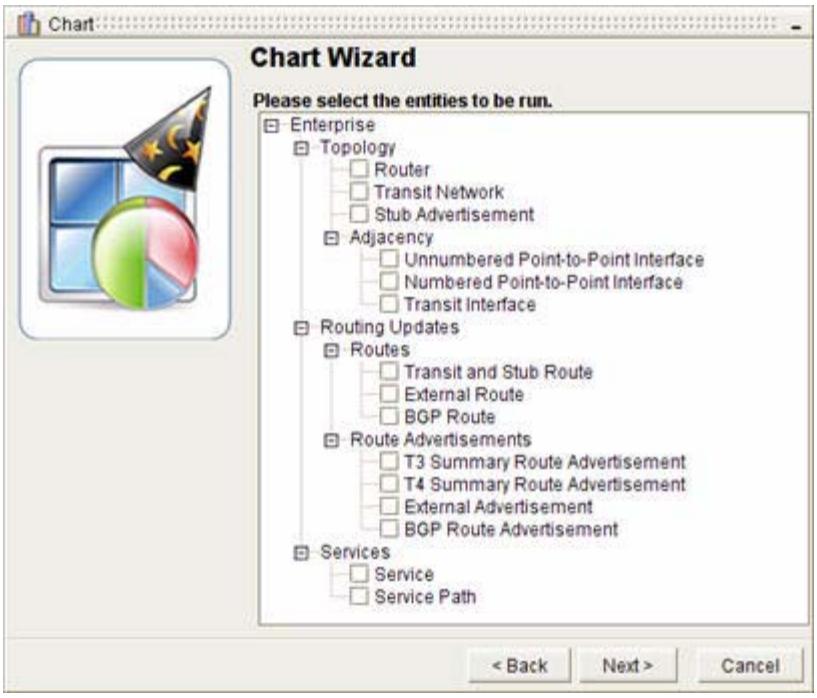
The Select Entities screen appears.

Select Entities

To select entities in the advanced chart wizard (see Figure 10-6):

Step 1 Select the entities associated with the following charts in the Select Entities, page 10-46 screen: Topology, Adjacency, Routes, Route Advertisements, Services, and/or Service Path.

Figure 10-6 Select Entities to Be Run Screen in Advanced Chart Wizard



To view the entities associated with charts, expand the tree by clicking on the (**+**) symbol. To collapse the tree, click on the (**–**) symbol. By default, the tree should already be expanded.

For more information, see Select Entities, page 10-46.

Step 2 Click **Next**.

The Select an Autonomous System and Domain wizard screen appears.

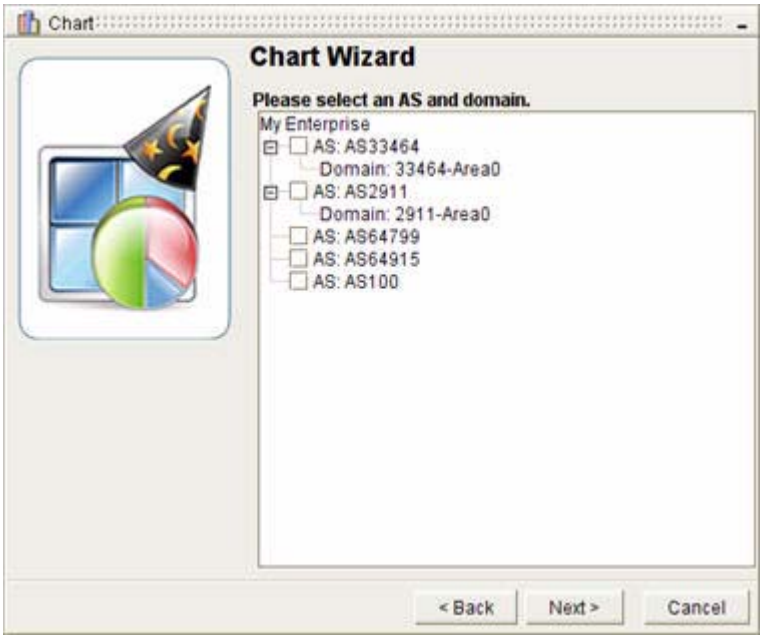
Select an Autonomous System and Domain

To select an autonomous system and domain in the advanced chart wizard (see Figure 10-7):

Step 1 Click the check box of at least one autonomous system in the Select an Autonomous System and Domain screen.

A check mark is displayed in the check box to indicate that the option is selected.

Figure 10-7 Select an AS and Domain Screen in Advanced Chart Wizard



Step 2 Click **Next**.

The Select Entity Types wizard screen appears.

Select Entity Types

To select entity types in the advanced chart wizard (see Figure 10-8):

Step 1 Select entity types in the Select entity types field:

a. Select the **Choose All Existing Entities** radio button to return data about all entities of a selected type.

or

a. Select the **Choose Specific Entities** radio button.

b. In the fields below Choose Specific Entities, either provide the unique identifier of the entity, or keep the wildcard asterisk (*) in the field to return data for all entities of the selected type. Please note that you cannot use a wildcard in conjunction with a string.

c. When you click **Next**, the Select the Specific Entity Types to be Used screen appears. It is populated with entities that match what you entered in the previous screen, or all available entities if you entered a wildcard asterisk. You can select specific entities by clicking their corresponding check boxes, or you can click the **Select all Entities** button. Please note that you will not see this screen if you selected **Choose All Existing Entities** in the Select Entity Types screen.

Figure 10-8 Select Entity Types Screen in Advanced Chart Wizard

Depending on the number of entities selected in the Select Entity Types, page 10-16 screen, you may have to select the entity types on multiple pages before arriving at the Select Time Period screen.

Step 2 Click **Next**.

Note The list of entity options varies depending on the data set you selected in the first Create Advanced Chart wizard screen.

Select the Time Period

To select the time period (see Figure 10-9):

Step 1 In the Select Time Period portion of the wizard screen:

Set a Predefined Period of Time, page 10-9.

or

Customize a Period of Time, page 10-10.

Figure 10-9 Select a Time Period Screen in Advanced Chart Wizard

Step 2 Click **Next** after setting the period of time.

The Select the Name, Mode, and Type of Chart, page 10-18 wizard screen appears.

Select the Name, Mode, and Type of Chart

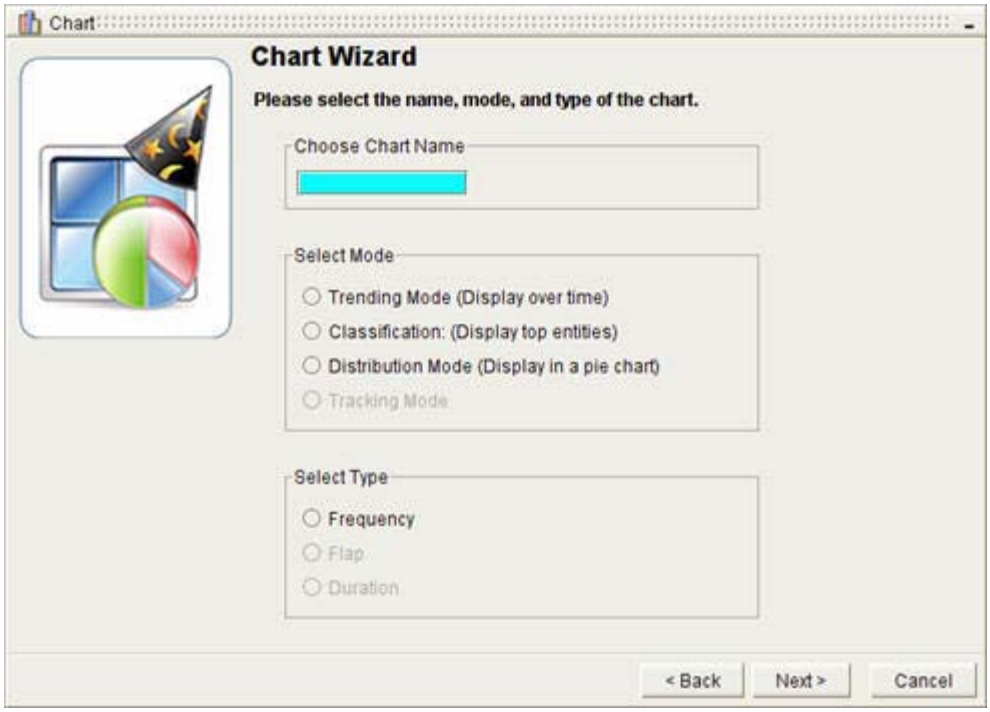
In the Select the Name, Mode, and Type of Chart screen:

- Enter a Name for the Chart, page 10-18
- Select the Mode, page 10-19
- Select Type, page 10-20

Enter a Name for the Chart

In the Choose Chart Name field (see Figure 10-10), enter a name for the chart.

Figure 10-10 Select the Name, Mode, and Type of Chart Screen in Advanced Chart Wizard



Select the Mode

To select the mode of the chart:

Step 1 Select one of the following options from the Select Mode portion of the wizard screen:

- **Trending Mode (Display over time)**—Shows trends by graphing changes that occur on your network over the selected time period.
- **Classification Mode (Display top entities)—**Shows the top ten network entities that experienced the most change in the selected time period.
- **Distribution Mode (Display in a pie chart)**—Shows the distribution of change across routing domains and autonomous systems.
- **Tracking Mode—**Shows network activity that occurs on your network at an exact instance. This option is only available when you have selected the **Choose Specific Entities** option on the Select Entity Types, page 10-16 screen for the following advanced charts:
  - Availability
  - Reachability
  - Redundancy
  - Baseline Conformity
  - Service Health

Select Type

To select the type of advanced chart, in the Select Type portion of the wizard screen, select one of the following options:

- **Frequency**
- **Flap**
- **Duration**

Please note that depending on the Data Set and Entities you selected, you may not be able to choose Flap or Duration.

Select the Time Divisions of a Trending Chart

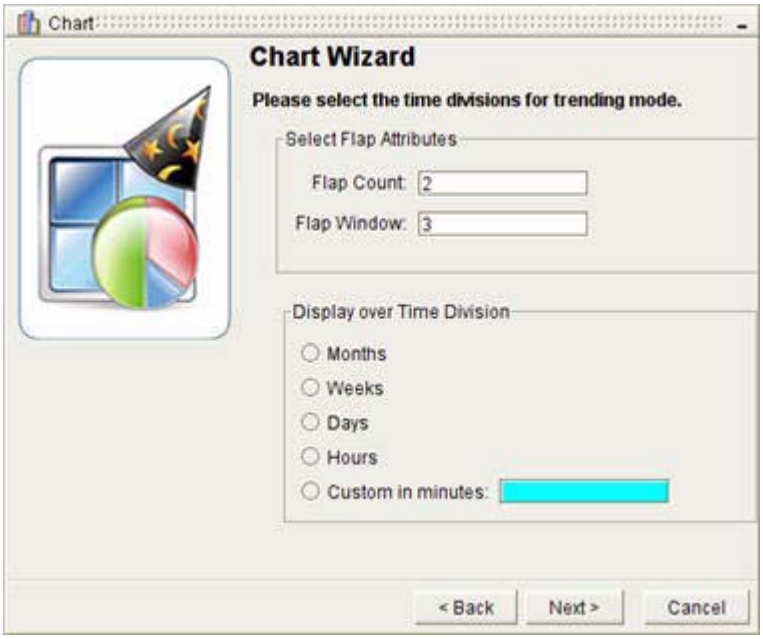
To select the time divisions for Trending charts (if **Flap** was selected from Select the Name, Mode, and Type of Chart, page 10-18 wizard screen):

Step 1 Enter the flap count (the number of flaps that occur in a selected period of time) and the flap window (number of seconds in which flaps occur) in the Flap Count and Flap Window fields (see Figure 10-11).

Step 2 Divide the period of time in the Display over Time Division area into one of the following options:

- **Months**
- **Weeks**
- **Days**
- **Hours**
- **Custom in Minutes**

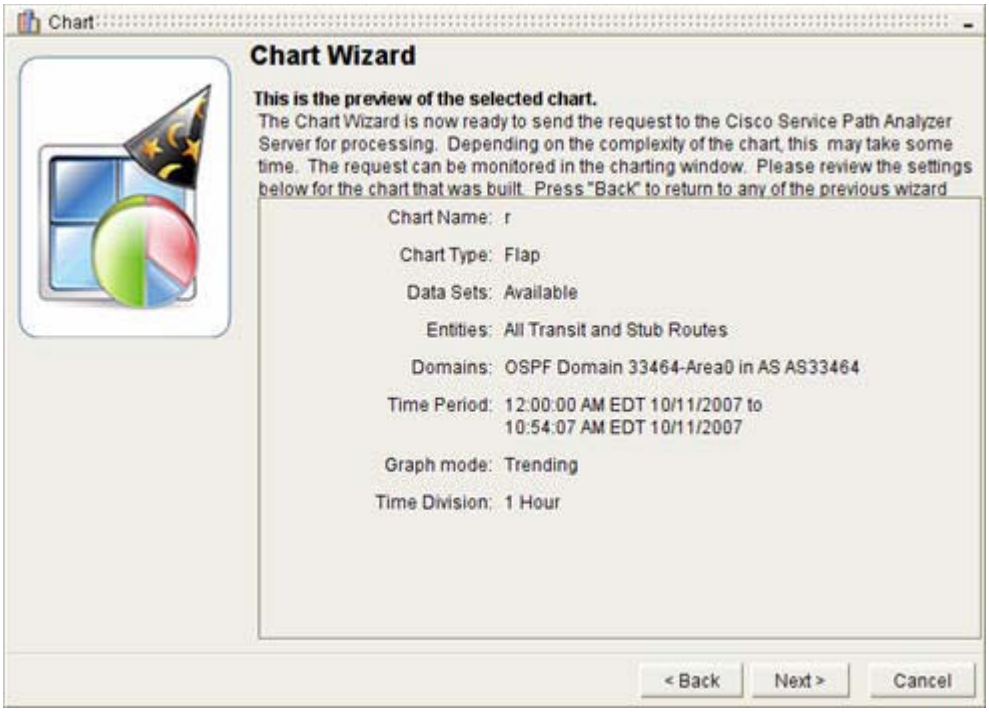
Figure 10-11 Select Time Divisions for Trending Mode in Advanced Chart Wizard



Step 3 Click **Next**.

The Preview of Chart wizard screen appears, in which you can Preview the Chart (see Figure 10-12).

Figure 10-12 Preview Selected Chart Screen in Advanced Chart Wizard



Select the Aggregators and Entities of a Classification Chart

To select the aggregators and entities for Classification charts (if **Flap** was selected from Select the Name, Mode, and Type of Chart, page 10-18 wizard screen):

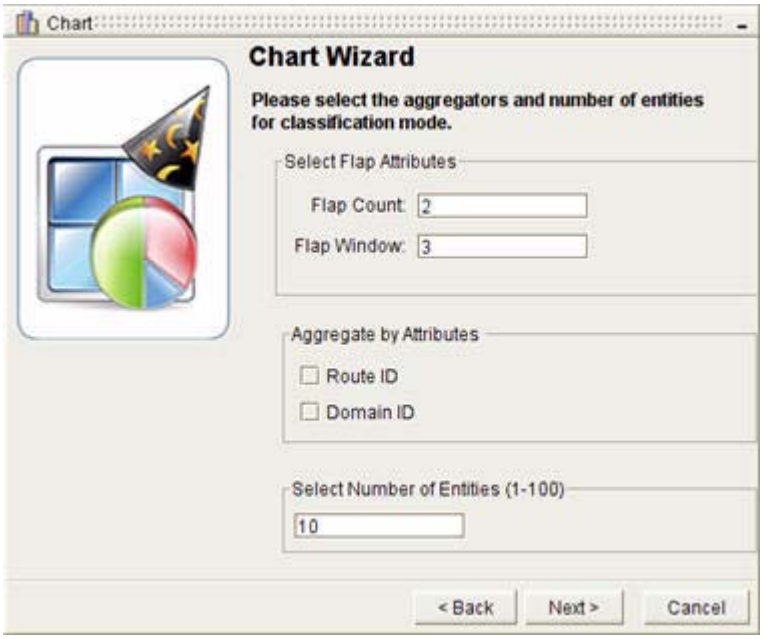
Step 1 Enter the flap count (the number of flaps that occur in a selected period of time) and the flap window (number of seconds in which flaps occur) in the Flap Count and Flap Window fields (see Figure 10-13).

Step 2 Select one of the following options in the Aggregate by Attributes area, which helps you to collect and organize the data by entity type:

- The chart type (for example, Service Name or Route ID).
- Domain ID

Step 3 Select the total number of entities to display in the chart, from 1 to 100, in the Select the Number of Entities field.

Figure 10-13 Select Aggregates by Attributes for Classification Charts Screen in Advanced Chart Wizard



Step 4 Click **Next**.

The Preview of Chart wizard screen appears, in which you can Preview the Chart, page 10-22.

Preview the Chart

To preview the chart and finish the advanced chart wizard (see Figure 10-14):

Step 1 Scroll through the list of chart settings to review your selections. To change a selection, click **Back** until you find the wizard screen that contains options you want to reset, then complete the wizard.

Figure 10-14 Preview of Selected Chart Screen in Advanced Chart Wizard

Step 2 Click **Next**. The Sending Chart Request wizard screen appears, indicating that your selections are sent to the Path Analyzer Server.

Step 3 Click **Finish**.

The Finish the Wizard screen allows you to view the status of the chart you wish to generate. This is the last screen of the Chart Wizard for advanced charts.

After you click Finish, the generated chart is listed in the Chart Manager window.

Generating a Derived Chart

Once you have created a chart either using the basic or advanced charting feature, you can create derived charts based on those generated charts.

In Chart Manager, you derived charts are created using the Derive Chart Wizard.

Start the Wizard

To start the derive a chart wizard:

Step 1 Use the procedure to Start Chart Manager, page 10-2.

Step 2 Select a chart that has already been generated from the Chart Manager window.

Step 3 Click the **Derive Chart** icon in the Chart Manager Toolbar, page 10-48.

The Chart Wizard opens, showing the Select Data Set, page 10-12 screen.

Step 4 From this point, you can follow the steps from Generating an Advanced Chart, page 10-11. You will be following the following procedures:

- View Charts, page 10-12
- Select Data Set, page 10-12
- Select Entities, page 10-14
- Select an Autonomous System and Domain, page 10-15
- Select Entity Types, page 10-16
- Select the Time Period, page 10-17
- Enter a Name for the Chart, page 10-18
- Select the Mode, page 10-19
- Select Type, page 10-20
- Select the Time Divisions of a Trending Chart, page 10-20 or Select the Aggregators and Entities of a Classification Chart, page 10-21
- Preview the Chart, page 10-22

Viewing Generated Charts

This section contains information on viewing the following aspects of charts:

- Chart Detail, page 10-24
- Chart Tab, page 10-25
- View a Chart, page 10-25
- Raw Data Tab, page 10-26
- Properties Tab, page 10-26

Chart Detail

Charts are viewed in the Chart Detail window. The title bar of the Chart Detail window lists the type of chart generated, while its tabs provide more detailed information. All charts have the following features:

- **Chart tab—**The generated graph, which is part of the chart.
- **Raw Data tab—**A view of raw data in tabular form.
- **Properties tab—**A list of the parameters you selected to generate the chart.

Chart Tab

The generated chart appears in the Chart tab. The Chart tab shows the chart as either a bar chart or pie chart, depending upon the mode that you selected in Advanced Charting. For more information, see Select the Mode, page 10-19.

Each bar chart contains the following features:

- **Title**—The title of the chart.
- **Legend**—Defines the types of entities depicted in the chart and the shows colors used to distinguish different types of entities.

Note All charts include a title and a legend that explains the data displayed. Additionally, by clicking an item's color box in the legend, you can omit all of its related data from the chart. Omitting one or more series of data allows you to isolate a specific series for closer analysis.

The following features are exclusive to Trending, Classification, and Normalized charts:

- **Y Axis**—Provides the quantitative measurement of the data presented, such as the number of interface flaps or the amount of available time.
- **X Axis**—Provides the period of time in Trending Mode or the identifiers of entities in Classification Mode.

Only Distribution charts display as a pie chart structure, which shows the distribution of data by entity and condition across the selected period of time.

View a Chart

To view a chart:

Step 1 Double-click the row that contains the chart you want to view in the table of charts in Chart Manager.

or

Select the chart from the Chart Manager Toolbar, page 10-48, and click the **View Chart** icon.

Note If you have generated more than one chart, select the first chart entry in the table of charts. The most recently generated chart is always displayed as the top entry in the table, unless otherwise sorted.

Step 2 The selected chart appears in the Chart Detail, page 10-24 dialog box.

Zoom on Chart Data

To zoom in on data in the Chart tab of the Chart Detail, page 10-24 dialog box:

Step 1 Click a bar or an axis of the chart to zoom in on chart data.

Step 2 Continue to click the chart to zoom in further on a selection.

Please note that you cannot zoom in on a Distribution (pie) chart, though you can enlarge or shrink it by resizing the Chart Manager window.

Reset the Zoom

To reset the zoom in the **Chart** tab of the Chart Detail dialog box, click **Reset Zoom** to refresh your view of the chart.

Resize a Chart

To resize a chart:

Step 1 Place the mouse pointer on the edge of a chart and hold the button down.

Step 2 Drag the edge of the chart downward, toward the taskbar, to expand your viewing area of the chart.

View Legend

In the **Chart** tab of the Chart Detail, page 10-24 dialog box, you can view a legend with colored squares next to each item. If you click on the colored square, the color will appear, disappear or reappear in the chart.

Raw Data Tab

To view a chart's raw data, click the **Raw Data** tab.

The table presents the same set of data as the chart, but in tabular form. The following fields are displayed in the Raw Data tab:

- Time—Allows you to view a unit of time measurement for the chart.
- Activity—Allows you to view the type of detailed activity within the chart.

Properties Tab

To view a chart's properties, click the **Properties** tab.

The Properties tab displays, showing the following properties of the chart:

- **Time Period**—Shows the start and end date of the period of time you selected in the Select Chart's Time and Mode Wizard screen. The period of time is displayed in the format defined in your user preferences (Set the Formatting of Dates and Times, page 1-32). See Select the Period of Time, page 10-8.
- **Time Division—**Shows the units of time, referred to as time divisions, that you used to divide the X-Axis into specific data points.

- **Entities**—Shows the types of entities, such as routers and routes, displayed in the chart.
- **Data Sets—**Shows the type of action displayed in the chart, for example, Activity or Flaps, as well as the data set of the action.
- **Graph Mode**—Shows the mode of the chart. For more information on chart modes, see Select the Mode, page 10-10.

Managing Charts

Once charts have been created, you can perform the following tasks with them:

- Delete a Chart, page 10-27
- Print a Chart, page 10-27
- Save a Chart, page 10-28
- Load a Chart, page 10-28
- Scheduling a Chart, page 10-29
- Picking up a Chart, page 10-29

Delete a Chart

To delete a chart:

Step 1 Select the row that contains the chart you want to delete in the table of charts in Chart Manager.

Step 2 Click the **Delete Chart** icon in the Chart Manager Toolbar, page 10-48.

Please note that you will not be asked for confirmation. Clicking the **Delete Chart** icon deletes the chart immediately.

The selected chart is removed from the list of charts in Chart Manager.

Note You can select and deselect more than one chart by using the Ctrl and Shift keys with your mouse.

Print a Chart

To print a chart:

Step 1 Click the row in the table of charts in Chart Manager that contains the chart you want to print.

Step 2 Click the **Print Chart** icon in the Chart Manager Toolbar, page 10-48.

The selected chart is sent to your system printer.

Save a Chart

To save a chart:

Step 1 Click the row in the table of charts in Chart Manager that contains the chart you want to save to a file.

Step 2 Click the **Save Chart** icon in the Chart Manager Toolbar, page 10-48.

The Choose File dialog box appears.

Step 3 Enter a name for the chart in the File Name field.

Step 4 Select a folder in which to store the chart file, then click **Save**.

Note On some systems, an **Open** icon may be displayed instead of the **Save** icon in the Choose File dialog box.

Load a Chart

To load a previously saved chart:

Step 1 Click the **Load Chart** icon in the Chart Manager Toolbar, page 10-48.

The Choose File dialog box appears.

Step 2 Locate the folder that contains the chart you want to load.

Step 3 Click **Open**.

The Choose File dialog box closes. In Chart Manager, a new entry for the chart appears in the list of charts.

Scheduling a Chart

You can schedule any chart or advanced chart to be processed in the future, either one time or on a recurring basis. For more complete information on scheduling charts, please see Scheduling Charts, page 11-9.

Picking up a Chart

To pick up a scheduled or previously-generated chart:

Step 1 Select a chart or advanced chart from the Chart Manager.

Step 2 Click **Pickup my Charts** in the Chart Manager Toolbar, page 10-48.

Your completed scheduled charts appear in the Chart Manager window.

Descriptions of Charts

The Chart Wizard provides a selection of charts you can generate, organized by type. See Select the Type of Chart to Generate, page 10-3 for an overview about the types of charts provided.

If you choose to generate a Trending chart, you can view information about trends that occur in routing changes over time. If you select to generate a Classification chart, you can view the top ten network entities that were most affected by changes in routing. If you select to generate a Distribution chart, you can view the distribution of an activity in a selected period of time. For more complete definitions of trending and classification charts, see Select the Mode of the Chart, page 10-4.

The following sections provide tables that describe information shown in each classification mode or trending mode chart. In the Chart Wizard, you first select a chart under its high-level charting category:

- Enterprise Charts, page 10-29
- Topology Charts, page 10-30
- Routing Update Charts, page 10-34
- Service Charts, page 10-41

Enterprise Charts

Table 10-1 describes each of the Enterprise charts in Trending, Distribution, Classification, and Normalized mode.

Table 10-1 Enterprise Chart Descriptions

Chart Name	Trending and Distribution Chart Description	Classification and Normalized Chart Description
Routing Activity Overview	Shows the amount of Interface, External advertisement, T3 and T4 advertisements, and BGP routing activity that occurred in your network in the selected period of time. **As a Trending Chart:** Each bar represents routing activity at each division point of the period of time. **As a Distribution Chart:** Shows the percentage of each type of activity that occurred.	**As a Classification Chart:** Shows the routers responsible for routing changes in a selected period of time. **As a Normalized Chart:** Shows T-Score values representing routing activity at a division point in a selected period of time. This is similar to what you can view in Event Monitor. For more information, see Monitoring Network Activity, page 5-1.

Topology Charts

Table 10-2 describes each of the Topology charts in Trending, Distribution, and Classification mode.

Table 10-2 Topology Chart Descriptions

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Topology Charts		
Topology Growth Overview	Shows the number of new entities—including Transit networks, Routers, Stub Routes, and External advertisements—that were added to your network in the selected period of time. **As a Trending Chart:** Each bar represents the number of entities added at each division point in the selected period of time. **As a Distribution Chart:** Shows the total distribution of new entities added to the enterprise in the selected period of time.	**As a Classification Chart:** Shows the autonomous systems or OSPF areas that had the greatest number of new entities added in the selected period of time.

Table 10-2 Topology Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Topology Contraction Overview	Shows the number of entities—including Transit networks, Routers, Stub routes, and External advertisements—that were removed from your network in the selected period of time. **As a Trending Chart:** Each bar represents the number of entities removed during each division point in the selected period of time. **As a Distribution Chart:** Shows the total distribution of entities removed from the enterprise in the selected period of time.	**As a Classification Chart:** Shows the autonomous systems or OSPF areas that had the greatest number of entities removed in the selected period of time.
BGP Charts		
BGP Route Activity	Shows the amount and type of BGP routing activity that occurred between and within autonomous systems of your network in a selected period of time. Please note that this is the same BGP Route Activity chart that appears in the Routing Updates Charts, page 10-35 section. **As a Trending Chart:** Each bar represents BGP routing activity during each division point of the selected period of time. **As a Distribution Chart:** Shows the total distribution of BGP activity by type.	**As a Classification Chart:** Shows the most active BGP routes in your network and their availability in the selected period of time.

Table 10-2 Topology Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
OSPF Charts		
OSPF Router Activity	Shows a comparison of changes that occur on your OSPF routers in the selected period of time. **As a Trending Chart:** Each bar represents the number and type of changes that occurred at each division point in the selected period of time. **As a Distribution Chart:** Shows the total distribution of routing changes in the selected period of time.	**As a Classification Chart:** Shows the number and type of changes that occurred on the most active routers in the selected period of time.
OSPF Router Flap	Shows the number of flaps that occurred on all OSPF routers in the selected period of time. **As a Trending Chart:** Each bar represents the total number of router flaps that occurred during each division point in the selected period of time. **As a Distribution Chart:** Shows the total distribution of router flaps across specific OSPF domains in the selected period of time.	**As a Classification Chart:** Shows the top routers that had the most flaps in the selected period of time.
Adjacency Activity	Shows the number of adjacency changes between routers in the selected period of time. **As a Trending Chart:** Each bar represents the number of available or unavailable adjacencies, or metric changes during each division point in the selected period of time. **As a Distribution Chart:** Shows the total distribution of changes in adjacency between routers, and metric activity, in the selected period of time.	**As a Classification Chart:** Shows the top routers that had the most adjacency changes and metric activity in the selected period of time.

Table 10-2 Topology Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Adjacency Flap	Shows the number and types of flaps between routers for Stub routes, Transit interfaces, Numbered Point-to-Point interfaces, and Unnumbered Point-to-Point interfaces in the selected period of time. **As a Trending Chart:** Each bar represents the amount of flaps on adjacencies between routers at each division point in the selected period of time. **As a Distribution Chart:** Shows the total distribution of flaps on adjacencies between routers in the selected period of time.	**As a Classification Chart:** Shows the routers that had the most adjacency flaps in the selected period of time.
Transit Network Activity	Shows the number of events that occurred in the selected period of time, affecting one or more Transit networks. **As a Trending Chart:** Each bar represents the number of events that occurred on all Transit networks in the selected period of time. **As a Distribution Chart:** Shows the total distribution of events that occurred on Transit networks in the selected period of time.	**As a Classification Chart:** Shows the Transit networks that experienced the most events, and the number of events that occurred on each Transit network, in the selected period of time.

Table 10-2 Topology Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Designated Router Activity	Shows the number of times, in the selected period of time, that the Designated Router (DR) for a Transit network changed as a result of the DR election process. **As a Trending Chart:** Each bar represents the number of times the DR changed as a result of the DR election process in the selected period of time. **As a Distribution Chart:** Shows all DR changes distributed by Transit Networks in the selected period of time.	**As a Classification Chart:** Shows the Transit networks that had the most DR changes in the selected period of time.
Stub Advertise-ment Activity	Shows the number and type of changes availability, unavailability, and metric changes to Stub routes in the selected period of time. Please note that this is the same Stub advertisement Activity chart that appears in the Routing Updates Charts, page 10-35. **As a Trending Chart:** Each bar represents the number and type of changes to Stub routes that occurred in the selected period of time. **As a Distribution Chart:** Shows the distribution of changes to Stub routes in the selected period of time.	**As a Classification Chart:** Shows the Stub routes that changed the most in the selected period of time.

Routing Update Charts

Table 10-3 describes each of the Routing Update charts in Trending, Distribution, and Classification mode.

Table 10-3 Routing Update Chart Descriptions

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Routing Updates Charts		
Routing Update Growth Overview	Shows the number of new OSPF Interfaces and external routes and BGP routes added to your network in the selected period of time. **As a Trending Chart:** Each bar represents the number of new routes at each division point in the selected period of time. **As a Distribution Chart:** Shows the distribution of new routes by type in the selected period of time.	**As a Classification Chart:** Shows the OSPF domains and AS's with the most recently advertised routes in the selected period of time.
Routing Update Contraction Overview	Shows the number of OSPF Interfaces and external prefixes and BGP routes removed from your network in the selected period of time. **As a Trending Chart:** Each bar represents the number of withdrawn routes at each division point in the selected period of time. **As a Distribution Chart:** Shows the distribution of changes by type of route in the selected period of time.	**As a Classification Chart:** Shows the OSPF domains and AS's with the most withdrawn routes in the selected period of time.

Table 10-3 Routing Update Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Routes Charts		
BGP Route Activity	Shows the amount and type of BGP routing activity that occurred between and within autonomous systems of your network in a selected period of time. Please note that this is the same BGP Route Activity chart that appears in the BGP Charts, page 10-31 section. **As a Trending Chart:** Each bar represents BGP routing activity during each division point of the selected period of time. **As a Distribution Chart:** Shows the total distribution of BGP activity by type.	**As a Classification Chart:** Shows the most active BGP routes in your network in the selected period of time.
External Route Redundancy	Shows the number of redundant external routes that were advertised in the selected period of time. **As a Trending Chart:** Each bar represents the number of redundancy changes that were detected at each division point in the selected period of time. **As a Distribution Chart:** Shows the distribution of changes to redundancy for external routes that were advertised in the selected period of time.	**As a Classification Chart:** Shows external routes which had the most redundancy changes in the selected period of time.

Table 10-3 Routing Update Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
External Route Not Reachable	Shows the number of times external routes became unreachable in the selected period of time. **As a Trending Chart:** Each bar represents the number of times external routes became unreachable in the selected period of time. **As a Distribution Chart:** Shows the distribution of unreachable external routes by OSPF domain that were detected in the selected period of time.	**As a Classification Chart:** Shows external routes that became unreachable the most number of times in the selected period of time.
Transit and Stub Redundancy	Shows the number and type of redundancy changes to Transit and Stub routes that were detected in the selected period of time. **As a Trending Chart:** Each bar represents the number of redundancy changes to Transit and Stub routes that were detected at each division point in the selected period of time. **As a Distribution Chart:** Shows the distribution by type of redundancy changes to Transit and Stub routes that were detected in the selected period of time.	**As a Classification Chart:** Shows Transit and Stub routes that had the most redundancy changes in the selected period of time.

Table 10-3 Routing Update Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Transit and Stub Not Reachable	Shows the number of times Transit and Stub routes became unreachable in the selected period of time. **As a Trending Chart:** Each bar represents the number of times Transit and Stub routes became unreachable at each division point in the selected period of time. **As a Distribution Chart:** Shows the distribution by domain of the number of Transit and Stub routes that became unreachable in a selected period of time.	**As a Classification Chart:** Shows Transit and Stub routes that became unreachable the most number of times in the selected period of time.
Route Advertisements Charts		
BGP Route Advertise-ment Activity	Shows the number of changes to BGP route advertisements, including unavailable BGP routes, available BGP routes, within autonomous systems at each division point in the selected period of time. **As a Trending Chart:** Each bar represents the number of changes to route advertisements per type of change within autonomous systems at each division point in the selected period of time. **As a Distribution Chart:** Shows the distribution by type of BGP route advertisements for each type of change advertised.	**As a Classification Chart:** Shows the areas that had the most BGP changes to availability, unavailability and community attributes in the selected period of time.

Table 10-3 Routing Update Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
External Advertisement Activity	Shows the number of availability and metric changes to external route advertisements within an AS at each division point in the selected period of time. **As a Trending Chart:** Each bar represents the number of external route advertisements per type of change broadcast to other OSPF speakers within an autonomous system at each division point in the selected period of time. **As a Distribution Chart:** Shows the distribution of external route advertisements for each type of change advertised.	**As a Classification Chart:** Shows the external route advertisements that had the most metric and availability changes on external route advertisements in the selected period of time.
External Advertisement Flap	Shows the number of external route advertisement availability flaps, defined as intermittent periods of availability and unavailability, detected within an autonomous system. **As a Trending Chart:** Each bar represents the number of availability flaps on external route advertisements in the relevant period of time. **As a Distribution Chart:** Shows the distribution by OSPF domain of all detected availability flaps on external route advertisements within the selected domains and in the selected period of time.	**As a Classification Chart:** Shows the external route advertisements that had the highest number of availability flaps in the selected period of time.

Table 10-3 Routing Update Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Stub Advertise-ment Activity	Shows the number and type of activity on Stub route advertisements in the selected period of time. Activity includes metric changes, and availability events, and unavailability events. Please note that this is the same Stub Advertisement Activity chart that appears in the OSPF Charts, page 10-32 section. **As a Trending Chart:** Each bar represents the number of Stub route advertisement events per type of change detected in the selected OSPF area. **As a Distribution Chart:** Shows the distribution of Stub route advertisement activity for each type of change advertised.	**As a Classification Chart:** Shows the Stub route advertisements that had the most metric, availability, and unavailability activity in the selected period of time.

Table 10-3 Routing Update Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
T3 and T4 Advertise-ment Activity	Shows the amount of activity on Type 3 and Type 4 Summary route advertisements during each division point in the selected period of time. Activity includes metric changes, and changes to availability and unavailability. **As a Trending Chart:** Each bar represents the amount of activity on Type 3 and Type 4 Summary route advertisements in an OSPF area. Activity includes metric changes, and changes to availability and unavailability. **As a Distribution Chart:** Shows the distribution of Stub route advertisements for each type of change advertised.	**As a Classification Chart:** Shows the Area Border Routers (ABR) that had the most T3 and T4 advertisement activity in the selected period of time. Type 3 metric changes occur on the interface of the ABR that advertises the route to a destination in another OSPF area. Type 4 metric changes occur on the interface of the ABR that advertises how to reach the ASBR that advertises an external route.
T3 and T4 Advertise-ment Flap	Shows the number of flaps detected on T3 and T4 advertisements within the selected period of time. Flaps are defined as intermittent periods of availability and unavailability. **As a Trending Chart:** Each bar represents the number of flaps detected on a Type 3 or Type 4 Summary route advertisement in a particular OSPF domain. **As a Distribution Chart:** Shows the distribution of flaps on Type 3 and Type 4 Summary route advertisements per selected domain and in the selected period of time.	**As a Classification Chart:** Shows the Area Border Routers (ABR) that had the most flaps detected on Type 3 and Type 4 Summary route advertisements in the selected period of time.

Service Charts

Table 10-4 describes each of the Service charts in Trending, Distribution, Classification, and Normalized mode.

Table 10-4 Service Chart Descriptions

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Service Charts		
Service Growth Overview	Shows the number of services and service paths added to your network in a selected period of time. **As a Trending Chart:** Each bar represents the number of services and service paths added to your network at each division point in the period of time. **As a Distribution Chart:** Shows the distribution of new services and service paths configured for, added to, and traversing across routing domains and autonomous systems of your network in the selected period of time.	**As a Classification Chart:** Shows, the total number of services and service paths added to your network in the selected period of time.
Service Contraction Overview	Shows the number of services and service paths removed from your network in a selected period of time. **As a Trending Chart:** Each bar represents the number of services and service paths removed from your network at each division point in the period of time. **As a Distribution Chart:** Shows the distribution of services and service paths removed from routing domains and autonomous systems of your network in the selected period of time.	**As a Classification Chart:** Shows the total number of services and service paths removed from your network in the selected period of time.

Table 10-4 Service Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Service Health Activity	Shows the number of changes, such as the availability or conformance of a service to its baseline, that occurred in the selected period of time. A service can be available and conformant to its baseline, available and deviant from its baseline, or unavailable. **As a Trending Chart:** Each bar represents the number of times a service changed to be available and conformant to its baseline, available and deviant to its baseline, or unavailable in the selected period of time. **As a Distribution Chart:** Shows the distribution of changes to services showing how frequently services become available and conformant to their baseline, available and deviant to their baseline, or unavailable in routing domains and autonomous systems of your network.	**As a Classification Chart:** Shows, by name, the services that experienced the most changes in availability or conformance in the selected period of time.

Table 10-4 Service Chart Descriptions (continued)

Chart Name	Trending and Distribution Chart Description	Classification Chart Description
Service Path Health Activity	Shows the number of changes, such as the availability or conformance of a service path to its baseline, that occurred in the selected period of time. A service path can be available and conformant to its baseline, available and deviant from its baseline, or unavailable. **As a Trending Chart:** Each bar represents the number of times a service path changed to be available and conformant to its baseline, available and deviant to its baseline, or unavailable in a selected period of time. **As a Distribution Chart:** Shows the distribution of changes to service paths showing how frequently service paths become available and conformant to their baseline, available and deviant to their baseline, or unavailable in routing domains and autonomous systems of your network.	**As a Classification Chart:** Shows, by name, the service paths that experienced the most changes in availability or conformance in the selected period of time.

Descriptions of Advanced Charting Charts

Clicking the **Create Advanced Chart** icon provides a selection of charts to generate, organized by category, data set and entity. See Generating an Advanced Chart, page 10-11 for information about how to generate an advanced chart in Chart Manager.

Chart Types Associated with Data Sets

Table 10-5 Chart Type Descriptions

Chart	Description
Activity	Measures the amount of change to a network entity or the entire network. Encompasses all types of change, including stability, availability, reachability, redundancy, loss, and growth. Activity level is determined by the number of events generated and stored by the system.
Availability	Measures the presence or readiness of a network device component, such as an interface, link, network, service, or other network element. In the Path Analyzer Tabular Map, availability is indicated by an Up status; in the Graphical Map, availability is indicated by the color of a map element. For example, blue routers and green links are available. **Tracking Mode**—You can select Tracking Mode for specific entities associated with Availability chart.
Reachability	The availability of something within a certain scope. An enterprise network is a hierarchy of connected AS's, domains, and areas. Routing updates flow through the hierarchy creating a connected fabric of routeable network addresses. Reachability is the term used to describe the accessibility of an address within a specific scope of the network. **Tracking Mode**—You can select Tracking Mode for specific entities associated with Reachability chart.
Redundancy	Measures the number of ways to reach a network device or appliance. Exists when one appliance can reach another over more than one path. For example, a service path is redundant if its multiple segments, or branches, provide more than one distinct way of getting from the source to the destination. A prefix is redundant if more than one router advertises a route for it. Redundancy is not defined for route advertisements. **Tracking Mode**—You can select Tracking Mode for specific entities associated with Redundancy chart.
Growth	Number of new and purged routeable IP addresses in the network. Growth includes addresses of routers, interfaces, external prefixes, subnets, and other addressable components of the network.

Table 10-5 Chart Type Descriptions (continued)

Chart	Description
Baseline Conformity	Measures the degree to which a service and its service paths conform to an engineered baseline. Conformance is a binary state calculated as the Boolean AND of the conformance of all service paths associated with a service. A service is considered to be non-conforming when any of its associated service paths deviates from the set baseline. **Tracking Mode**—You can select Tracking Mode for specific entities associated with Baseline Conformity chart.
Service Health	Shows the number of changes, such as the availability or conformance of a service to its baseline, that occurred in the selected period of time. A service can be available and conformant to its baseline, available and deviant from its baseline, or unavailable. **Tracking Mode**—You can select Tracking Mode for specific entities associated with Service Health chart.

Select Entities

Table 10-6 describes the entities that you can select to run with the Chart Wizard.

Table 10-6 Entity Descriptions for Advanced Charting

Chart	Entity	Description
Topology Chart		
	Router	Network device or software that determines the next node to forward a packet toward its destination. Returns data about selected routers in your network.
	Transit Network	Returns data about selected routers that connect to a Transit network.
	Stub Advertisement	Returns data about the route to a destination in a Stub network.

Table 10-6 Entity Descriptions for Advanced Charting (continued)

Chart	Entity	Description
Adjacency Chart		
	Unnumbered Point-to-Point Interface	Returns data about the connection between two routers on an OSPF network. Routers exchange hello packets and establish adjacencies over numbered interfaces that are identified by unnumbered interfaces, which are identified by Management Information Base (MIB) addresses.
	Numbered Point-to-Point Interface	Returns data about the connection between two routers on an OSPF network. Routers exchange hello packets and establish adjacencies over numbered interfaces, which are identified by IP addresses.
	Transit Interface	Returns data about the router interface that connects to a Transit network.
Routing Updates Chart		
Routes Chart		
	Transit and Stub Route	Returns data about the route to a destination in a Transit or Stub network.
	External Route	Returns data about the route to a destination in an autonomous system outside of the local area. Advertised by an Autonomous System Boundary Router (ASBR) via Open Shortest Path First (OSPF).
	BGP Route	Returns data about the route to a BGP speaker.
Route Advertisements		
	T3 Summary	Returns data about the route to a destination in another OSPF area. ABRs advertise Type 3 Summary Link State Advertisements (LSAs) in their local area to announce how to reach destinations in another area.

Table 10-6 Entity Descriptions for Advanced Charting (continued)

Chart	Entity	Description
	T4 Summary	Returns data about the route to an ASBR in another OSPF area. ABRs advertise Type 4 Summary LSAs in their local area to announce how to reach an ASBR in another area.
Route Advertisements (continued)		
	External Advertisement	Returns data about the route to a destination in another autonomous system. ASBRs advertise Type 5 LSAs via Open Shortest Path First (OSPF), which announce how to reach destinations in other autonomous systems.
	BGP Advertisement	Returns data about the route to a Border Gateway Protocol (BGP) router.
Services Chart		
	Service	Returns data about selected Path Analyzer services. In Path Analyzer terminology, a service is a collection of paths that are critical to the reliability, stability, and availability of the application.
	Service Path	Returns data about selected Path Analyzer service paths, the business-critical paths of a service.

Related Forms

This section contains tables that detail graphical elements and dialog boxes in the Chart Manager.

Chart Manager Toolbar

Table 10-7 describes the buttons of the Chart Manager Toolbar, page 10-48.

Table 10-7 Chart Manager Toolbar Buttons

Button	Description
Create New Chart 	Starts the Chart Wizard, in which you can select and create a basic chart.
Create Advanced Chart 	Starts the Chart Wizard in advanced mode. This allows you to create an advanced chart through wizard screens.
Derive Chart 	Allows you to select the data sets associated with specific chart types using the Chart Wizard in advanced mode.
View Chart 	Opens a chart after you select its thumbnail from the list in the Chart Manager Toolbar, page 10-48.
Cancel Chart 	Cancels the creation of a chart.
Delete Chart 	Deletes a selected chart.
Print Chart 	Prints a selected chart.
Save Chart 	Saves a chart to a selected location.
Load Chart 	Loads a saved chart in the Chart Manager window.

Table 10-7 Chart Manager Toolbar Buttons (continued)

Button	Description
Schedule Chart 	Allows you to schedule a chart or an advanced chart.
Pick Up My Charts 	Allows you to pick up your scheduled chart or advanced chart.

Chart Wizard Pages for Advanced Charting

Clicking the **Create Advanced Chart** button in the Chart Manager Toolbar, page 10-48 starts the Chart Wizard for Advanced Charts. The Chart Wizard consists of pages that guide you through the steps for creating an Advanced Chart. The number of wizard pages depend upon the entities you select.

Table 10-8 describes wizard pages of the Chart Wizard for Advanced Charting. See the Generating an Advanced Chart, page 10-11 for more information.

Table 10-8 Advanced Charting Wizard Pages

Wizard Screen	Description
Select Data Set, page 10-12	Allows you to create an advanced chart from data sets listed in the Chart Wizard. This is the first screen of the Chart Wizard for advanced charts.
Select Entities, page 10-14	Allows you to select entities listed in the Chart Wizard. This is the second screen of the Chart Wizard for advanced charts. Later pages in the wizard depend upon the data set and entities you select.
Select an Autonomous System and Domain, page 10-15	Allows you to select at least one autonomous system that you want to associate with the chart. This is the third screen of the Chart Wizard for advanced charts.
Choose Entities for Routers, page 10-53	Allows you to choose if you want to select all entities or specific entities for routers. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for Routers, page 10-54	Allows you to select specific entities for routers on your network.
Choose Entities for Transit Network, page 10-54	Allows you to choose if you want to select all entities or specific entities for Transit nodes, including Area ID and Route ID. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for Transit Networks, page 10-55	Allows you to select specific entities for Transit nodes on your network.

Table 10-8 Advanced Charting Wizard Pages (continued)

Wizard Screen	Description
Choose Entities for Stub Routes, page 10-55	Allows you to choose if you want to select all entities or specific entities for Stub routes, including Area ID, Route ID, and Router Name. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for Stub Routes, page 10-56	Allows you to select specific entities for Stub routes on your network.
Choose Entities for Unnumbered Point-to-Point Interfaces, page 10-56	Allows you to choose if you want to select all entities or specific entities for Unnumbered Point-to-Point interfaces, including Area ID, Router Name, Connected/Attached Router, and MIB Index, Router Name, Connected/Attached Router, and MIB Index. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for Unnumbered Point-to-Point Interfaces, page 10-57	Allows you to select specific entities for Unnumbered Point-to-Point interfaces on your network.
Choose Entities for Numbered Point-to-Point Interfaces, page 10-58	Allows you to choose if you want to select all entities or specific entities for numbered point-to-point interfaces. Includes Area ID, Router Name, Connected/Attached Router, and MIB Index. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to Be Included for Numbered Point-to-Point Interfaces, page 10-58	Allows you to select specific entities for numbered point-to-point interfaces on your network.
Choose Entities for Transit Interface, page 10-59	Allows you to choose if you want to select all entities or specific entities for Transit interfaces. Includes Area ID, Router Name, and Interface. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for Transit Interface, page 10-60	Allows you to select specific entities for Transit interfaces on your network.
Choose Entities for Transit and Stub Route, page 10-60	Allows you to choose if you want to select all entities or specific entities for Transit and Stub routes. Includes Route ID. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for Transit and Stub Route, page 10-60	Allows you to select specific entities for Transit and Stub routes on your network.
Choose Entities for External Route, page 10-61	Allows you to choose if you want to select all entities or specific entities for external routes. Includes Route ID. This wizard screen depends upon the data sets and entities you previously selected.

Table 10-8 Advanced Charting Wizard Pages (continued)

Wizard Screen	Description
Entity Types to be Included for External Route, page 10-61	Allows you to select specific entities for external routes on your network.
Choose Entities for BGP Route, page 10-62	Allows you to choose if you want to select all entities or specific entities for BGP routes. Includes Route ID. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for BGP Route, page 10-62	Allows you to select specific entities for BGP routes on your network.
Choose Entities for T3 Summary, page 10-63	Allows you to choose if you want to select all entities or specific entities for T3 summary advertisements. Includes Area ID, Route Name, and Route ID. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for T3 Summary, page 10-63	Allows you to select specific entities for T3 summary advertisements on your network.
Choose Entities for T4 Summary, page 10-64	Allows you to choose if you want to select all entities or specific entities for T4 summary advertisements. Includes Area ID, Route Name, and Asbr Name. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for T4 Summary, page 10-65	Allows you to select specific entities for T4 summary advertisements on your network.
Choose Entities for External Advertisement, page 10-65	Allows you to choose if you want to select all entities or specific entities for Type 5 external advertisements. Includes Area ID, Router Name, and Route ID. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for External Advertisement, page 10-66	Allows you to select specific entities for Type 5 external advertisements on your network.
Choose Entities for BGP Route Advertisement, page 10-66	Allows you to choose if you want to select all entities or specific entities for BGP route advertisements. Includes Route ID, Router Name, and Prefix Length. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for BGP Route Advertisement, page 10-67	Allows you to select specific entities for BGP route advertisements on your network.

Table 10-8 Advanced Charting Wizard Pages (continued)

Wizard Screen	Description
Choose Entities for Service, page 10-68	Allows you to choose if you want to select all entities or specific entities for service. Includes Service Name. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for Service, page 10-68	Allows you to select specific entities for services on your network.
Choose Entities for Service Path, page 10-68	Allows you to choose if you want to select all entities or specific entities for service paths. Includes Service Name and Service Path Name. This wizard screen depends upon the data sets and entities you previously selected.
Entity Types to be Included for Service Path, page 10-69	Allows you to select specific entities for service paths on your network.
Select the Time Period, page 10-17	Allows you to select the time period of the chart that you want to associate with the chart. From this screen, you can select a predefined time or customize a time period.
Select the Name, Mode, and Type of Chart, page 10-18	Allows you to enter the name and select the mode and type of chart.
Select the Time Divisions of a Trending Chart, page 10-20	Allows you to select the time division for the chart if you previously selected Trending mode.
Select the Aggregators and Entities of a Classification Chart, page 10-21	Allows you to select the aggregate attribute value, if you previously selected Classification mode, as well as the number of entities to view on the chart.
Preview the Chart, page 10-22	Allows you to preview the chart before generating it.
Finish the Wizard	Allows you to view the status of the chart you wish to generate. The Chart Manager window indicates the status of the report as it is generated. This is the last screen of the Chart Wizard for advanced charts.

Choose Entities for Routers

In the Choose Entities for Routers screen, you can choose specific entities for routers or you can choose all entities for routers.

Table 10-9 describes the generic fields and buttons of the Choose Entities for Routers screen.

Table 10-9 Choose Entities for Routers

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific routers in your network. If you choose this radio button, you can select which routers you want to include for your chart in the following screens.
Router Name (text box)	Enter the IP address of the router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for Routers

In the Entity Types to be Included for Routers screen, you can choose specific entities for routers from the table.

Table 10-10 describes the generic fields and buttons of the Choose Entities for Routers screen.

Table 10-10 Entity Types to be Included for Routers

Field	Description
Check Box	Select this check box next to the specific router or routers you wish to include in the chart.
Router Name (field)	The IP address of the specific router or routers present on your network that you may wish to include in the chart.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for Transit Network

In the Choose Entities for Transit Network screen, you can choose specific entities for Transit networks, or you can choose all entities for Transit networks to include in your chart.

Table 10-11 describes the generic fields and buttons of the Choose Entities for Transit Networks screen.

Table 10-11 Choose Entities for Transit Nodes

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific Transit nodes in your network. If you choose this radio button, you can select which Transit nodes you want to include for your chart in the following screens.

Table 10-11 Choose Entities for Transit Nodes (continued)

Field	Description
Area ID (text box)	Enter the IP address of the area that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Route ID (text box)	Enter the IP address of the route ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for Transit Networks

In the Entity Types to be Included for Transit Networks screen, you can choose specific entities for Transit networks from the table.

Table 10-12 describes the generic fields and buttons of the Choose Entities for Transit Networks screen.

Table 10-12 Entity Types to Be Included for Transit Nodes

Field	Description
Check Box	Select this check box next to the specific Transit nodes or Transit networks you wish to include in the chart.
Transit Node (field)	The IP address of the specific Transit node present on your network that you may wish to include in the chart.
Area (field)	The IP address of the area where the Transit node is located.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for Stub Routes

In the Choose Entities for Stub Routes screen, you can choose specific entities for Stub routes, or you can choose all entities for Stub routes to include in your chart.

Table 10-13 describes the generic fields and buttons of the Choose Entities for Stub Routes screen.

Table 10-13 Choose Entities for Stub Routes

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific Stub routes in your network. If you choose this radio button, you can select which Stub interfaces you want to include for your chart in the following screens.

Table 10-13 Choose Entities for Stub Routes (continued)

Field	Description
Area ID (text box)	Enter the IP address of the area that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Route Name (text box)	Enter the IP address/subnet mask of the route ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Router Name (text box)	Enter the IP address of the router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for Stub Routes

In the Entity Types to Be Included for Stub Routes screen, you can choose specific entities for Stub routes.

Table 10-14 describes the generic fields and buttons of the Choose Entities for Stub Routes screen.

Table 10-14 Entity Types to be Included for Stub Routes

Field	Description
Check Box	Select this check box next to the specific Stub routes you wish to include in the chart.
Stub Route (field)	The IP address of the specific Stub route present on your network that you may wish to include in the chart.
Connected Router Name (field)	The IP address of the connected router.
Area (field)	The IP address of the area where the Transit network or Transit networks is located.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for Unnumbered Point-to-Point Interfaces

In the Choose Entities for Unnumbered Point-to-Point Interfaces screen, you can choose specific entities for Unnumbered Point-to-Point interfaces, or you can choose all entities for Unnumbered Point-to-Point interfaces to include in your chart.

Table 10-15 describes the generic fields and buttons of the Choose Entities for Unnumbered Point-to-Point Interfaces screen.

Table 10-15 Choose Entities for UP2P Interfaces

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific Unnumbered Point-to-Point interfaces in your network. If you choose this radio button, you can select which Unnumbered Point-to-Point interfaces you want to include for your chart in the following screens.
Area ID (text box)	Enter the IP address of the area that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Router Name (text box)	Enter the IP address of the router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Connected/Attached Router (text box)	Enter the IP address of the connected/attached router that you want to include in the chart. You can enter * for a wildcard, though you cannot use a wildcard in conjunction with a string.
MIB Index (text box)	Enter the MIB Index number that you want to include in the chart. You can enter * for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for Unnumbered Point-to-Point Interfaces

In the Entity Types to be Included for Unnumbered Point-to-Point Interfaces screen, you can choose specific entities for Unnumbered Point-to-Point interfaces from the table.

Table 10-16 describes the generic fields and buttons of the Choose Entities for Unnumbered Point-to-Point Interfaces screen.

Table 10-16 Entity Types to be Included for UP2P Interfaces

Field	Description
Check Box	Select this check box next to the specific Unnumbered Point-to-Point interface or interfaces you wish to include in the chart.
Router Name (field)	The IP address of the specific router present on your network that you may wish to include in the chart.
Connected Router Name (field)	The IP address of the connected router.
Area (field)	The IP address of the area where the Transit network or Transit networks is located.

Table 10-16 Entity Types to be Included for UP2P Interfaces (continued)

Field	Description
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for Numbered Point-to-Point Interfaces

In the Choose Entities for Numbered Point-to-Point Interfaces screen, you can choose specific entities for numbered point-to-point interfaces or you can choose all entities for numbered point-to-point interfaces to include in your chart.

Table 10-17 describes the generic fields and buttons of the Choose Entities for Numbered Point-to-Point Interfaces screen.

Table 10-17 Choose Entities for NP2P Interfaces

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific numbered point-to-point interfaces in your network. If you choose this radio button, you can select which numbered point-to-point interfaces you want to include for your chart in the following screens.
Area ID (text box)	Enter the IP address of the area that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Router Name (text box)	Enter the IP address of the router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Interface (text box)	Enter the IP of the interface that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Connected/Attached Router (text box)	Enter the IP address of the connected/attached router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to Be Included for Numbered Point-to-Point Interfaces

In the Entity Types to Be Included for Numbered Point-to-Point Interfaces screen, you can choose specific entities for numbered point-to-point interfaces from the table.

Table 10-18 describes the generic fields and buttons of the Choose Entities for Numbered Point-to-Point Interfaces screen.

Table 10-18 Entity Types to Be Included for NP2P Interfaces

Field	Description
Check Box	Select this check box next to the specific numbered point-to-point interface or interfaces you wish to include in the chart.
Router Name (field)	The IP address of the specific router present on your network that you may wish to include in the chart.
Connected Router Name (field)	The IP address of the connected router.
Interface (field)	The IP address of the interface.
Area (field)	The IP address of the area where the Transit network or Transit networks is located.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for Transit Interface

In the Choose Entities for Transit Interface screen, you can choose specific entities for Transit interfaces or you can choose all entities for Transit interfaces to include in your chart.

Table 10-19 describes the generic fields and buttons of the Choose Entities for Transit Interface screen.

Table 10-19 Choose Entities for Transit Interface

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific Transit interfaces in your network. If you choose this radio button, you can select which Transit interfaces you want to include for your chart in the following screens.
Area ID (text box)	Enter the IP address of the area that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Router Name (text box)	Enter the IP address of the router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Interface (text box)	Enter the IP address of the Interface that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for Transit Interface

In the Entity Types to be Included for Transit Interface screen, you can choose specific entities for Transit interfaces from the table.

Table 10-20 describes the generic fields and buttons of the Choose Entities for Transit Interface screen.

Table 10-20 Entity Types to be Included for Transit Interface

Field	Description
Check Box	Select this check box next to the specific Transit interface or interfaces you wish to include in the chart.
Router Name (field)	The IP address of the specific router present on your network that you may wish to include in the chart.
Interface (field)	The IP address of the interface.
Area (field)	The IP address of the area where the Transit network is located.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for Transit and Stub Route

In the Choose Entities for Transit and Stub Route screen, you can choose specific entities for Transit and Stub routes or you can choose all entities for Transit and Stub routes to include in your chart.

Table 10-21 describes the generic fields and buttons of the Choose Entities for Transit and Stub Route screen.

Table 10-21 Choose Entities for Transit and Stub Route

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific Transit and Stub routes in your network. If you choose this radio button, you can select which OSPF Interface Routes you want to include for your chart in the following screens.
Route ID (text box)	Enter the IP address and subnet mask of the route ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for Transit and Stub Route

In the Entity Types to be Included for Transit and Stub Route screen, you can choose specific entities for Transit and Stub routes from the table.

Table 10-22 describes the generic fields and buttons of the Choose Entities for Transit and Stub Route screen.

Table 10-22 Entity Types to be Included for Transit and Stub Route

Field	Description
Check Box	Select this check box next to the specific Transit and Stub routes you wish to include in the chart.
Transit and Stub Route (field)	The IP address and subnet mask of the specific Transit and Stub routes present on your network that you may wish to include in the chart.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for External Route

In the Choose Entities for External Route screen, you can choose specific entities for external routes or you can choose all entities for external routes to include in your chart.

Table 10-23 describes the generic fields and buttons of the Choose Entities for External Route screen.

Table 10-23 Choose Entities for External Route

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific external routes in your network. If you choose this radio button, you can select which external routes you want to include for your chart in the following screens.
Route ID (text box)	Enter the IP address and subnet mask of the route that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for External Route

In the Entity Types to be Included for External Route screen, you can choose specific entities for external routes from the table.

Table 10-24 describes the generic fields and buttons of the Choose Entities for External Route screen.

Table 10-24 Entity Types to be Included for External Route

Field	Description
Check Box	Select this check box next to the specific OSPF External Prefixes you wish to include in the chart.
External Route (field)	The IP address and subnet mask of the external route present on your network that you may wish to include in the chart.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for BGP Route

In the Choose Entities for BGP Route screen, you can choose specific entities for BGP routes or you can choose all entities for BGP routes to include in your chart.

Table 10-25 describes the generic fields and buttons of the Choose Entities for BGP Route screen.

Table 10-25 Choose Entities for BGP Route

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific BGP routes in your network. If you choose this radio button, you can select which BGP routes you want to include for your chart in the following screens.
Route ID (text box)	Enter the IP address/subnet mask of the route ID that you want to include in the chart. You can enter an asterisk(*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for BGP Route

In the Entity Types to be Included for BGP Route screen, you can choose specific entities for BGP routes from the table.

Table 10-26 describes the generic fields and buttons of the Choose Entities for BGP Route screen.

Table 10-26 Entity Types to be Included for BGP Routes

Field	Description
Check Box	Select this check box next to the specific BGP route you wish to include in the chart.
BGP Route (field)	The IP address and subnet mask of the BGP route on your network that you may wish to include in the chart.

Table 10-26 Entity Types to be Included for BGP Routes (continued)

Field	Description
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for T3 Summary

In the Choose Entities for T3 Summary screen, you can choose specific entities for T3 summary advertisements or you can choose all entities for T3 summary advertisements to include in your chart.

Table 10-27 describes the generic fields and buttons of the Choose Entities for T3 Summary screen.

Table 10-27 Choose Entities for T3 Summary

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific T3 summary advertisements in your network. If you choose this radio button, you can select which T3 summary advertisements you want to include for your chart in the following screens.
Area ID (text box)	Enter the IP address of the area ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Router Name (text box)	Enter the IP address of the router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Route ID (text box)	Enter the IP address/subnet mask of the route ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for T3 Summary

In the Entity Types to be Included for T3 Summary screen, you can choose specific entities for T3 summary advertisements from the table.

Table 10-28 describes the generic fields and buttons of the Choose Entities for T3 Summary screen.

Table 10-28 Entity Types to be Included for T3 Summary

Field	Description
Check Box	Select this check box next to the specific T3 summary advertisements or interfaces you wish to include in the chart.
T3 Summary (field)	The IP address and subnet mask of the T3 summary advertisement on your network that you may wish to include in the chart.
Advertising Router (field)	The IP address of the advertising router.
Area (field)	The IP address of the area where the T3 summary advertisement is located.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for T4 Summary

In the Choose Entities for T4 Summary screen, you can choose specific entities for T4 summary advertisements or you can choose all entities for T4 summary advertisements to include in your chart.

Table 10-29 describes the generic fields and buttons of the Choose Entities for T4 Summary screen.

Table 10-29 Choose Entities for T4 Summary

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates.
Choose Specific Entities (radio button)	Returns a list of specific T4 summary advertisements in your network. If you choose this radio button, you can select which T4 summary advertisements you want to include for your chart in the following screens.
Area ID (text box)	Enter the IP address of the area ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Router Name (text box)	Enter the IP address of the router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Asbr ID (text box)	Enter the IP address of the ASBR ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for T4 Summary

In the Entity Types to be Included for T4 Summary screen, you can choose specific entities for T4 Summary advertisements from the table.

Table 10-30 describes the generic fields and buttons of the Choose Entities for T4 Summary screen.

Table 10-30 Entity Types to be Included for T4 Summary

Field	Description
Check Box	Select this check box next to the specific T4 summary advertisements you wish to include in the chart.
T4 Summary ASBR (field)	The IP address of the T4 summary ASBR on your network that you may wish to include in the chart.
Advertising Router (field)	The IP address of the advertising router.
Area (field)	The IP address of the area where the T4 summary route is located.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for External Advertisement

In the Choose Entities for External Advertisement screen, you can choose specific entities for an external advertisements or you can choose all entities for external advertisements to include in your chart.

Table 10-31 describes the generic fields and buttons of the Choose Entities for External Advertisement screen.

Table 10-31 Choose Entities for External Advertisement

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific external advertisements in your network. If you choose this radio button, you can select which external advertisements you want to include for your chart in the following screens.
Area ID (text box)	Enter the IP address of the area ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Table 10-31 Choose Entities for External Advertisement (continued)

Field	Description
Router Name (text box)	Enter the IP address of the router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Route ID (text box)	Enter the IP address/subnet mask of the route ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for External Advertisement

In the Entity Types to be Included for External Advertisement screen, you can choose specific entities for external advertisements from the table.

Table 10-32 describes the generic fields and buttons of the Choose Entities for External Advertisement screen.

Table 10-32 Entity Types to be Included for External Advertisement

Field	Description
Check Box	Select this check box next to the specific external interfaces you wish to include in the chart.
External Advertisement (field)	The IP address of the external advertisement on your network that you may wish to include in the chart.
Advertising Router (field)	The IP address of the advertising router.
Area (field)	The IP address of the area where the external interface is located.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for BGP Route Advertisement

In the Choose Entities for BGP Route Advertisement screen, you can choose specific entities for BGP route advertisements or you can choose all entities for BGP route advertisements to include in your chart.

Table 10-33 describes the generic fields and buttons of the Choose Entities for BGP Route Advertisement screen.

Table 10-33 Choose Entities for BGP Route Advertisement

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific BGP route advertisements in your network. If you choose this radio button, you can select which BGP route advertisements you want to include for your chart in the following screens.
Route ID (text box)	Enter the IP address/subnet mask of the route ID that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Router Name (text box)	Enter the IP address of the router that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Prefix Length (text box)	Enter the prefix length number in the Prefix Length field that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for BGP Route Advertisement

In the Entity Types to be Included for BGP Route Advertisement screen, you can choose specific entities for BGP route advertisements from the table.

Table 10-34 describes the generic fields and buttons of the Choose Entities for BGP Route Advertisement screen.

Table 10-34 Entity Types to be Included for BGP Route Advertisement

Field	Description
Check Box	Select this check box next to the specific external interfaces you wish to include in the chart.
BGP Route Advertisement (field)	The IP address and subnet mask of the BGP route advertisement on your network that you may wish to include in the chart.
Router Name (field)	The IP address of the route.
Prefix Length (field)	The numerical value of the prefix length associated with the BGP route advertisement.
Domain (field)	The domain where the entity is located.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for Service

In the Choose Entities for Service screen, you can choose specific entities for services or you can choose all entities for services to include in your chart.

Table 10-35 describes the generic fields and buttons of the Choose Entities for Services screen.

Table 10-35 Choose Entities for Services

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific Services in your network. If you choose this radio button, you can select which services you want to include for your chart in the following screens.
Service Name (text box)	Enter the name of the service in the Service Name text box that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for Service

In the Entity Types to be Included for Service screen, you can choose specific entities for Services from the table.

Table 10-36 describes the generic fields and buttons of the Choose Entities for Services screen.

Table 10-36 Entity Types to be Included for Services

Field	Description
Check Box	Select this check box next to the service you wish to include in the chart.
Service (field)	Shows the service name.
Select all Entities (button)	Click this button to include all entities in the chart.

Choose Entities for Service Path

In the Choose Entities for Service Path screen, you can choose specific entities for service paths or you can choose all entities for service paths to include in your chart.

Table 10-37 describes the generic fields and buttons of the Choose Entities for Service Path screen.

Table 10-37 Choose Entities for Service Path

Field	Description
Choose All Existing Entities (radio button)	Returns a list of all entities of a given type in the chart and aggregates them.
Choose Specific Entities (radio button)	Returns a list of specific service paths in your network. If you choose this radio button, you can select which service paths you want to include for your chart in the following screens.
Service Name (text box)	Enter the name of the service in the Service Name text box that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.
Service Path Name (text box)	Enter the name of the service path in the Service Path Name text box that you want to include in the chart. You can enter an asterisk (*) for a wildcard, though you cannot use a wildcard in conjunction with a string.

Entity Types to be Included for Service Path

In the Entity Types to be Included for Service Path screen, you can choose specific entities for service paths from the table.

Table 10-38 describes the generic fields and buttons of the Choose Entities for Service Path screen.

Table 10-38 Entity Types to be Included for Service Path

Field	Description
Check Box	Select this check box next to the service path you wish to include in the chart.
Service Path (field)	Shows the service path name.
Service (field)	Shows the service name.
Select all Entities (button)	Click this button to include all entities in the chart.

CHAPTER 11

Scheduling Reports and Charts

Managing Scheduled Tasks with Path Analyzer Schedule Manager

Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) Schedule Manager allows you to manage schedules and tasks for reports, charts, and advanced charts.

- "Scheduling" means setting up a date and time to generate a report, chart, or advanced chart.
- A "task" is the frequency you run a report, chart, or advanced chart.
- Once a report, chart, or advanced chart is generated, it can be sent to the Report Manager or Chart Manager for viewing ("picked up").

  The Schedule Manager allows you to set up a single schedule that is used to identify those reports and charts that should be run recurrently, over a selected period of time. For example, you can schedule a task to run a weekly report.

Use the Schedule Manager to create schedules for the charts and reports that you generate using Chart Manager and Report Manager.

The Schedule Manager stores charts and reports in the Path Analyzer database to guarantee their availability.

Schedule Manager Tasks

- Starting Schedule Manager, page 11-2
- Scheduling Reports, page 11-2
- Scheduling Charts, page 11-9
- Scheduling Advanced Charts, page 11-17
- Managing Scheduled Reports, Charts, and Advanced Charts, page 11-32

Schedule Manager Details

- Related Forms, page 11-42

Starting Schedule Manager

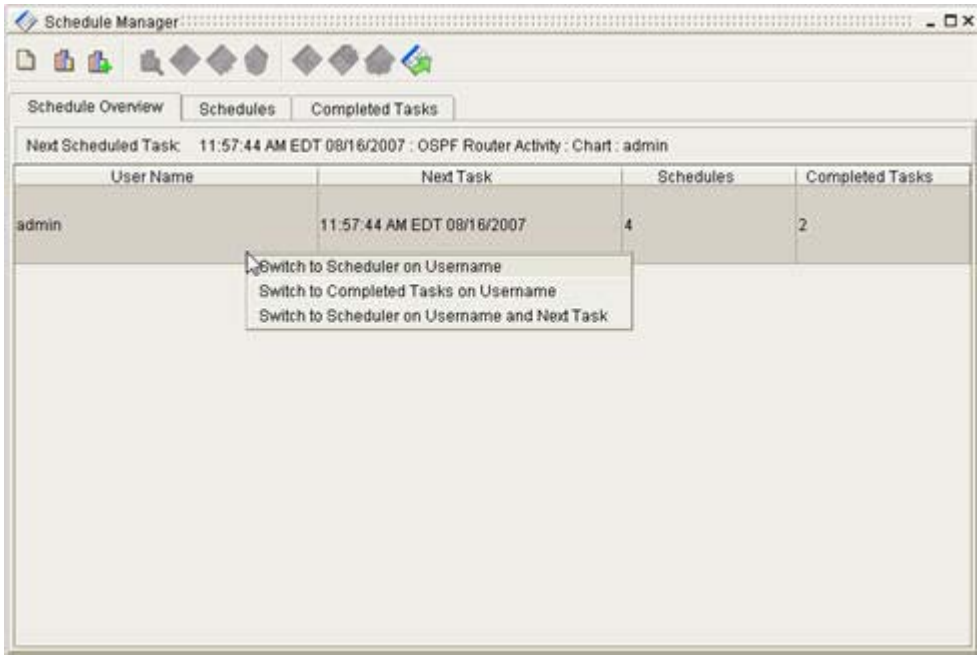
If you want to schedule reports and charts to run in the future, or recurrently, you must start the Schedule Manager.

Start Schedule Manager

To start the Schedule Manager, click **Start > Schedule Manager**.

The Schedule Manager window opens in the Path Analyzer Management Console (see Figure 11-1).

Figure 11-1 Schedule Manager



Scheduling Reports

With Path Analyzer Schedule Manager, you can generate and schedule one-time and recurring reports.

Schedule One-Time Reports

When you create a task in Schedule Manager, you select the date you want to run a report and the number of times you want to run it. One-time reports are scheduled to run once.

Reports created with Schedule Manager can be picked up (viewed) once or multiple times. For more information, see Pick Up Completed Task, page 11-42.

Start the Schedule Report Wizard

To start the Schedule Report wizard:

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager window appears.

Step 2 Click the **Schedule New Report** icon in the Schedule Manager Toolbar, page 11-42.

The Schedule Report wizard opens. If it is the first time you are scheduling a report during this session, the Report Wizard Welcome Screen appears. You can choose to view the Welcome Screen only once by selecting the **Do not show this screen again** check box.

Step 3 Click **Next**.

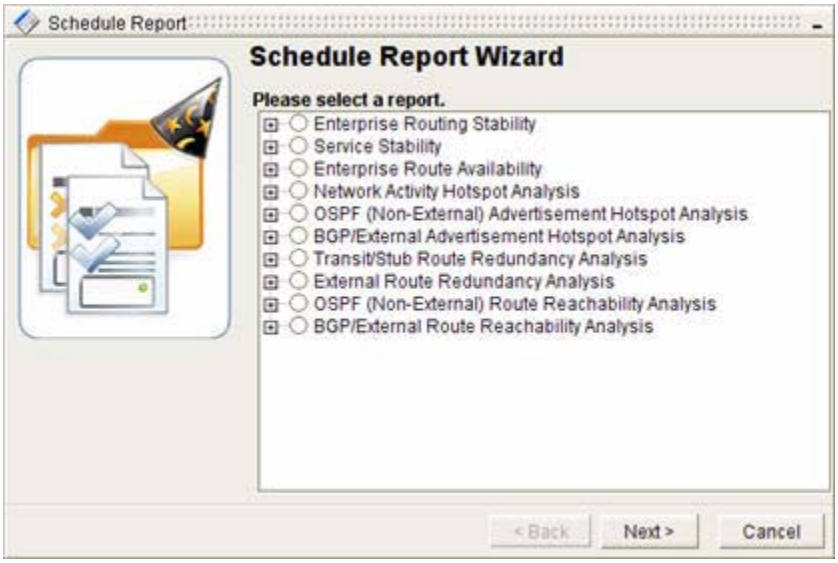
The Select a Report wizard screen appears.

Select a Report

To select a report in the Schedule wizard (see Figure 11-2):

Step 1 Select a report in the Select a Report screen by clicking its radio button.

Figure 11-2 Select a Report Screen in Schedule Report Wizard



Step 2 Click **Next**.

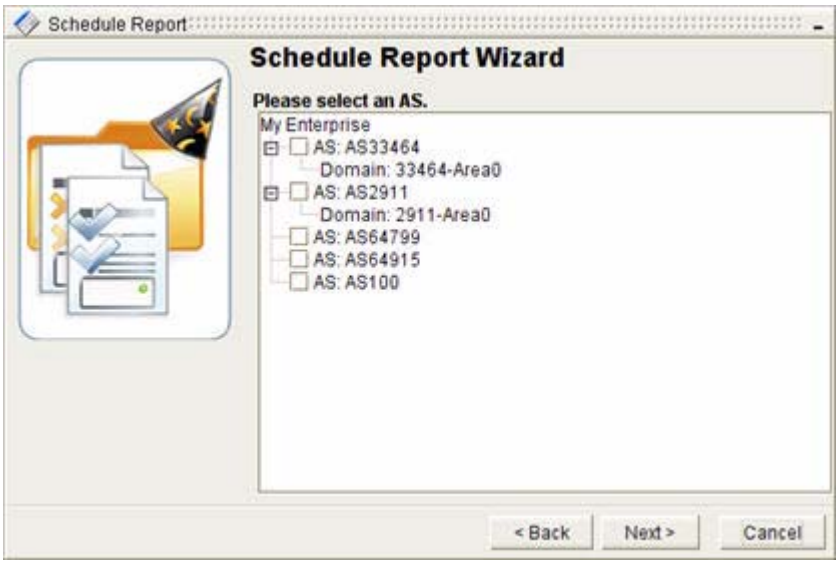
The Select an AS wizard screen appears.

Select an Autonomous System

To select an autonomous system in the Schedule wizard:

Step 1 Select one or more autonomous systems in the Select an AS screen (see Figure 11-3).

Figure 11-3 Select an AS Screen in Schedule Report Wizard



Step 2 Click **Next**.

The Select Time Period wizard screen appears. Use this screen to select the time period the report should cover.

Select Time Period

To select a time period in the Schedule wizard:

Step 1 Select one of the following in the Select Time Period wizard screen (see Figure 11-4):

- **Current Day**—Covers from midnight to the time the report is run.
- **Full Day**—Covers the 24 hours prior to the time the report is run.
- **Current Week**—Covers from Sunday at midnight to the time the report is run.
- **Full Week**—Covers the seven days prior to the time the report is run.
- **Current Month**—Covers from the first of the month to the time the report is run.
- **Full Month**—Covers one month prior to the time the report is run.
- **Full Year**—Covers from the first of the year to the time the report is run.
- **Complete History**—Covers from the last database purge to the time the report is run.

Figure 11-4 Select a Time Period Screen in Schedule Reports Wizard

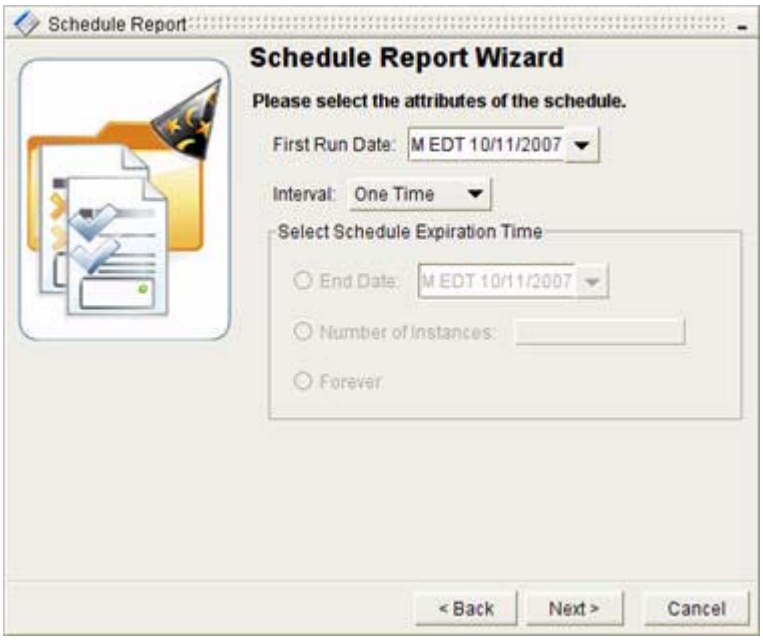
Step 2 Click **Next**.

The Select Schedule Attributes wizard screen appears.

Select Schedule Attributes

From the Select Schedule Attributes wizard screen, you can select the run date, frequency, and end date of the task.

Figure 11-5 Select Schedule Attributes Screen in Schedule Report Wizard



To select the attributes of a schedule in the schedule wizard:

Step 1 Select the date, year, month, hour, minute, second, and AM or PM options from the First Run Date drop-down box (see Figure 11-5).

Step 2 Select **One Time** from the Interval drop-down box.

Step 3 Click **Next**.

A message appears to indicate that the Path Analyzer Server successfully received the schedule request (see Figure 11-6).

Figure 11-6 Finish Schedule Report Wizard Screen

Step 4 Click **Finish**.

The new scheduled report appears in the Schedule Manager.

Schedule Recurring Reports

Recurring reports are scheduled to run more than once. With the Schedule Manager, you can run reports daily, weekly, monthly, at the end of month, and annually.

Because you created the reports with the Schedule Manager, you can pick them up once or multiple times.

Start the Schedule Report Wizard

To start the Schedule Report wizard:

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar window appears.

Step 2 Click **Schedule New Report** in the Schedule Manager Toolbar, page 11-42.

The Schedule Report Wizard opens. If it is the first time you are scheduling a report during this session, the Report Wizard Welcome Screen appears. You can choose to view the Welcome Screen only once by selecting the appropriate check box.

Step 3 Click **Next**.

The Select a Report wizard screen appears.

Select a Report

To select a report in the Schedule Report wizard:

Step 1 Use the procedure to Select a Report, page 11-3 by clicking its radio button. See Figure 11-2 for more information.

Step 2 Click **Next**.

The Select an Autonomous System screen appears.

Select an Autonomous System

To select an autonomous system in the Schedule Report wizard:

Step 1 Use the procedure to Select an Autonomous System, page 11-3. See Figure 11-3 for more information.

Step 2 Click **Next**.

The Select Time Period wizard screen appears.

Select Time Period

To select the time period in the Schedule Report wizard:

Step 1 Select one of the following in the Select Time Period, page 11-4 wizard screen:

- **Current Day**—Covers from Midnight to the Run Time.
- **Full Day**—Covers the 24 Hours prior to the Run Time.
- **Current Week**—Covers from Sunday at Midnight to the Run Time.
- **Full Week**—Covers the seven Days prior to the Run Time.
- **Current Month**—Covers from the First of the Month to the Run Time.
- **Full Month**—Covers one Month prior to the Run Time.
- **Full Year**—Covers from the First of the Year to the Run Time.
- **Complete History**—Covers from the Last Database Purge to the Run Time.

See Figure 11-4 for more information.

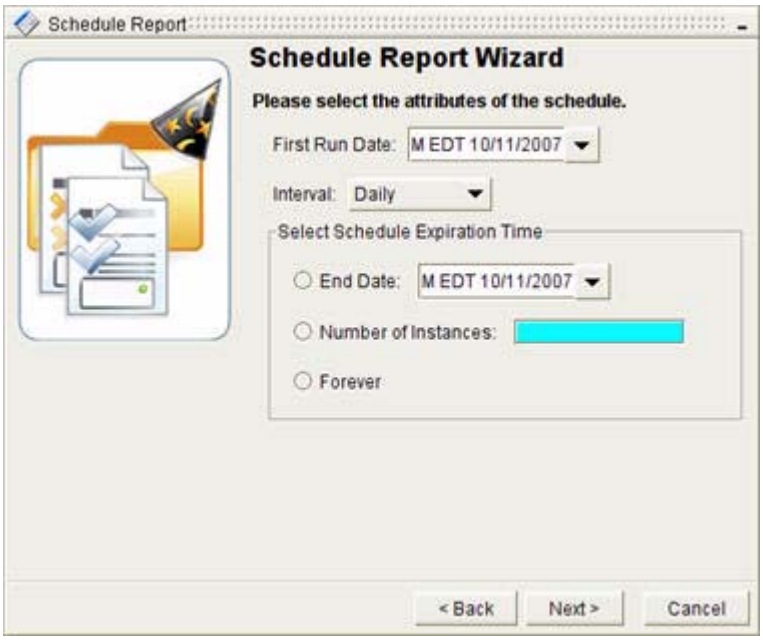
Step 2 Click **Next**.

The Select Schedule Attributes wizard screen appears.

Select Schedule Attributes

From the Select Schedule Attributes, page 11-8 wizard screen, select the run date, frequency, and end date of the task (see Figure 11-7).

Figure 11-7 Select Schedule Attributes Screen in Schedule Report Wizard



Step 1 Select the date, year, month, hour, minute, second, and AM or PM options in the First Run Date drop-down box.

Step 2 Select one of the following from the Interval drop-down box:

- **Daily**
- **Weekly**
- **Monthly**
- **End of Month**
- **Yearly**

Step 3 Select one of the following radio buttons from the Schedule Expiration Time field:

- **End Date**—Select an end date by selecting the **End Date** radio button, clicking the **End Date** drop-down box, and selecting the date, year, month, hour, minute, second, and AM or PM options. If you select this option, you must enter an end date for the schedule and its corresponding tasks. The schedule will stop running on this date.
- **Number of Instances**—Select how many times you want to run a schedule and its corresponding tasks by selecting the **Number of Instances** radio button, and entering the number of times the task should be repeated.
- **Forever—**Select the **Forever** radio button to run the schedule and its tasks perpetually.

Step 4 Click **Next**.

A message appears to indicate that the Path Analyzer Server successfully received the schedule request.

Step 5 Click **Finish**.

The new scheduled report appears in the Schedule Manager.

Scheduling Charts

With Path Analyzer Schedule Manager, you can generate and schedule one-time and recurring charts.

Schedule One-Time Charts

One-time charts are scheduled to run once. Choose a specific date using the Schedule Manager. Charts that have been created with the Schedule Manager can be picked up once or multiple times.

Start the Schedule Chart Wizard

To start the Schedule Chart wizard:

Step 1 Use the procedure to Start Schedule Manager, page 11-2. The Schedule Manager Toolbar window appears.

Step 2 Click **Schedule New Chart** in the Schedule Manager Toolbar, page 11-42.

The Schedule Chart Wizard opens. If it is the first time you are scheduling a chart during this session, the Chart Wizard Welcome Screen appears. You can choose to view the Welcome Screen only once by selecting the appropriate check box.

Step 3 Click **Next**.

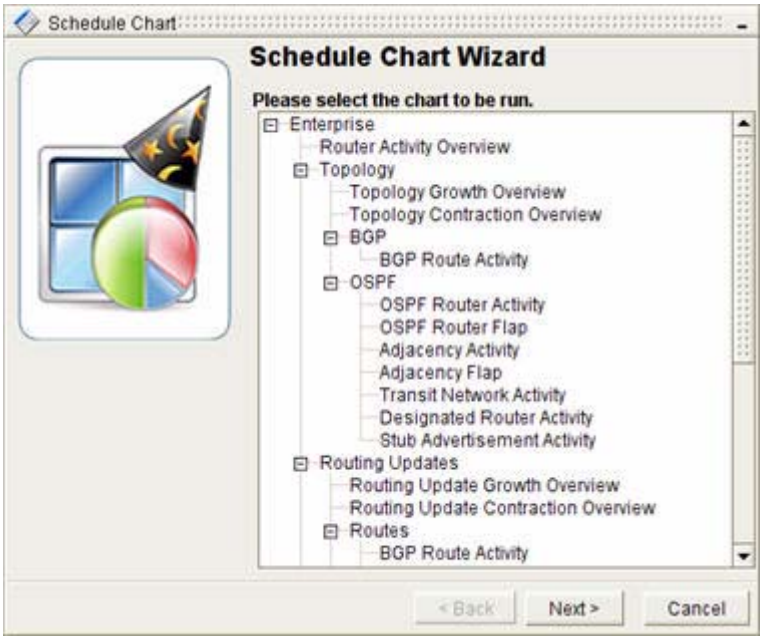
The Select a Chart wizard screen appears.

Select a Chart

To select a chart in the Schedule Chart wizard:

Step 1 Select a chart In the Select a Chart, page 11-10 screen by clicking on it (see Figure 11-8).

Figure 11-8 Select a Chart Screen in Schedule Chart Wizard



Step 2 Click **Next**.

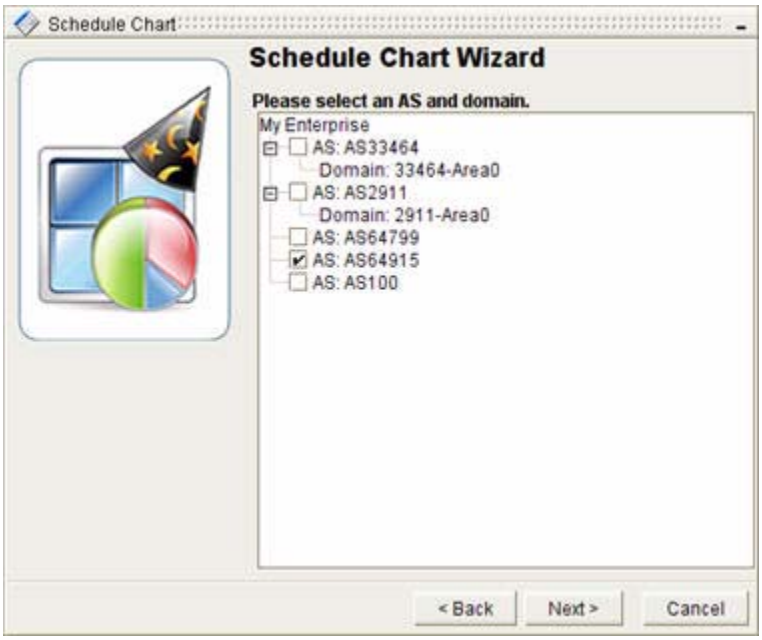
The Select an Autonomous System and Domain screen appears.

Select an AS and Domain

To select an autonomous system and domain in the Schedule Chart wizard:

Step 1 Select an autonomous system and domain by clicking its check box in the Select an AS and Domain, page 11-10 screen (see Figure 11-9).

Figure 11-9 Select an AS and Domain Screen in Schedule Chart Wizard



Step 2 Click **Next**.

The Select Relative Time Period and Mode, page 11-11 wizard screen appears.

Select Relative Time Period and Mode

To select a relative time period and mode in the Schedule Chart wizard (see Figure 11-10):

Step 1 Select one of the following in the Select Time Period field:

- **Current Day**—Covers from Midnight to the Run Time.
- **Full Day**—Covers the 24 Hours prior to the Run Time.
- **Current Week**—Covers from Sunday at Midnight to the Run Time.
- **Full Week**—Covers the seven Days prior to the Run Time.
- **Current Month**—Covers from the First of the Month to the Run Time.
- **Full Month**—Covers one Month prior to the Run Time.
- **Full Year**—Covers from the First of the Year to the Run Time.
- **Complete History**—Covers from the Last Database Purge to the Run Time.

Figure 11-10 Select a Time Period and Mode Screen in Schedule Chart Wizard

Step 2 Select one of the following options from the Select Mode field:

- **Trending Mode (Display over time)**—Shows trends by graphing changes that occur on your network in a selected time period.
- **Classification Mode (Display 10 top entities)—**Shows the top ten network entities that experienced the most change in the selected time period.
- **Distribution Mode (Display in pie chart)**—Shows, as a pie chart, the distribution of change across routing domains and autonomous systems.
- **Normalized Mode—**Shows a high-level view of network activity that occurred during a selected period of time using T-Score values.

Note You can select Normalized mode for the Routing Activity Overview chart only. This is a predefined, basic chart. For more information about basic charts, see Generating a Basic Chart, page 10-6.

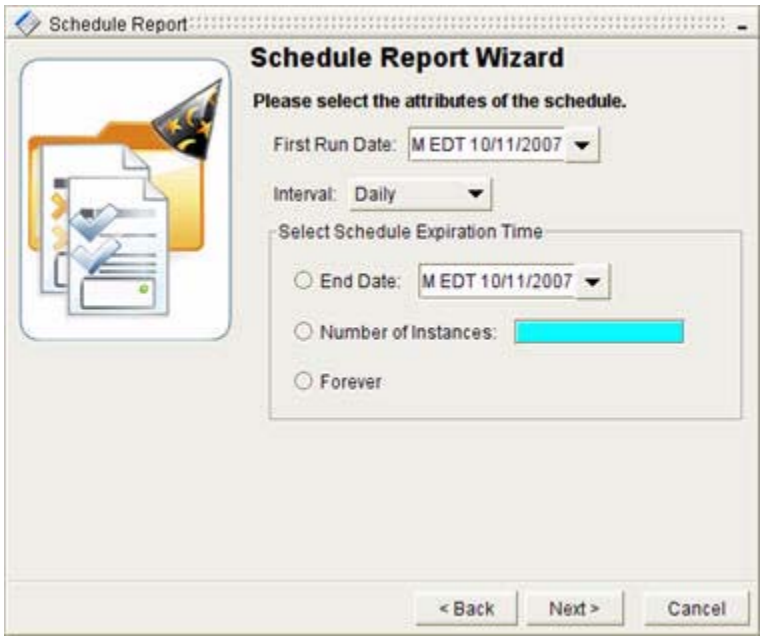
Step 3 Click **Next**.

The Select Schedule Attributes wizard screen appears.

Select Schedule Attributes

From the Select Schedule Attributes, page 11-12 wizard screen, select the run date, frequency, and end date of the task.

Figure 11-11 Select Schedule Attributes Screen in Schedule Chart Wizard



To select schedule attributes in the Schedule Chart wizard:

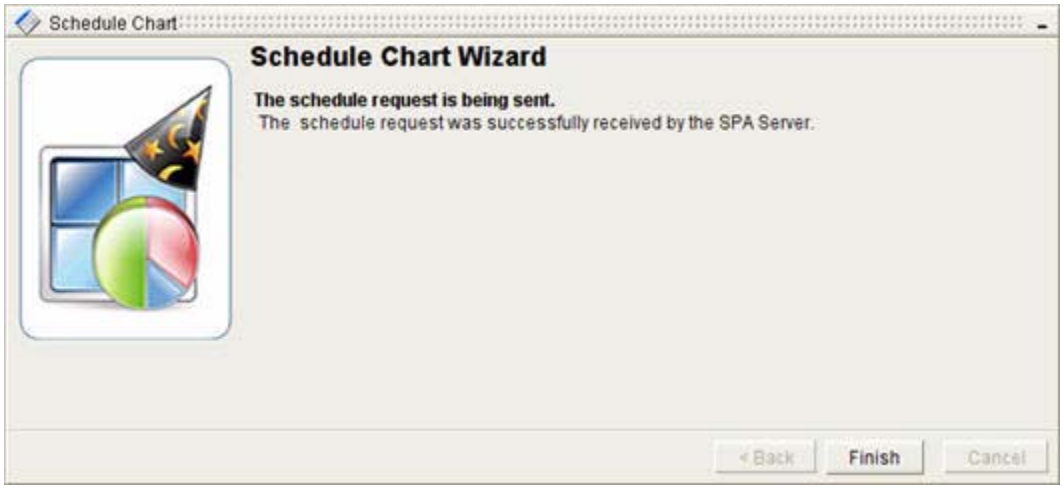
Step 1 Select the date, year, month, hour, minute, second, and AM or PM options from the First Run Date drop-down box (see Figure 11-11).

Step 2 Select **One Time** from the Interval drop-down box.

Step 3 Click **Next**.

A message appears to indicate that the Path Analyzer Server successfully received the schedule request (see Figure 11-12).

Figure 11-12 Finish Schedule Chart Wizard Screen



Step 4 Click **Finish**.

The new scheduled task appears in the Schedule Manager.

Schedule Recurring Charts

Recurring charts are scheduled to run more than once. With the Schedule Manager, you can run charts daily, weekly, monthly, end of month, and annually. Because you create the charts with the Schedule Manager, you can pick them up once or multiple times.

Start the Schedule Chart Wizard

To start the Schedule Chart wizard:

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar window appears.

Step 2 Click **Schedule New Chart** from the Schedule Manager Toolbar, page 11-42.

The Schedule Chart Wizard opens. If it is the first time you are scheduling a chart during this session, the Chart Wizard Welcome Screen appears. You can choose to view the Welcome Screen only once by selecting the appropriate check box.

Step 3 Click **Next**.

The Select the Chart wizard screen appears.

Select a Chart

To select a chart in the Schedule Chart wizard:

Step 1 Select a chart by clicking on it in the Select a Chart, page 11-10 screen. See Figure 11-8 for more information.

Step 2 Click **Next**.

The Select an Autonomous System and Domain screen appears.

Select an Autonomous System and Domain

To select an autonomous system and domain in the Schedule Chart wizard:

Step 1 Select an autonomous system and domain by clicking its check box in the Select an AS and Domain, page 11-10 screen. See Figure 11-9 for more information.

Step 2 Click **Next**.

The Select Relative Time Period and Mode, page 11-11 wizard screen appears.

Select Relative Time Period and Mode

To select a relative time period and mode in the Schedule Chart wizard:

Step 1 Select one of the following in the Select Time Period field:

- **Current Day**—Covers from Midnight to the Run Time.
- **Full Day**—Covers the 24 Hours prior to the Run Time.
- **Current Week**—Covers from Sunday at Midnight to the Run Time.
- **Full Week**—Covers the seven Days prior to the Run Time.
- **Current Month**—Covers from the First of the Month to the Run Time.
- **Full Month**—Covers one Month prior to the Run Time.
- **Full Year**—Covers from the First of the Year to the Run Time.
- **Complete History**—Covers from the Last Database Purge to the Run Time.

Step 2 Select one of the following options in the Select Mode field:

- **Trending Mode (Display over time)**—Shows trends by graphing changes that occur on your network in a selected time period.
- **Classification Mode (Display 10 top entities)—**Shows the top ten network entities that experienced the most change in the selected time period.
- **Distribution Mode (Display in pie chart)**—Shows, as a pie chart, the distribution of change across routing domains and autonomous systems.
- **Normalized Mode—**Shows a high-level view of network activity that occurred during a selected period of time using T-Score values.

See Figure 11-10 for more information.

Note You can only select normalized mode for the Routing Activity Overview chart. For more information about basic charts, see Generating a Basic Chart, page 10-6.

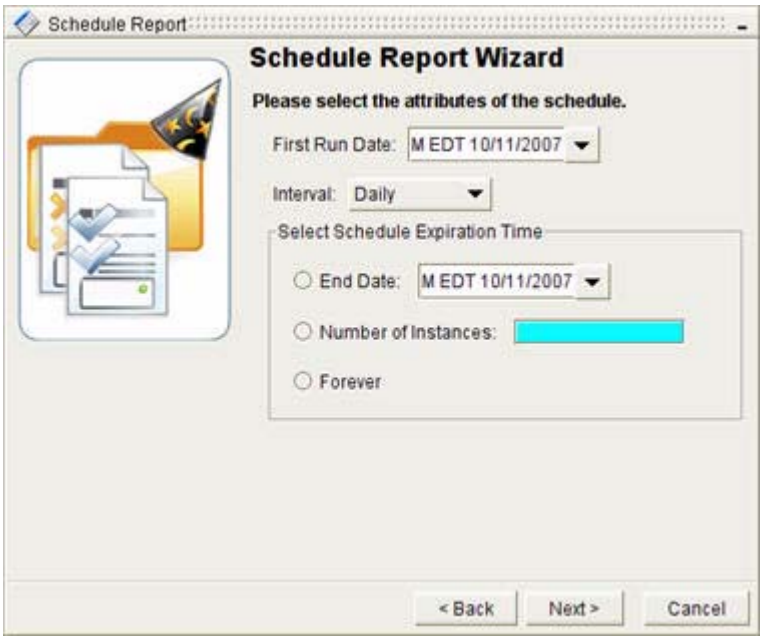
Step 3 Click **Next**.

The Select Schedule Attributes wizard screen appears.

Select Schedule Attributes

From the Select Schedule Attributes, page 11-15 wizard screen, select the run date, frequency, and end date of the task (see Figure 11-13).

Figure 11-13 Select Schedule Attributes Screen in Schedule Chart Wizard



To select schedule attributes in the Schedule Chart wizard:

Step 1 Select the date, year, month, hour, minute, second, and AM or PM options from the First Run Date drop down-box.

Step 2 Select one of the following from the Interval drop-down box:

- **Daily**
- **Weekly**
- **Monthly**
- **End of Month**
- **Yearly**

Step 3 Select one of the following radio buttons from the Schedule Expiration Time field:

- **End Date**—Select an end date by selecting the **End Date** radio button, clicking the **End Date** drop-down box, and selecting the date, year, month, hour, minute, second, and AM or PM options. If you select this option, you will enter an end date of a schedule and its corresponding tasks. The schedule will stop running on this date.
- **Number of Instances**—Select how many times you want to run a schedule and its corresponding tasks by selecting the **Number of Instances** radio button, and entering the number of times the task should be repeated.
- **Forever**—Select the **Forever** radio button to run the schedule and its tasks perpetually.

Step 4 Click **Next**.

A message appears to indicate that the Path Analyzer Server successfully received the schedule request.

Step 5 Click **Finish**.

The new scheduled task appears in the Schedule Manager.

Scheduling Advanced Charts

With Path Analyzer Schedule Manager, you can generate and schedule one-time and recurring advanced charts.

Schedule One-Time Advanced Charts

One-time advanced charts are scheduled to run once. Choose a specific date the Schedule Manager. Advanced charts that are created with the Schedule Manager can be picked up once, or multiple times.

Start the Schedule Advanced Chart Wizard

To start the Schedule Advanced Chart wizard:

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar window appears.

Step 2 Click **Schedule New Advanced Chart** in the Schedule Manager Toolbar, page 11-42.

The Schedule Advanced Chart Wizard wizard opens. If it is the first time you are scheduling a chart during this session, the Advanced Chart Wizard Welcome Screen appears. You can choose to view the Welcome Screen only once by selecting the appropriate check box.

Step 3 Click **Next**.

The Select Data Sets wizard screen appears.

Select Data Sets

Figure 11-14 Select Data Set Screen in Schedule Advanced Chart Wizard

To select data sets in the Schedule Advanced Chart wizard:

Step 1 Select Data Sets by clicking their check boxes (see Figure 11-14).

Step 2 Click **Next**.

The Select Entities screen appears.

Select Entities

Figure 11-15 Select Entities Screen in Schedule Advanced Chart Wizard

To select entities in the Schedule Advanced Chart wizard:

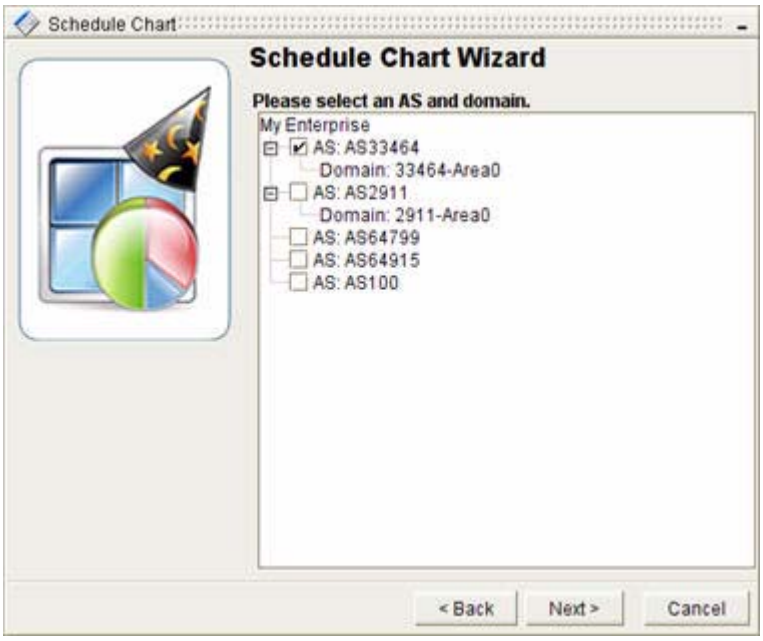
Step 1 Select Entities by clicking their check boxes in the Select Entities screen (see Figure 11-15). For a complete explanation of selecting entities in the Advanced Chart Wizard, see Select Entities, page 10-14.

Step 2 Click **Next**.

The Select an Autonomous System and Domain screen appears.

Select an AS and Domain

Figure 11-16 Select an AS and Domain Screen in Schedule Advanced Chart Wizard



To select an autonomous system and domain in the Schedule Advanced Chart wizard:

Step 1 Select an autonomous system and domain by clicking its check box in the Select an AS and Domain, page 11-20 screen (see Figure 11-16).

Step 2 Click **Next**.

The Specify Related Entity Types screen appears.

Specify Related Entity Types

Figure 11-17 Specify Entity Types Screen in Schedule Advanced Chart Wizard

To select related entity types in the Schedule Advanced Chart wizard:

Step 1 Specify Related Entity Types by choosing either the **Choose All Existing Entities** or the **Choose Specific Entities** radio button in the Specify Related Entity Types screen (see Figure 11-17). For more complete information on selecting related entity types, see Select Entity Types, page 10-16.

Note The fields displayed in the Choose Specific Entities section of the Select Entity Types screen will depend on the entities you selected in the previous Select Entities screen.

Step 2 Click **Next**.

Select Relative Time Period

Figure 11-18 Select Time Period Screen in Schedule Advanced Chart Wizard

To select a relative time period in the Schedule Advanced Chart wizard:

Step 1 Select one of the following in the Select Relative Time Period, page 11-22 wizard screen (see Figure 11-18):

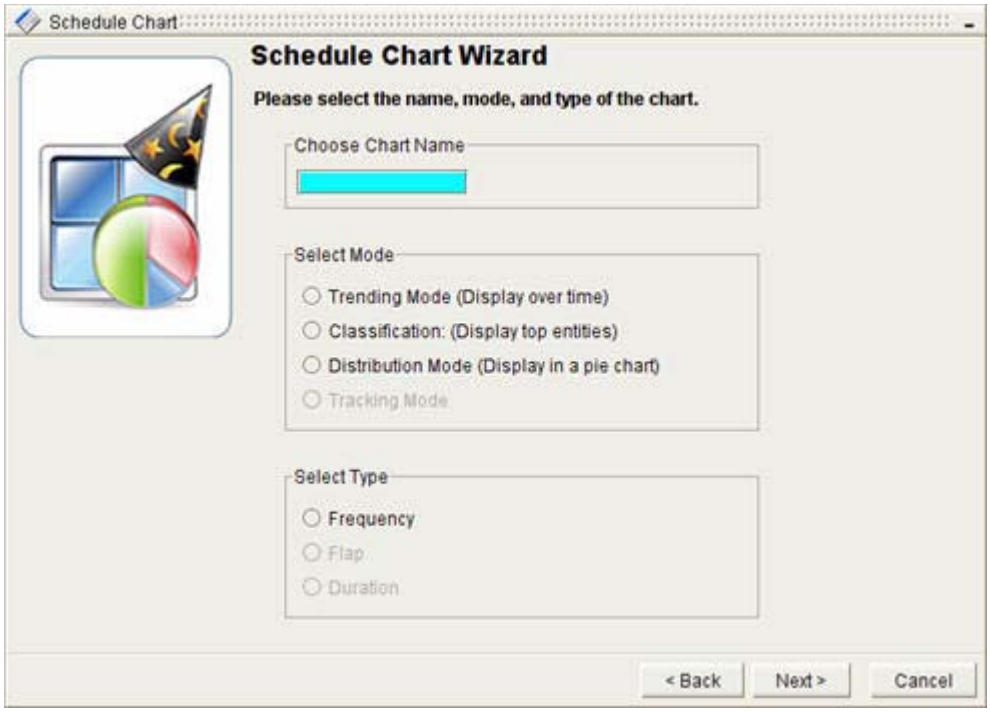
- **Current Day**—Covers from Midnight to the Run Time.
- **Full Day**—Covers the 24 Hours prior to the Run Time.
- **Current Week**—Covers from Sunday at Midnight to the Run Time.
- **Full Week**—Covers the seven Days prior to the Run Time.
- **Current Month**—Covers from the First of the Month to the Run Time.
- **Full Month**—Covers one Month prior to the Run Time.
- **Full Year**—Covers from the First of the Year to the Run Time.
- **Complete History**—Covers from the Last Database Purge to the Run Time.

Step 2 Click **Next**.

The Select Name, Mode, and Type of Chart wizard screen appears.

Select the Name, Mode, and Type of Chart

Figure 11-19 Select Name, Mode, and Type of Chart Screen in Schedule Advanced Chart Wizard



To select the name, mode, and type of chart in the Schedule Advanced Chart wizard:

Step 1 Enter a name for the chart in the Choose Chart Name field (see Figure 11-19).

For more complete information on this and the following two steps, see Select the Name, Mode, and Type of Chart, page 10-18.

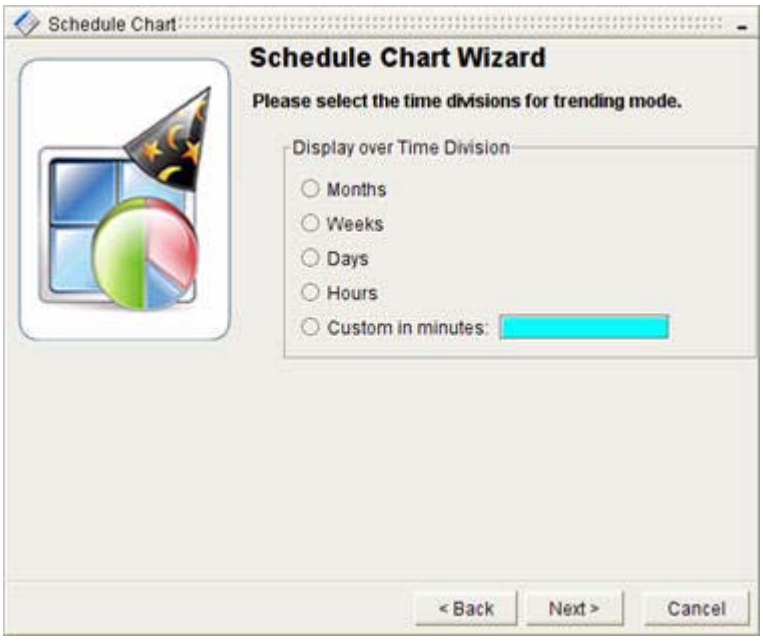
Step 2 Select the Mode, page 10-19 in the Select Mode field.

Step 3 Select Type, page 10-20 in the Select Type field.

Step 4 Click **Next**.

Divide the Period of Time

Figure 11-20 Select Time Divisions Screen in Schedule Advanced Chart Wizard



To select the time division in the Schedule Advanced Chart wizard (see Figure 11-20):

Step 1 Select how to divide the period of time of a Trending chart (if applicable). In the Display over Time Division area, divide the period of time into one of the following options:

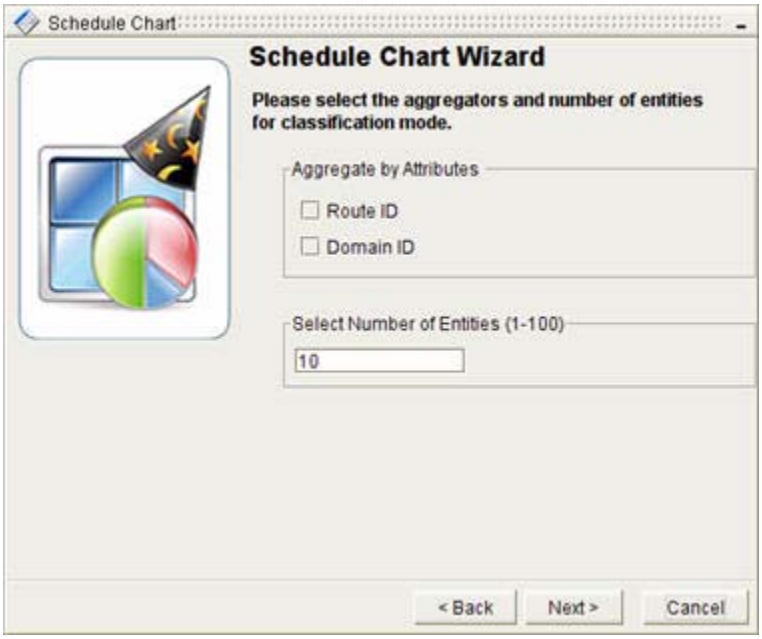
- **Months**
- **Weeks**
- **Days**
- **Hours**
- **Custom in Minutes**

For more information on dividing the period of time, see Select the Time Divisions of a Trending Chart, page 10-20.

Step 2 Click **Next**.

Select Aggregators and Entities (Classification)

Figure 11-21 Select Aggregators and Entities of a Classification Chart Screen in Schedule Advanced Chart Wizard



To select aggregators and entities for a classification chart in the Schedule Advanced Chart wizard (see Figure 11-21):

Step 1 Select the Aggregators and Entities of a Classification Chart (if applicable). For more information on selecting aggregators and entities, please see Select the Aggregators and Entities of a Classification Chart, page 10-21.

Step 2 Click **Next**.

The Preview the Chart screen appears.

Preview the Chart

Figure 11-22 Preview Screen in Schedule Advanced Chart Wizard

To preview the chart in the Schedule Advanced Chart wizard:

Step 1 Preview the chart to make sure you have selected the correct charts, autonomous systems, entities, mode, and period of time (see Figure 11-22).

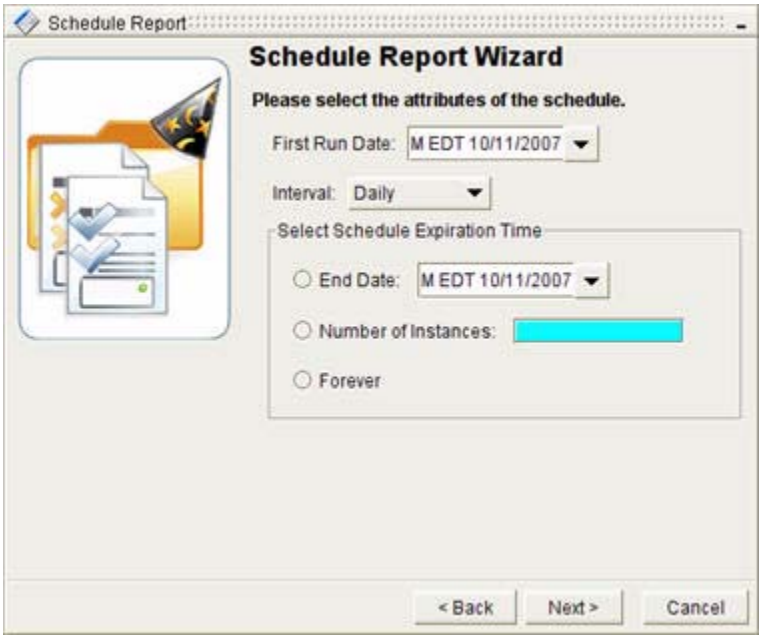
Step 2 Click **Next**.

The Select Schedule Attributes wizard screen appears.

Select Schedule Attributes

From the Select Schedule Attributes, page 11-26 wizard screen, select the run date, frequency, and end date of the task.

Figure 11-23 Select Schedule Attributes Screen in Advanced Charts in Schedule Advanced Chart Wizard



To select schedule attributes in the Schedule Advanced Chart wizard (see Figure 11-23):

Step 1 Select the date, year, month, hour, minute, second, and AM or PM options from the First Run Date drop-down box.

Step 2 Select **One Time** from the Interval drop-down box.

Step 3 Click **Next**.

A message appears to indicate that the Path Analyzer Server successfully received the schedule request.

Step 4 Click **Finish**.

The new scheduled task appears in the Schedule Manager.

Schedule Recurring Advanced Charts

Recurring advanced charts are scheduled to run more than once. With the Schedule Manager, you can run advanced charts daily, weekly, monthly, end of month, and yearly. Because you create the advanced charts with the Schedule Manager, you can pick them up once or multiple times.

Start the Schedule Advanced Chart Wizard

To start the Schedule Advanced Chart wizard:

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar window appears.

Step 2 Click **Schedule New Advanced Chart** in the Schedule Manager Toolbar, page 11-42. The Schedule Advanced Chart Wizard wizard opens. If it is the first time you are scheduling a chart during this session, the Advanced Chart Wizard Welcome Screen appears. You can choose to view the Welcome Screen only once by selecting the appropriate check box.

Step 3 Click **Next** if you are viewing the Welcome Screen.

Note The following section steps through scheduling an advanced chart. For more complete information on each of the following steps, see Generating an Advanced Chart, page 10-11.

Select Data Sets

To select data sets in the Schedule Advanced Chart wizard:

Step 1 Select Data Sets, page 11-18 by clicking their check boxes in the Select Data Sets screen.

See Figure 11-14: *Select Data Set Screen in Schedule Advanced Chart Wizard* for more information.

Step 2 Click **Next**.

The Select Entities screen appears.

Select Entities

To select entities in the Schedule Advanced Chart wizard:

Step 1 Select Entities by clicking their check boxes in the Select Entities screen. For a complete explanation of selecting entities in the Advanced Chart Wizard, see Select Entities, page 11-19.

See Figure 11-15 for more information.

Step 2 Click **Next**.

The Select an Autonomous System and Domain screen appears.

Select an AS and Domain

To select an autonomous system and domain in the Schedule Advanced Chart wizard:

Step 1 Select an autonomous system and domain by clicking its check box in the Select an AS and Domain, page 11-20 screen.

See Figure 11-16 for more information.

Step 2 Click **Next**.

The Specify Related Entity Types screen appears.

Specify Related Entity Types

To select related entity types in the Schedule Advanced Chart wizard:

Step 1 Specify Related Entity Types by choosing either the **Choose All Existing Entities** or the **Choose Specific Entities** radio button in the Specify Related Entity Types, page 11-21 screen. For more complete information on selecting related entity types, see Select Entity Types, page 10-16.

See Figure 11-17 for more information.

Note The fields displayed in the Choose Specific Entities section of the Select Entity Types screen will depend on the entities you selected in the previous Select Entities screen.

Step 2 Click **Next**.

Select Relative Time Period

To select the relative time period in the Schedule Advanced Chart wizard:

Step 1 Select one of the following in the Select Relative Time Period, page 11-22 wizard screen:

- **Current Day**—Covers from Midnight to the Run Time.
- **Full Day**—Covers the 24 Hours prior to the Run Time.
- **Current Week**—Covers from Sunday at Midnight to the Run Time.
- **Full Week**—Covers the seven Days prior to the Run Time.
- **Current Month**—Covers from the First of the Month to the Run Time.
- **Full Month**—Covers one Month prior to the Run Time.
- **Full Year**—Covers from the First of the Year to the Run Time.
- **Complete History**—Covers from the Last Database Purge to the Run Time.

See Figure 11-18: *Select Time Period Screen in Schedule Advanced Chart Wizard* for more information.

Step 2 Click **Next**.

The Select Name, Mode, and Type of Chart wizard screen appears.

Select the Name, Mode, and Type of Chart

To select the name, mode, and type of chart in the Schedule Advanced Chart wizard:

Step 1 Enter a name for the chart in the **Choose Chart Name** field.

For more complete information on this and the following two steps, see Select the Name, Mode, and Type of Chart, page 10-18, or Figure 11-19.

Step 2 Select the Mode in the Select Mode field.

Step 3 Select Type in the Select Type field.

Step 4 Click **Next**.

Divide the Period of Time

To select the time division in the Schedule Advanced Chart wizard:

Step 1 Select how to divide the period of time of a Trending chart (if applicable). In the Display over Time Division area, divide the period of time into one of the following options:

- **Months**
- **Weeks**
- **Days**
- **Hours**
- **Custom in Minutes**

For more information on dividing the period of time, see Select the Time Divisions of a Trending Chart, page 10-20, or Figure 11-20.

Step 2 Click **Next**.

Select Aggregators and Entities (Classification)

To select the aggregators and entities for a classification chart in the Schedule Advanced Chart wizard:

Step 1 Select the Aggregators and Entities of a Classification Chart (if applicable). For more information on selecting aggregators and entities, please see Select the Aggregators and Entities of a Classification Chart, page 10-21, or Figure 11-21.

Step 2 Click **Next**.

The Preview the Chart screen appears.

Preview the Chart

To preview the chart in the Schedule Advanced Chart wizard:

Step 1 Preview the chart to make sure you have selected the correct charts, autonomous systems, entities, mode, and period of time.

See Figure 11-28 for more information.

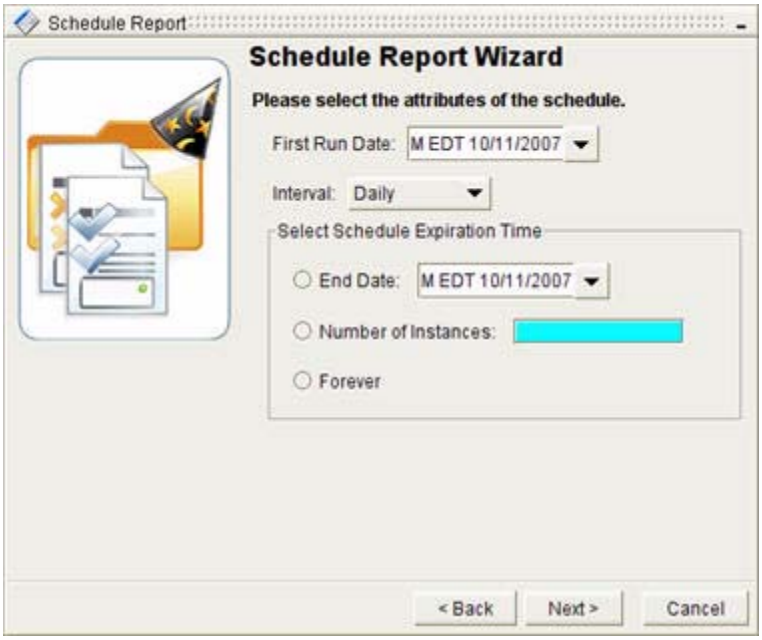
Step 2 Click **Next**.

The Select Schedule Attributes wizard screen appears.

Select Schedule Attributes

From the Select Schedule Attributes wizard screen, select the run date, frequency, and end date of the task (see Figure 11-24).

Figure 11-24 Select Schedule Attributes Screen in Schedule Advanced Chart Wizard



To select schedule attributes in the Schedule Advanced Chart wizard:

Step 1 select the date, year, month, hour, minute, second, and AM or PM options from the First Run Date drop-down box.

Step 2 Select one of the following from the Interval drop-down box:

- **Daily**
- **Weekly**
- **Monthly**
- **End of Month**
- **Yearly**

Step 3 Select one of the following radio buttons from the Schedule Expiration Time field:

- **End Date**—Select an end date by selecting the **End Date** radio button, clicking the **End Date** drop-down box, and selecting the date, year, month, hour, minute, second, and AM or PM options. If you select this option, you must enter an end date for the schedule and its corresponding tasks. The schedule will stop running on this date.
- **Number of Instances**—Select how many times you want to run a schedule and its corresponding tasks by selecting the **Number of Instances** radio button, and entering the number of times the task should be repeated.
- **Forever—**Select the **Forever** radio button to run the schedule and its tasks perpetually.

Step 4 Click **Next**.

A message appears to indicate that the Path Analyzer Server successfully received the schedule request.

Step 5 Click **Finish**. The new scheduled task appears in the Schedule Manager.

Managing Scheduled Reports, Charts, and Advanced Charts

In Schedule Manager, you can perform the following tasks:

- Filter Scheduled Tasks, page 11-33
- View Scheduled Tasks, page 11-35
- Preview Scheduled Task, page 11-35
- Derive Scheduled Tasks, page 11-37
- Derive One-time Scheduled Tasks, page 11-38
- Derive Recurring Scheduled Tasks, page 11-38
- Modify Scheduled Tasks, page 11-39
- Modify One-time Scheduled Tasks, page 11-39
- Modify Recurring Scheduled Tasks, page 11-39
- Delete Scheduled Task, page 11-40
- Skip an Occurrence of Scheduled Task, page 11-40
- Extend Purge Date, page 11-41
- Perpetuate Schedule, page 11-41
- Pick Up Completed Task, page 11-42

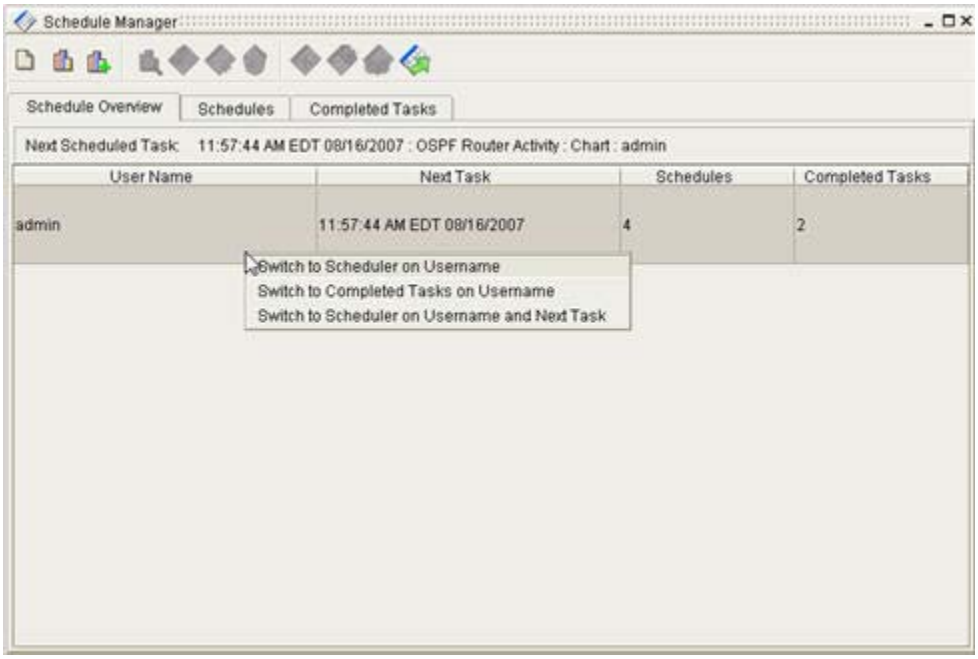
Schedule Manager

Using the Path Analyzer Schedule Manager, you can access and modify your scheduled charts and reports. The Schedule Manager has three tabs (see Figure 11-25):

- The **Schedule Overview** tab allows you to manage your list of scheduled tasks. In this tab, you can preview, derive, modify, delete, and/or skip any scheduled task. In addition, right-clicking an item in the table displays a menu where you can select one of the following options:
  - **Switch to Scheduler on Username**—Displays the **Schedules** tab sorted by user name.
  - **Switch to Completed Tasks on Username**—Displays the **Completed Tasks** tab sorted by user name.
  - **Switch to Scheduler on Username and Next Task**—Displays the **Schedules** tab sorted by user name and next task.
- The **Schedules** tab of the Schedule Manager allows you to filter or sort your list of scheduled tasks by the following criteria:
  - Schedule Name
  - Creator
  - Type (Chart, Report, None)

  - Interval (One Time, Daily, Weekly, Monthly, End of Month, Yearly, None)
  - Date Created
  - Next Task
- The **Completed Tasks** tab of the Schedule Manager allows you to filter, sort, preview, delete, and/or pick up any completed task.

Figure 11-25 Schedule Manager



Filter Scheduled Tasks

To filter scheduled tasks:

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager appears.

Step 2 Click the **Schedules** or **Completed Tasks** tab in Schedule Manager Toolbar, page 11-42.

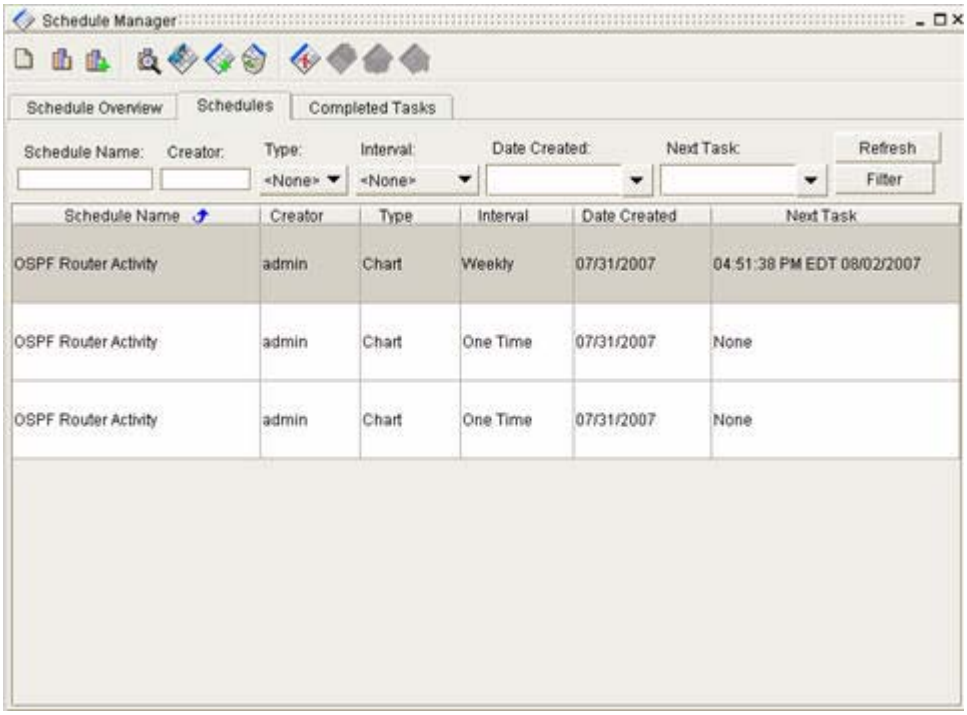
Step 3 Filter by Schedule Name, Creator, Type, Interval, Date Created, or Next Task in the Schedules tab by either:

- Entering the Schedule Name, Creator, Type, Interval, Date Created, or Next Task in the corresponding field and clicking the **Filter** button

  or

- Clicking on the corresponding column heading. When you filter on a column heading, a blue arrow is displayed to indicate which criteria is being used to filter and in what direction, as shown in Figure 11-26.

Figure 11-26 Schedules Tab in Schedule Manager



Step 4 Filter by Task Name, Creator, Type, Interval, Date Created, Run Date, or Purge Date from the Completed Tasks tab by either:

- Entering the Task Name, Creator, Type, Interval, Date Created, Run Date or Purge Date in the corresponding field and clicking the **Filter** button

  or

- Clicking on the corresponding table heading.

Figure 11-27 Completed Tasks Tab in Schedule Manager

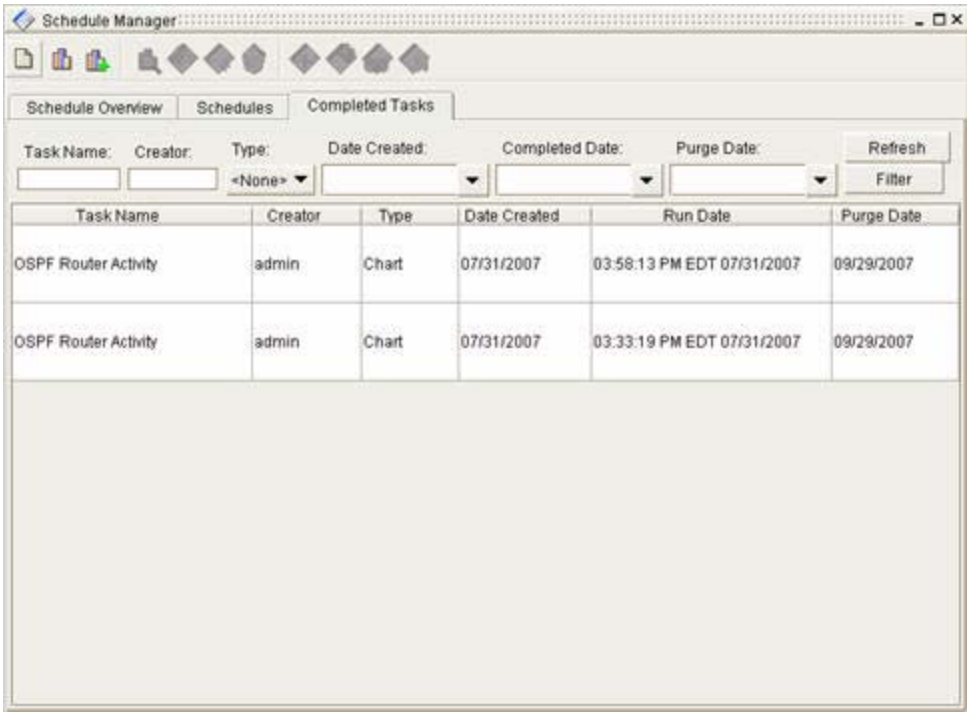


Figure 11-27 shows the Completed Tasks tab of Schedule Manager.

Note After filtering scheduled tasks, you can refresh the list of scheduled tasks by clicking the **Refresh** button.

View Scheduled Tasks

To view a scheduled task,

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager appears.

Step 2 Click the **Schedules** tab in Schedule Manager Toolbar, page 11-42.

Step 3 In the Schedules tab, you can view a list of scheduled tasks in a table. From the table, you can filter or sort the scheduled events by any of the column headings.

Note You can also view scheduled tasks from the Completed Tasks tab. See Completed Tasks, page 11-45 for more information.

Preview Scheduled Task

To preview a scheduled task:

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager appears.

Step 2 Click the **Schedules** tab.

Step 3 Select a report, chart, or advanced chart from the table in the Schedules tab.

Step 4 Click the **Preview Schedule** icon in the Schedule Manager Toolbar, page 11-42.

The Preview Schedule window appears (see Figure 11-28).

Figure 11-28 Preview Schedule in Schedule Manager

Note The Preview Schedule window differs for scheduled reports and scheduled charts. There are also slight variations among charts, depending upon which graph mode was selected.

Preview Scheduled Reports

The Preview Schedule window for Reports displays the following data:

- **Report Name**—The report's name.
- **Chart Names**—The names of charts associated with the report.
- **Domains**—The names of domains included in the report.
- **Time Period**—The report's time period.
- **Schedule Creation Date**—The schedule's creation date.
- **Schedule Interval—**The schedule's interval.
- **Previous Run Date—**The schedule's previous run date (if applicable).

- **Next Run Date**—The schedule's next run date.
- **Schedule Instances**—The number of instances remaining in the schedule (if applicable).

Preview Scheduled Reports

The Preview Schedule window for Charts displays the following data:

- **Chart Name**—The chart's name.
- **Data Sets—**The names of the data sets selected for the chart.
- **Entities—**The names of the entities selected for the chart.
- **Domains**—The names of domains included in the chart.
- **Time Period**—The report's time period.
- **Graph Mode**—The graph mode in which the chart was run.
- **Time Division**—The chart's time division. Please note that this field is dependent upon the graph mode.
- **Schedule Creation Date**—The schedule's creation date.
- **Schedule Interval—**The schedule's interval.
- **Previous Run Date—**The schedule's previous run date (if applicable).
- **Next Run Date**—The schedule's next run date.
- **Schedule Instances**—The number of instances remaining in the schedule (if applicable).

Derive Scheduled Tasks

To derive a scheduled task,

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar appears.

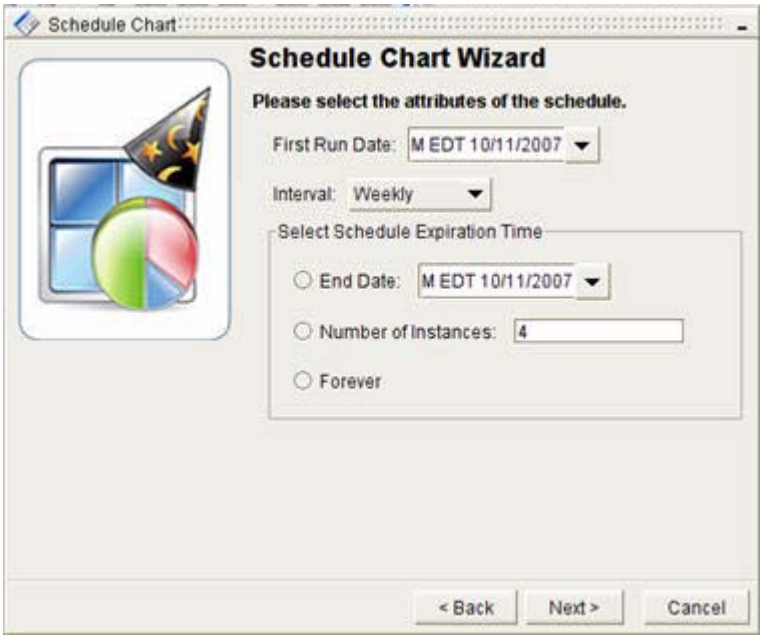
Step 2 Click the **Schedules** tab.

Step 3 Select a report, chart, or advanced chart from the table from the Schedules tab.

Step 4 Click the **Derive Schedule** icon in the Schedule Manager Toolbar, page 11-42.

The Select Schedule Attributes screen appears (see Figure 11-29). From the Select Schedule Attributes, page 11-5 window, you can create a new schedule based on the report, chart, or advanced chart that already exists from the Schedules tab.

Figure 11-29 Select Schedule Attributes Screen in Schedule Wizard



See Scheduling Reports, page 11-2, Scheduling Charts, page 11-9, or Scheduling Advanced Charts, page 11-17 for more information about how to schedule a report, chart, or advanced chart.

Step 5 Select the run date, frequency, and end date of the task in the Select Schedule Attributes, page 11-15 window.

Derive One-time Scheduled Tasks

To derive a one-time scheduled task:

Step 1 Select the date, year, month, hour, minute, second, and AM or PM options from the First Run Date drop-down box.

Step 2 From the Interval drop-down box, select **One Time**.

Step 3 Click **Next**.

Derive Recurring Scheduled Tasks

To derive recurring scheduled tasks:

Step 1 Select the date, year, month, hour, minute, second, and AM or PM options from the First Run Date drop-down box.

Step 2 Select daily, weekly, monthly, end of month, or yearly from the Interval drop-down box.

Step 3 Select one of the following radio buttons from the Schedule Expiration Time field:

- **End Date**—Select an end date by selecting the **End Date** radio button, clicking the **End Date** drop down box, and selecting the date, year, month, hour, minute, second, and AM or PM options. If you select this option, you will enter an end date of a schedule and its corresponding tasks. The schedule will stop running on this date.
- **Number of Instances**—Select how many times you want to run a schedule and its corresponding tasks by selecting the Number **of Instances** radio button, and entering the number of times the task should be repeated.
- **Forever**—Select the **Forever** radio button to run the schedule and its tasks perpetually.

Step 4 Click **Next**.

Step 5 Click **Finish**.

The new scheduled task appears in the Schedule Manager.

Modify Scheduled Tasks

To modify a scheduled task,

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar appears.

Step 2 Click the **Schedules** tab.

Step 3 Select a report, chart, or advanced chart from the table.

Step 4 Click the **Modify Schedule** icon from the Schedule Manager Toolbar, page 11-42.

The Select Schedule Attributes screen appears.

From the Select Schedule Attributes, page 11-31 screen, you can modify the run date, frequency, and end date of the task.

Modify One-time Scheduled Tasks

To modify a one-time scheduled task,

Step 1 Modify the date, year, month, hour, minute, second, and AM or PM options in the First Run Date drop-down box.

Step 2 Select **One Time** from the Interval drop-down box.

Step 3 Click **Next**.

Modify Recurring Scheduled Tasks

To modify recurring scheduled tasks:

Step 1 Modify the date, year, month, hour, minute, second, and AM or PM options from the First Run Date drop-down box.

Step 2 Select **Daily**, **Weekly**, **Monthly**, **End of Month**, or **Yearly** from the Interval drop-down box.

Step 3 Select one of the following radio buttons from the Schedule Expiration Time field:

- **End Date**—Select an end date by selecting the **End Date** radio button, clicking the **End Date** drop-down box, and selecting the date, year, month, hour, minute, second, and AM or PM options. If you select this option, you will enter an end date of a schedule and its corresponding tasks. The schedule will stop running on this date.
- **Number of Instances**—Select how many times you want to run a schedule and its corresponding tasks by selecting the **Number of Instances** radio button, and entering the number of times the task should be repeated.
- **Forever**—Select the **Forever** radio button to run the schedule and its tasks perpetually.

Step 4 Click **Next**.

Step 5 Click **Finish**.

The modified scheduled task appears in the Schedule Manager.

Delete Scheduled Task

To delete a scheduled task,

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar appears.

Step 2 Click the **Schedules** or **Completed Tasks** tab.

Step 3 Select a report, chart, or advanced chart from the table.

Step 4 Click the **Delete Schedule** icon in the Schedule Manager Toolbar, page 11-42.

The scheduled task is deleted from the table.

Note You can delete scheduled tasks from the **Completed Tasks** tab, however, these tasks have already been completed. See Completed Tasks, page 11-45 for more information.

Skip an Occurrence of Scheduled Task

To skip an occurrence of a scheduled task,

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar appears.

Step 2 Click the **Schedules** tab.

Step 3 Select a report, chart, or advanced chart from the table.

Step 4 Click the **Skip Schedule** icon in the Schedule Manager Toolbar, page 11-42.

In the Next Task column, the date changes to the next scheduled date. For example, if a report is scheduled to run weekly and the originally scheduled date is 11:58:27 AM EST 02/22/2007, click **Skip Schedule** to skip that date. The new date that appears in the Next Task column becomes 11:58:27 AM EST 03/01/2007.

Note If you selected **Number of Instances** in the Schedule Expiration Time field, the next scheduled task date still increments by one in the Next Task column.

Extend Purge Date

Once a task is completed, you can make sure the resulting report or chart is kept in the system for longer than originally planned.

To extend the purge date of a completed task,

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar appears.

Step 2 Click the **Completed Tasks** tab.

Step 3 Select a report, chart, or advanced chart from the table.

Step 4 Click the **Extend Purge Date** icon in the Schedule Manager Toolbar, page 11-42.

The Purge Date column displays an additional life span added to the purge date. The life span for keeping completed tasks in Schedule Manager is defined in User Preferences. For additional information on changing the life span of your schedules and tasks, please see Set Preferences on page 1-24.

Perpetuate Schedule

You can keep a completed task in the Schedule Manager forever, ensuring its chart or report will never be deleted.

To change the purge date to forever,

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar appears.

Step 2 Click the **Completed Tasks** tab.

Step 3 Select a report, chart, or advanced chart from the table.

Step 4 Click the **Perpetuate Tasks** icon in the Schedule Manager Toolbar, page 11-42.

In the Purge Date column, the date changes from a specific date to Forever.

Pick Up Completed Task

Use the Schedule Manager to pick up a completed task. Picking up a completed task means that the selected task is sent to the Report Manager or Chart Manager for viewing. The task will only remain in the Report Manager or Chart Manager for that session. However, you can repeat sending the task to the Report Manager or Chart Manager as long as it remains in the Schedule Manager.

To pick up a completed task:

Step 1 Use the procedure to Start Schedule Manager, page 11-2.

The Schedule Manager Toolbar appears.

Step 2 Click the **Completed Tasks** tab.

Step 3 Select a report, chart, or advanced chart from the table.

Step 4 Click the **Pick Up Tasks** icon in the Schedule Manager Toolbar, page 11-42.

The report, chart, or advanced chart is sent to Report Manager or Chart Manager to view.

Note You can select multiple reports or charts using the Shift-Click function and pick up all the selected items at once.

Related Forms

This section contains tables that detail graphical elements and dialog boxes in the Schedule Manager.

Schedule Manager Toolbar

Table 11-1 describes Schedule Manager Toolbar buttons.

Table 11-1 Schedule Manager Toolbar Buttons

Button	Description
Schedule New Report 	Enables you to Start the Schedule Report Wizard, page 11-3, from which you can generate and schedule reports. Available from all three Schedule Manager tabs.
Schedule New Chart 	Enables you to Start the Schedule Chart Wizard, page 11-9, from which you can generate and schedule charts. Available from all three Schedule Manager tabs.
Schedule New Advanced Chart 	Enables you to Start the Schedule Advanced Chart Wizard, page 11-17, from which you can generate and schedule advanced charts. Available from all three Schedule Manager tabs.
Preview Schedule 	Allows you to view the properties of a scheduled report, chart, or advanced chart, from the Schedules tab.
Derive Schedule 	Allows you to derive a new schedule, based on an already existing schedule, from the Schedules tab.
Modify Schedule 	Allows you to modify a schedule from the Schedules tab.
Delete Schedule 	Allows you to delete a schedule from the Schedules or Completed Tasks tabs.
Skip Schedule 	Allows you to skip an occurrence of a scheduled task from the Schedules tab.

Table 11-1 Schedule Manager Toolbar Buttons (continued)

Button	Description
Extend Purge Date 	Allows you to extend the purge date by a life span (as defined in User Preferences), in the Completed Tasks tab. Extending the purge date keeps the generated report, chart, or advanced chart in the Schedule Manager longer. For more information on changing the life span of your schedules and tasks, please see Set Preferences, page 1-24.
Perpetuate Task 	Allows you to change the purge date to Forever in the Completed Tasks tab, meaning the generated report, chart, or advanced chart will never be deleted from the Schedule Manager.
Pickup Task 	Allows you to select a completed task from the Completed Tasks tab, and send it to be viewed in Report Manager or Chart Manager.

Schedules

From the Schedules tab in the Schedule Manager, you can preview, derive, modify, delete, and skip scheduled tasks.

Table 11-2 describes the fields and buttons in the **Schedules** tab of the Schedule Manager.

Table 11-2 Scheduler Tab Fields and Buttons

Field or Button	Description
Schedule Name	Text box that allows you to filter the scheduled tasks by schedule name.
Creator	Text box that allows you to filter the scheduled tasks by creator.
Type	Drop-down box that allows you to filter the scheduled tasks by chart, report, or none.
Interval	Drop-down box that allows you to filter the scheduled tasks by frequency (One Time, Daily, Weekly, Monthly, End of Month, Yearly, or None).
Date Created	Drop-down box that allows you to filter the scheduled tasks by the date it was created.
Next Task	Drop-down box that allows you to filter the scheduled tasks by the next date that they are run.
Filter	Click this button to filter table by schedule name, creator, type (report or chart), interval (one time, daily, weekly, monthly, end of month, or yearly), date created, or next task.

Table 11-2 Scheduler Tab Fields and Buttons (continued)

Field or Button	Description
Refresh	Click this button to refresh the table after filtering it by a specific column name.
Schedule Name	Displays the name of the scheduled task. You can also sort by this column.
Creator	Displays the creator of the scheduled task. You can also sort by this column.
Type	Displays the type of scheduled task: Report, Chart, or Advanced Chart. You can also sort by this column.
Interval	Displays the frequency of the scheduled task. You can also sort by this column.
Date Created	Displays the date the scheduled task was created. You can also sort by this column.
Next Task	Displays the date when the next task will be run. You can also sort by this column.
Switch to Completed Tasks on this Schedule	If you select and right-click on a scheduled task, a menu appears where you can select this option, which pivots you from the **Schedules** tab to **Completed Tasks** tab by a particular schedule.

Completed Tasks

In the Completed Tasks tab in the Schedule Manager, you can work with completed scheduled tasks.

Table 11-3 describes the fields and buttons in the **Completed Tasks** tab of the Schedule Manager.

Table 11-3 Completed Task List Tab Fields and Buttons

Field or Button	Description
Task Name	Text box that allows you to filter the scheduled tasks by task name.
Creator	Text box that allows you to filter the scheduled tasks by creator.
Type	Drop-down box that allows you to filter the scheduled task by chart, report, or none.
Date Created	Drop-down box that allows you to filter the scheduled task by the date it was created.
Completed Date	Drop-down box that allows you to filter the scheduled task by the date it was completed.
Purge Date	Drop-down box that allows you to filter the scheduled task by its purge date.
Filter	Click this button to filter table by task name, creator, type (report or chart), date created, date completed, or purge date.

Table 11-3 Completed Task List Tab Fields and Buttons (continued)

Field or Button	Description
Refresh	Click this button to refresh the table after filtering it by a specific column name.
Task Name	Displays the name of the scheduled task. You can also sort by this column.
Creator	Displays the creator of the scheduled task. You can also sort by this column.
Type	Displays the type of scheduled task: Report or Chart. You can also sort by this column.
Date Created	Displays the date the scheduled task was created. You can also sort by this column.
Run Date	Displays the date the scheduled task was run. You can also sort by this column.
Purge Date	Displays the purge date of the scheduled task. You can also sort by this column.

Note You can configure the Run Date and Purge Date in the Path Analyzer User Preferences. For more information, please see Set Preferences, page 1-24.

CHAPTER 12

Web-Based Report Management

Accessing Generated Charts and Reports from the Web

Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) Web Schedule Manager allows you to view and manage charts and reports created in Schedule Manager via a Web browser. For information about generating charts and reports, see Chapter 9, “Generating Reports” and Chapter 10, “Generating Charts”.

In the Web Schedule Manager, you can select and view all tasks that were scheduled previously in the Path Analyzer Schedule Manager. Charts and reports that were not previously scheduled in Schedule Manager cannot be viewed, opened, or accessed in the Web Schedule Manager. (For information on scheduling, see Chapter 11, “Scheduling Reports and Charts”.)

The Web Schedule Manager is accessed with a Web browser on any computer with a connection to the Path Analyzer Server. You can log into the Web Schedule Manager locally or remotely to monitor the status of schedules and tasks, view charts and reports.

Web Schedule Manager Details

- Starting the Path Analyzer Web Schedule Manager, page 12-1
- Viewing Current Schedules and Completed Tasks, page 12-5
- Managing Schedules, page 12-7
- Managing Completed Tasks, page 12-13
- Manage Your Own Schedule and Tasks, page 12-19

Note Mozilla Firefox is the recommended browser for accessing the Web Schedule Manager. Microsoft Internet Explorer can also be used, but certain search elements function better in Firefox.

Starting the Path Analyzer Web Schedule Manager

The Web Schedule Manager is accessed with a Web browser.

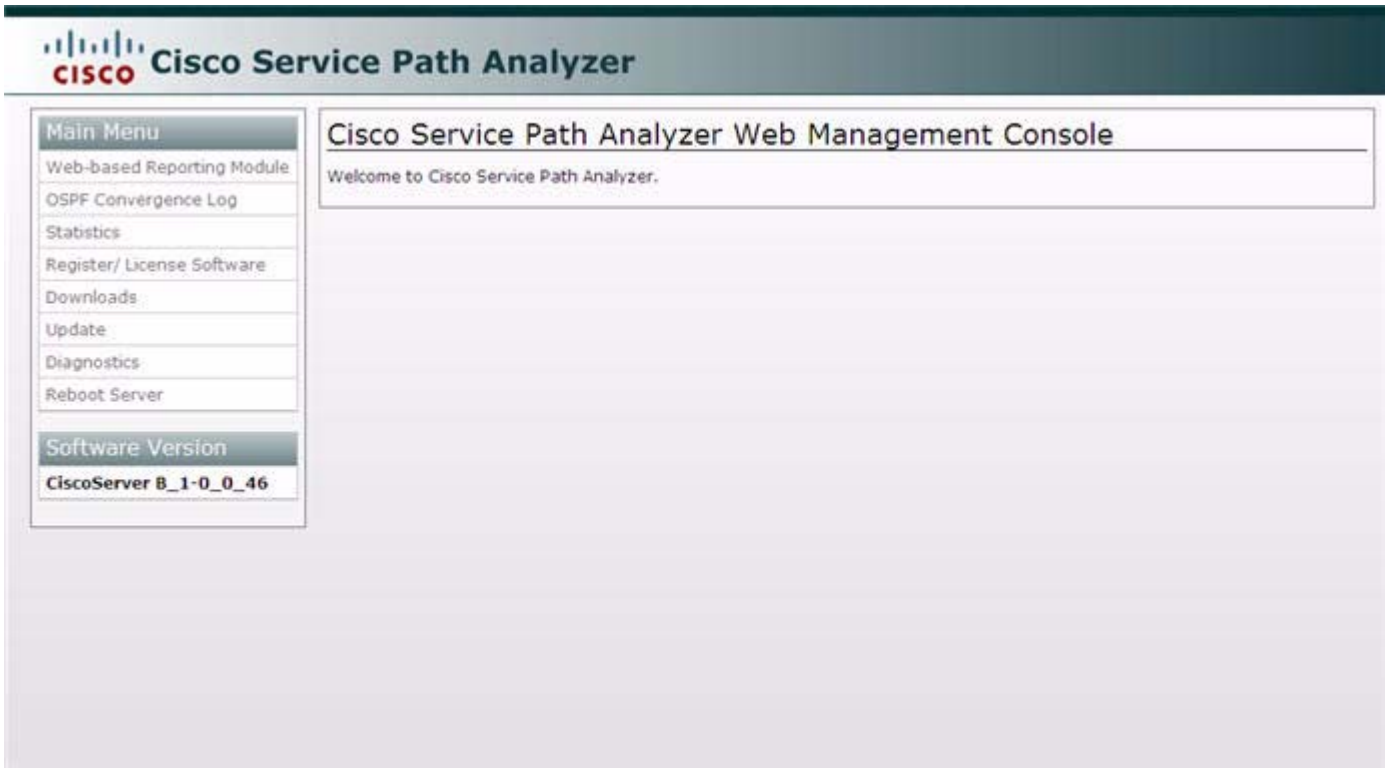
Start the Web Schedule Manager

To start the Web Schedule Manager:

Step 1 Enter the IP address of your Path Analyzer Server in the Locator or Address field of your web browser.

The Path Analyzer System Management Panel Main Menu appears (see Figure 12-1).

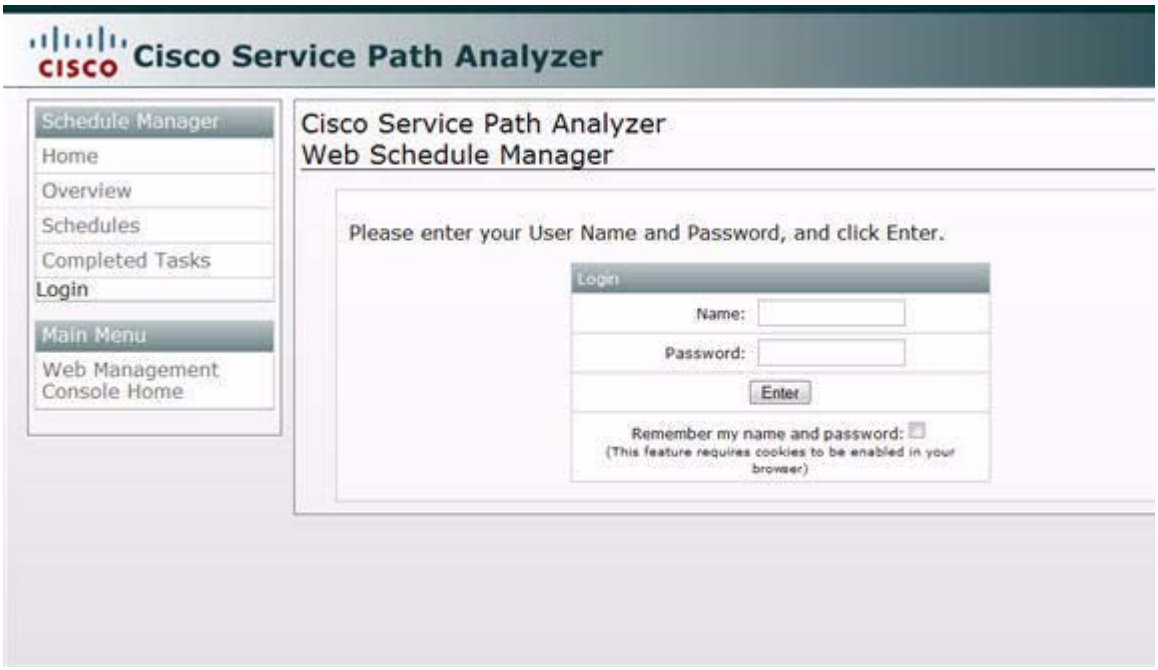
Figure 12-1 Main Menu



Step 2 Click **Web-based Reporting Module**.

The Web Schedule Manager window opens, showing the Login dialog box (see Figure 12-2).

Figure 12-2 Web Schedule Manager Login Screen



Step 3 Follow the procedure to Log In, page 12-3.

Log In

To log in to the Web Schedule Manager:

Step 1 Enter your user name in the **User Name** field.

Step 2 Enter your password in the **Password** field.

Step 3 (Optional) Click the **Remember my name and password** check box if you want the Web Schedule Manager to use your current name and password the next time you log in.

A check mark is displayed in the check box when this option is selected, indicating that your user name and password are stored for further logins.

Note Your user name and password are case sensitive.

The **Remember my name and password** option requires that cookies are enabled in your web browser.

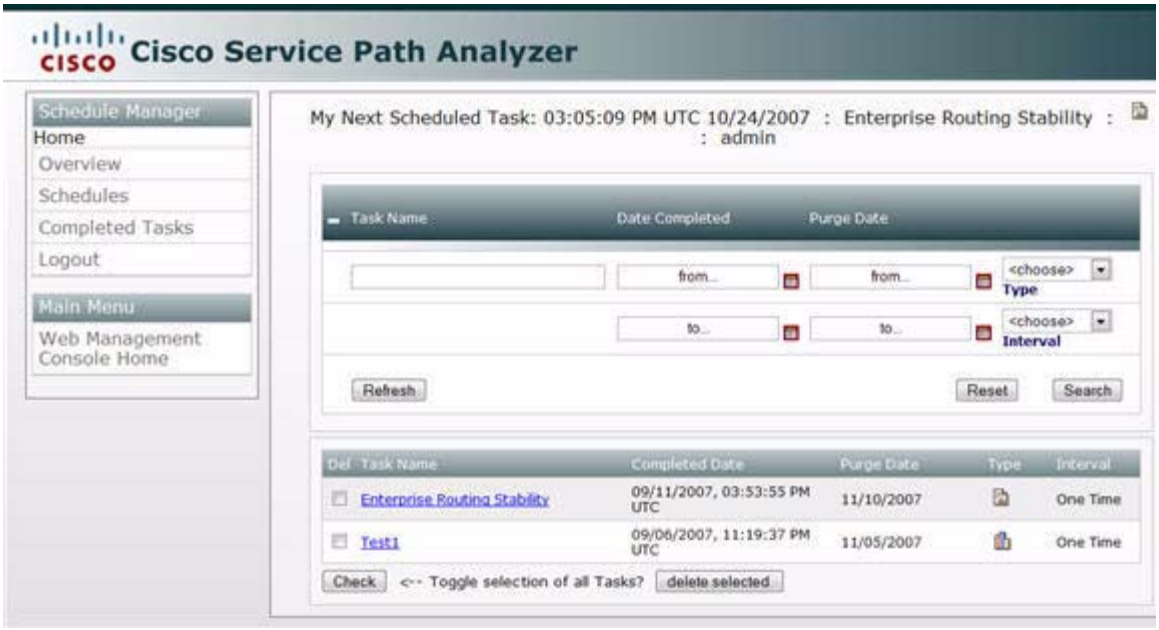
Step 4 Click **Enter** to log in to the Web Schedule Manager.

The Home Page appears, showing the charts associated with tasks you previously created and scheduled in Path Analyzer Schedule Manager.

Home Page

In the Home Page (see Figure 12-3), you can view your completed tasks, navigate to see all schedules and completed tasks, and open the charts or reports associated with a task. See Manage Your Own Schedule and Tasks, page 12-19 for more information on working with your schedules and tasks.

Figure 12-3 Home Page in Web Schedule Manager



Log Out

To log out of the Web Schedule Manager, select **Logout** from the navigational menu.

Navigating in the Web Schedule Manager

The Web Schedule Manager provides a navigational menu from which you can access different Schedule Manager screens. Clicking on a menu selection takes you to a screen in which you can manage schedules and completed tasks.

Pages of the Web Schedule Manager include:

- Home Page, page 12-4—Displays your completed tasks and provides options for managing the schedules you created in Schedule Manager.
- Overview Page, page 12-5—Displays the schedules that all authorized users created in Path Analyzer Schedule Manager, as well as the number of each user's scheduled and completed tasks. For an explanation of the difference between a schedule and a task, see Managing Scheduled Tasks with Path Analyzer Schedule Manager, page 11-1.
- Schedules Page, page 12-9—Displays detailed information about all schedules that were previously created in Path Analyzer Schedule Manager. You can search for specific schedules and delete schedules in this screen.

- Completed Tasks Page, page 12-15—Displays detailed information about all tasks that have been completed. In this screen, you can search for specific completed tasks to view and delete.

Note The same icon is used to represent basic and advanced charts in the pages of the Web Schedule Manager.

Viewing Current Schedules and Completed Tasks

Use the Web Schedule Manager to view details about schedules and tasks that were previously created in Path Analyzer Schedule Manager. For information about creating schedules and tasks in Path Analyzer Schedule Manager, see Scheduling Reports and Charts, page 11-1.

View Scheduling Information of All Users

The Overview screen of the Web Schedule Manager provides information about:

- Date, time, and report or chart name of each user's next task scheduled to run.
- Number of schedules created by each user.
- Number of completed tasks belonging to each user.

Overview Page

To access the Overview page:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears.

Step 2 Click on **Overview** in the navigational menu.

The Overview Page, page 12-5 appears (see Figure 12-4).

Figure 12-4 Overview Screen in Web Schedule Manager

Step 3 Locate a user to view his or her:

- Next scheduled task (name, date, and time).
- Number of exiting schedules.
- Number of tasks that have been completed.

View a User's Schedules

To view a user's schedules in the Overview screen, click the numerical link in the Schedules field, or click the **Schedules** link in the navigational menu to view a user's existing schedules.

The Schedules Page, page 12-9 appears, showing all of the user's schedules that were previously created in Path Analyzer Schedule Manager. For more information on schedules, see Managing Schedules, page 12-7.

View a User's Completed Tasks

To view a user's completed tasks in the Overview screen, click the numerical link in the Completed Tasks field, or click the **Completed Tasks** link in the navigational menu to view all of a user's completed tasks.

The Completed Tasks Page, page 12-15 appears, showing all of the user's completed tasks. For more information on completed tasks, see Managing Completed Tasks, page 12-13.

Refresh Page Values

To update the display of information in the Schedules Page, Completed Tasks Page, and Home Page of the Web Schedule Manager, click the **Refresh** button.

Managing Schedules

The Schedules Page, page 12-9 in the Web Schedule Manager displays a list of existing schedules that were created in Path Analyzer. In this screen, you can filter schedules based on the following criteria:

- Schedule name
- User name of the creator
- Start date
- End date
- Next date the schedule will run a task
- Type of entity to be generated, for example, a chart or report
- Schedule's interval

View Schedules

To view schedules in the Web Schedule Manager:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears.

Step 2 Click on the **Schedules** link in the navigational menu.

The Schedules page appears showing the schedules for all configured users (see Figure 12-5).

Figure 12-5 Schedules Screen in Web Schedule Manager

In the Schedules screen, you can view the:

- Name of the scheduled report or chart.
- Creator of the chart.
- Number of iterations in a schedule.
- End date of a schedule.
- Date for the next scheduled task to run.
- Type of schedule—whether it's a report or chart. Note that charts and advanced charts display using the same icon.
- Interval of the schedule.

Note The Schedules table can be sorted by clicking on each of the respective column heads. For example, to sort schedules by end date, click the End Date column head.

View Completed Tasks from the Schedules Screen

In the **Schedule Name** field of the Schedules screen, click the link of a schedule to view its related tasks.

The Completed Tasks Page, page 12-15 appears, showing all of the schedule's completed tasks. For more information on the Completed Tasks screen, see View Generated Charts or Reports in the Completed Tasks Screen, page 12-13.

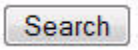
View a User's Schedules

To view a user's schedules:

Step 1 Select the user name of the user whose schedules you want to view from the Creator drop-down box in the Schedules Page, page 12-9.

Note To search for schedules by their creator when using Web Schedule Manager with Internet Explorer, you must also select the Type of schedule, either Chart or Report.

Step 2 Click the **Search** button.



The Schedules Page, page 12-9 displays, showing all of the schedules the selected user created.

Step 3 Click the schedule's name in the Schedule Name field if you want to view the tasks related to a schedule.

The Completed Tasks Page, page 12-15 appears, showing all tasks related to the selected schedule.

Search for Schedules

This section contains information about searching for schedules:

- Schedules Page, page 12-9
- Select Schedule Search Parameters, page 12-10

Schedules Page

To search for schedules from the Schedules page:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears.

Step 2 Select **Schedules** from the navigational menu.

The Schedules Page, page 12-9 appears. For more information on the Schedules screen, see Figure 12-5.

Step 3 Follow the procedure to Select Schedule Search Parameters, page 12-10 in the search form section at the top of the Schedules page. By entering data in or selecting options from the appropriate fields, you can:

- Search by Schedule Name, page 12-10
- Search by Creator, page 12-10
- Search by Date Completed, page 12-10
- Search by Purge Date, page 12-11
- Search by Type, page 12-11
- Search by Interval, page 12-11

Step 4 Click the **Search** button.

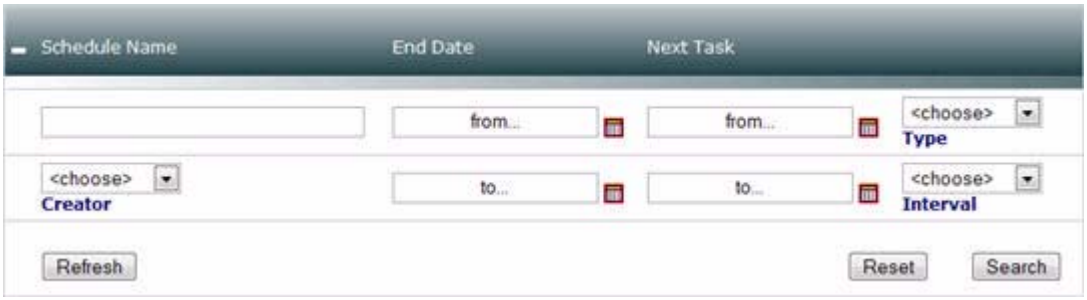
Search

Your search results are displayed in the table below the search form.

Select Schedule Search Parameters

Search parameters for searching schedules are selected in the gray box in the top part of the Schedules Page, page 12-9, as shown in Figure 12-6.

Figure 12-6 Search Schedules Box in Web Schedule Manager



Note When using Web Schedule Manager with Internet Explorer, most of the search fields must be used in conjunction with other search fields to yield results. The additionally required search fields for IE are noted below. If you are using Firefox, you can search on any individual parameter, without entering additional information in other fields.

Search by Schedule Name

To search for schedules by schedule name, enter the name of the schedule to locate in the Schedule Name field. You do not have to enter the full name of the schedule, just a string from the name. For example, if you are searching for the OSPF (Non-External) Advertisement Hotspot Analysis schedule, entering "OSPF" will yield the correct result.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator and Type fields.

Search by Creator

To search for schedules by creator, enter the user name of the user who created the schedule in the Creator field.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Type field.

Search by Date Completed

To search for schedules by the date they were completed:

Step 1 Click the calendar icon and select the start date in the from... section of the End Date field, for the search range of the schedule's end date.

Step 2 Click the calendar icon and select the end date in the to... section of the End Date field, for the search range of the schedule's end date.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator and Type fields.

Search by Purge Date

To search for schedules by their purge date:

Step 1 Click the calendar icon and select the start date and time in the from... section of the Next Task field, for the search range of when the next task you are searching for will run.

Step 2 Click the calendar icon and select the end date and time in the to... section of the Next Task field, for the search range of when the next task you are searching for will run.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator and Type fields.

Search by Type

To search for schedules by their type, select one of the following options in the Type field:

- **Chart**—Select this option if you are searching for scheduled charts.
- **Report**—Select this option if you are searching for scheduled reports.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator field.

Search by Interval

To search for schedules by their interval, select one of the following options in the Interval field:

- **One Time—**Select this option if the task is scheduled to occur only once.
- **Daily—**Select this option if the task is scheduled to occur daily.
- **Weekly—**Select this option if the task is scheduled to occur weekly.
- **Monthly—**Select this option if the task is scheduled to occur monthly.
- **End of Month—**Select this option if the task is scheduled to occur at the end of every month.
- **Yearly—**Select this option if the task is scheduled to occur annually.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator and Type fields.

Reset Search Fields

To reset search fields click the **Reset** button in the Schedules Page, Completed Tasks Page, or Home Page.

The values in the fields of the search form section are cleared.

Delete Schedules

When deleting schedules, you can:

- Delete One or More Schedules, page 12-12
- Delete All Schedules, page 12-12

Delete One or More Schedules

To delete one or more schedules:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears.

Step 2 Select **Schedules** from the navigational menu.

The Schedules Page, page 12-9 appears.

Step 3 Select the schedules you want to delete by clicking their check boxes in the Del column of the Schedules Page.

A check mark is displayed in the check box of each selected schedule.

Step 4 Click the **delete selected** button.

The selected schedules are removed from the Schedules Page.

Note When you delete a schedule from the Web Schedule Manager, it is also deleted from the Path Analyzer Schedule Manager.

Delete All Schedules

To delete all schedules in Path Analyzer:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears.

Step 2 Select **Schedules** from the navigational menu.

The Schedules Page, page 12-9 appears.

Step 3 Click the **Check** button next to <--Toggle selection of all tasks?

A check mark is displayed in the Del column check boxes for all listed schedules.

Step 4 Click the **delete selected** button.

All schedules are removed from the Schedules Page.

Managing Completed Tasks

In Completed Tasks page of the Web Schedule Manager, you can filter completed tasks by the following criteria:

- Task name
- User name of the creator
- Completion date of the task
- Purge date of the task (when the generated chart or report is removed from Path Analyzer)
- Type of entity to be generated (chart or report)
- Interval of the schedule (on time, daily, weekly, monthly, end of month, or annually)

View Generated Charts or Reports in the Completed Tasks Screen

From the Completed Tasks screen, you can view the chart or report associated with a completed task.

View a Chart or Report

To view a chart or report in Web Schedule Manager:

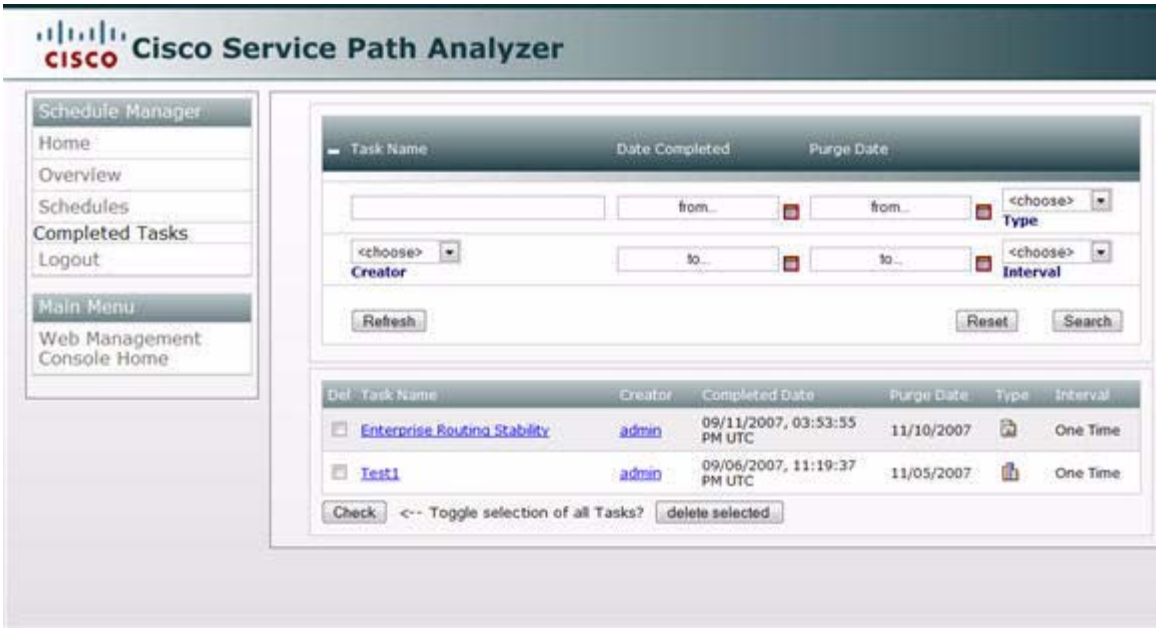
Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears.

Step 2 Select **Completed Tasks** in the navigational menu.

The Completed Tasks Page, page 12-15 appears (see Figure 12-7).

Figure 12-7 Completed Tasks Screen in Web Schedule Manager



Step 3 In the Task Name column of the table displaying completed tasks:

- Click the link of the chart task you want to view.

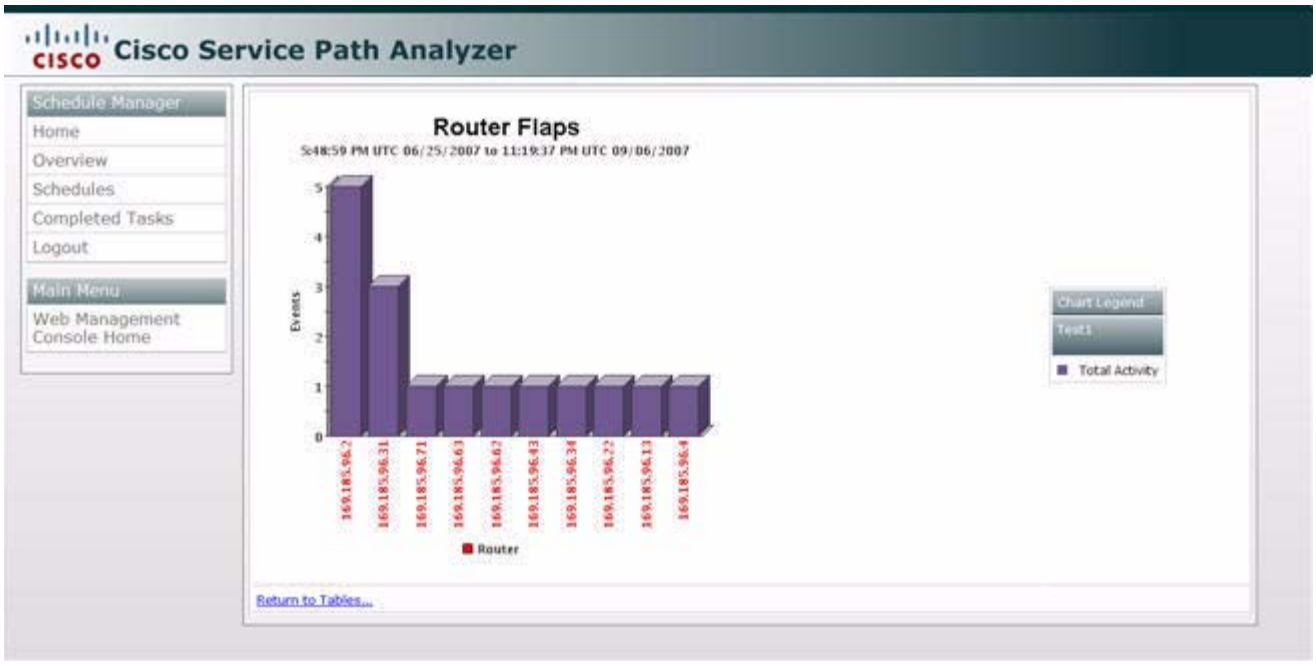
  The Chart Details page appears, showing the chart that was generated from the scheduled task.

or

- Click the link of the report task you want to view.

  The Report Details page appears, showing the report that was generated from the scheduled task (see Figure 12-8).

Figure 12-8 Chart Detail Screen in Web Schedule Manager



Search for Completed Tasks

You can use the Search Form on the Completed Tasks screen to find a completed task.

Completed Tasks Page

To search for completed tasks from the Completed Tasks page:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears.

Step 2 Select **Completed Tasks** in the navigational menu.

The Completed Tasks Page, page 12-15 appears. See Figure 12-7 for more information.

Step 3 In the Search Form section of the Completed Tasks Page, follow the procedure to Select Task Search Parameters, page 12-16. You can:

- Search by Task Name, page 12-16
- Search by Task Creator, page 12-16
- Search by Date Completed, page 12-16
- Search by Purge Date, page 12-17
- Search by Type, page 12-17
- Search by Interval, page 12-17

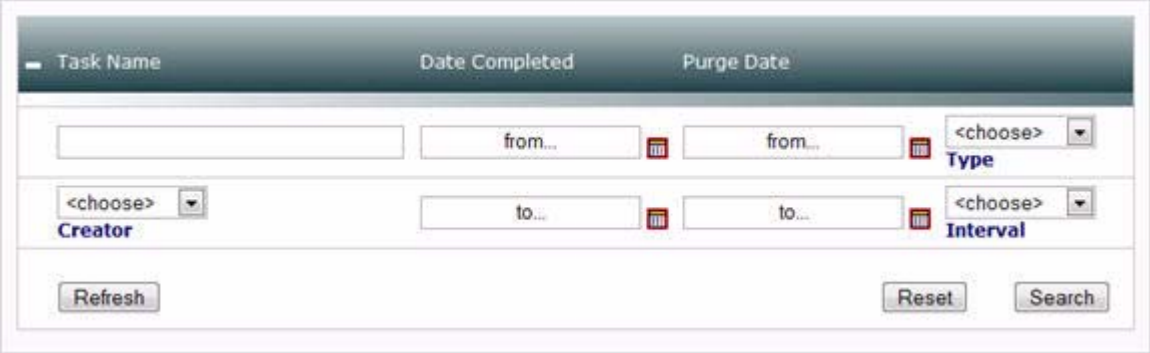
Step 4 Click **Search**.

Search results are displayed on the Completed Tasks page. You can Reset Search Fields at any time and enter new values to view different data.

Select Task Search Parameters

Search parameters for searching tasks are selected in the top box in the top part of the Completed Tasks Page (see Figure 12-9).

Figure 12-9 Search Tasks Box in Web Schedule Manager



Note When using Web Schedule Manager with Internet Explorer, most of the search fields must be used in conjunction with other search fields to yield results. The additionally required search fields for IE are noted below. If you are using Firefox, you can search on any individual parameter, without entering additional information in other fields.

Search by Task Name

To search by task name, enter the name of the task to locate in the Task Name field. You do not have to enter the full name of the task, just a string from the name. For example, if you are searching for the OSPF (Non-External) Advertisement Hotspot Analysis schedule, entering “OSPF” yields the correct result.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator and Type fields.

Search by Task Creator

To search by task creator, enter the user name of the user who scheduled the task in the Creator field.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Type field.

Search by Date Completed

To search by date completed:

Step 1 Click the calendar icon and select the start date in the from... section of the Date Completed field, for the search range of the schedule’s end date.

Step 2 Click the calendar icon and select the end date in the to... section of the Date Completed field, for the search range of the schedule's end date.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator and Type fields.

Search by Purge Date

To search by purge date:

Step 1 Click the calendar icon to select the start date of the search range in the from... section of the Purge Date field, for when the completed task will be removed from Path Analyzer.

Step 2 Click the calendar icon and select the end date of the search range in the to... section of the Purge Date field, for when the completed task will be removed from Path Analyzer.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator and Type fields.

Search by Type

To search by type, select one of the following options in the Type field:

- **Chart**—Select this option if you are searching for completed tasks that generated a chart.
- **Report**—Select this option if you are searching for completed tasks that generated a report.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator field.

Search by Interval

To search by interval, select one of the following options in the Interval field:

- **One Time—**Select this option if the task was scheduled to occur one time.
- **Daily—**Select this option if the task was scheduled to occur daily.
- **Weekly—**Select this option if the task was scheduled to occur weekly.
- **Monthly—**Select this option if the task was scheduled to occur monthly.
- **End of Month—**Select this option if the task was scheduled to occur at the end of every month.
- **Yearly—**Select this option if the task was scheduled to occur annually.

When using Web Schedule Manager with Internet Explorer, this field must be used in conjunction with the Creator and Type fields.

Reset Task Search Fields

To reset search fields in the Completed Tasks Page, page 12-15, click the **Reset** button.

The values in the fields of the search form section are cleared.

Delete Completed Tasks

If you want to delete tasks, you can:

- Delete One or More Completed Tasks, page 12-18
- Delete All Completed Tasks, page 12-18

Delete One or More Completed Tasks

To delete one or more completed tasks:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears.

Step 2 Select **Schedules** from the navigational menu.

The Completed Tasks Page, page 12-15 appears.

Step 3 Select the tasks you want to delete by clicking their check boxes In the Del column of the Completed Tasks page.

A check mark is displayed in the check box of each selected task.

Step 4 Click the **delete selected** button.

The selected tasks are removed from the Completed Tasks page.

Note When you delete a completed task from the Web Schedule Manager, it is also deleted from the Path Analyzer Schedule Manager.

Delete All Completed Tasks

To delete all completed tasks:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears.

Step 2 Select **Completed Tasks** from the navigational menu.

The Completed Tasks Page, page 12-15 appears.

Step 3 Click the **Check** button next to **<--Toggle selection of all tasks?**

A check mark is displayed in the **Del** column check boxes for all listed tasks.

Step 4 Click the **delete selected** button.

All tasks are removed from the Schedules Page.

Manage Your Own Schedule and Tasks

In Web Schedule Manager, you can view and manage all of the schedules and tasks you previously created in the Path Analyzer Schedule Manager.

View Your Tasks

You can view your next scheduled task, as well as your completed task details.

View Your Next Scheduled Task

To view your next scheduled task:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears. The top of the page shows the report or chart that is generated when your next scheduled task runs (see Figure 12-10).

Figure 12-10 Next Scheduled Task in Schedules Screen of Web Schedule Manager

Step 2 View the following information in the My Next Scheduled Task field:

- Date the task is scheduled to run
- Name of the task
- Type of task (chart or report)
- User name of the creator of the task

View Your Completed Task Details

To view your completed task details:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears, with your completed tasks shown in the table.

Step 2 Click the name of the task in Task Name column of the table to view its generated chart or report.

The related chart or report is displayed in the browser. For an example of a chart detail display, see Figure 12-8.

Search for Your Schedules

When viewing your schedules, you can search for a specific schedule.

View Your Schedules

To view your schedules:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears. The top of the page shows the charts and graphs that are generated when your next scheduled task runs.

Step 2 Click the **Schedules** link in the navigational menu.

Step 3 Select your user name from the Creator drop-down box in the search form box at the top of the Schedules screen.

When using Web Schedule Manager with Internet Explorer, you must also select the type of schedule from the Type field.

Step 4 Click the **Search** button.

Your schedules are displayed.

Search for Your Tasks

When viewing your tasks, you can search for a specific task.

View Your Tasks

To search for your tasks:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears. The top of the page shows the charts and graphs that are generated when your next scheduled task runs.

Step 2 Click in the **Completed Tasks** link in the navigational menu.

Step 3 Select your user name from the **Creator** drop-down box in the search form box at the top of the Completed Tasks screen.

When using Web Schedule Manager with Internet Explorer, you must also select the type of schedule from the Type field.

Step 4 Click the **Search** button.

Your completed tasks are displayed.

Reset Search Values

To reset search values in the Schedules Page, Completed Tasks Page, or Home Page, click the **Reset** button.

The values in the fields of the search form section are cleared.

Delete Your Schedules and Tasks

You can perform the following removals:

- Delete Your Schedules, page 12-21
- Delete Your Completed Tasks, page 12-21

Delete Your Schedules

To delete your schedules:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

The Home Page, page 12-4 of the Web Schedule Manager appears. The top of the page shows the charts and graphs that are generated when your next scheduled task runs.

Step 2 Click the **Schedules** link in the navigational menu.

Step 3 Select your user name from the Creator drop-down box in the search form box at the top of the Schedules screen.

When using Web Schedule Manager with Internet Explorer, you must also select the type of schedule from the Type field.

Step 4 Click the **Search** button.

Your schedules are displayed.

Step 5 Select the check box of the schedule you want to delete, or click the **Check** <-- Toggle selection of all Tasks? button to select all schedules.

Step 6 Click the **delete selected** button.

For more information, see Delete Schedules, page 12-12.

Delete Your Completed Tasks

To delete your completed tasks:

Step 1 Follow the procedures to Start the Web Schedule Manager, page 12-2 and Log In, page 12-3.

Step 2 The Home Page, page 12-4 of the Web Schedule Manager appears. The top of the page shows the charts and graphs that are generated when your next scheduled task runs.

Step 3 Click the **Completed Tasks** link in the navigational menu.

Step 4 Select your user name from the **Creator** drop-down box in the search form box at the top of the Completed Tasks screen.

When using Web Schedule Manager with Internet Explorer, you must also select the type of schedule from the Type field.

Step 5 Click the **Search** button.

Your completed tasks are displayed.

Step 6 Select the check box of the completed task you want to delete, or click the **Check <-- Toggle selection of all Tasks?** button to select all schedules.

Step 7 Click the **delete selected** button.

For more information, see Delete Completed Tasks, page 12-18.

CHAPTER 13

Replaying Your Network's History

Watching Historical Events Replay

Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) Listeners collect BGP routing messages and OSPF Link State Advertisements (LSAs) from adjacent routers on your network.

After receiving routing messages from Listeners, the Path Analyzer Server processes them and generates events—notifications with descriptions of changes that occur on your network—and maintains them in a database. Maintaining this information ensures that you can safeguard your network history and review it at a later date.

Each routing message provides one or more events, which include:

- Changes to the visual topology of your network, presented in the Topology Viewer.
- Changes to services that carry business-critical data across your network, shown in Service Monitor.
- Attributes of and changes to network elements, including autonomous systems, areas, routers, and routes, presented in the Topology Browser.
- Additions, withdrawals, and changes to routers, routes, and links, which are displayed in the Event Log.
- Changes to Path Analyzer labels for your network, and the autonomous systems and routing domains that make up the network, shown in the Domain Administration module.

During a historical session, you can replay the events, open Path Analyzer modules, and watch changes that occurred previously in your network.

Uses for Replaying Events

Viewing the replay of historical events may help with:

- Discovering the root cause of a past issue.
- Identifying or monitoring a problem by comparing a past sequence of events to a similar, current sequence.
- Determining future requirements.

Full Use of Path Analyzer Modules

The following Path Analyzer modules are available during historical sessions:

- Topology Viewer
- Service Monitor
- Real Time and Investigative Topology Browser
- Event Log
- Domain Administration

As the historical session plays, you can start any of these modules and watch the historical sequence replay within them.

Viewing Past Events: Like Watching a Movie

Viewing the replay of past events in a Path Analyzer module is like watching a movie. At the start of the movie, the module displays conditions as they existed at the start of the historical session. As the movie plays, you watch the events unfold in the exact manner and sequence that they occurred.

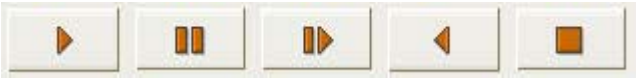
For example, when running the sequence of past events from the Topology Viewer, you watch as previous changes to your network topology recur. Automatically, you can view any additions or deletions of routers to your network, changes to IP addresses, links changing from red to green (indicating that a link changed from being unavailable to being available), and other events that occurred within the period of time. With the Event Log open while a historical session is playing, you can watch events populate the log, and change in severity.

Like Using a Media Player

The Historical Session provides a set of user controls similar to those on a tape recorder, VCR, or online media player (see Figure 13-1). These controls allow you to play, step forward through, pause, or stop the historical sequence of events.

The Path Analyzer historical sessions provide a wizard that guides you in selecting autonomous systems, routing domains, specific routers, and services to narrow the scope of historical data to be replayed.

Figure 13-1 Historical Session Controls



Historical Session Tasks

- Starting a Historical Session, page 13-3
- Using Controls of Historical Sessions, page 13-7
- Navigating Between Historical Sessions and the Realtime Console, page 13-8
- Analyzing Previous Network Conditions, page 13-11

Starting a Historical Session

Using the Historical Session wizard, you can select autonomous systems, routing domains, and services to view during the historical session. As the historical session unfolds, you watch the changes that were made previously, including the addition of new routers to an area, an OSPF routing domain, changes in the availability of service paths, and other past events.

Start a Historical Session

To start an historical session:

Step 1 Select **Start** > **Historical Session**.

The Historical Session wizard appears. If it is the first time you are creating a historical session while logged in to Path Analyzer, the Historical Session Wizard Welcome Screen appears. You can choose to view the Welcome Screen only once by selecting the appropriate check box, and clicking **Next**.

Step 2 The Select an Autonomous System, page 13-3 screen displays a hierarchy of autonomous systems and routing domains.

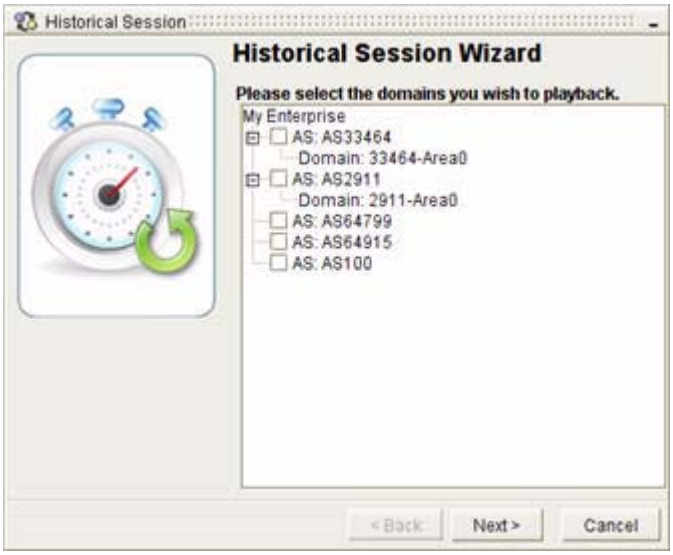
Select an Autonomous System

To select an autonomous system for an historical session:

Step 1 Select one or more autonomous systems you want to return to a previous historical state in the Select Domains screen (see Figure 13-2).

After selecting an autonomous system, a check mark is displayed in its check box.

Figure 13-2 Select Autonomous Systems Screen in Historical Session Wizard



Note Selecting autonomous systems narrows the amount of data returned and reduces the amount of bandwidth and processing power used by the Path Analyzer Server to retrieve the requested data and by the Management Console to present it. The fixed set of data returned allows you to view and analyze a smaller and more specific set of information.

Step 2 Click **Next**.

The Select a Period of Time, page 13-4 wizard screen appears, in which you can complete one of the following tasks:

Set a Predefined Period of Time, page 13-5

or

Customize a Period of Time, page 13-5

Select a Period of Time

In the Select a Start Time screen you can select a predefined or customized period of time (see Figure 13-3). When a start time is selected, the Historical Session wizard generates a historical session that runs from the start time to the current time.

Figure 13-3 Select Start Time Screen in Historical Session Wizard

Set a Predefined Period of Time

To set a predefined period of time for an historical session:

Step 1 Select one of the following options:

- **Today—**Selects events generated from routing updates that occurred today.
- **Yesterday—**Selects events generated from routing updates that occurred yesterday.
- **Last Week—**Selects events generated from routing updates that occurred last week.
- **Last Month—**Selects events generated from routing updates that occurred last month.
- **Last Year—**Selects events generated from routing updates that occurred last year.
- **Complete History**—Selects events generated from all routing updates over the full historical range (from the time that an entity became available on the network until the current date and time).

Step 2 Click **Next**.

The Select Services wizard page appears, in which you can Select Services to View Historically, page 13-6.

Customize a Period of Time

To customize a period of time for your historical session:

Step 1 Set the start date of the time period to be customized by clicking the **Custom** radio button.

Step 2 Click the down arrow of the Custom drop-down menu.

The calendar dialog box appears, containing the year and month, a calendar, and fields to set the time.

Step 3 Scroll to the year in the year scroll box in which you want the historical session's start date to occur.

Step 4 Scroll to the month in the month scroll box in which you want the historical session's start date to occur.

Step 5 Select the hour, minute, second, and AM or PM options for the start time of the historical session under the calendar.

Step 6 Click on the day you want the historical session to begin in the calendar.

Step 7 Clicking on a date closes the calendar.

Step 8 Click **Next**.

The Select Services wizard page appears, in which you can Select Services to View Historically, page 13-6.

Select Services to View Historically

Figure 13-4 Select Services Screen in Historical Session Wizard

To select the services to view in your historical session:

Step 1 Select a service from the Current Services field by clicking on it in the Select Services screen (see Figure 13-4).

Step 2 Click the Right Arrow (**>>**) to move the selected service into the Services To Import List.

Selecting services and moving them into the **Services to Import** field includes them in the historical session. When you start Service Monitor in the historical session, you can watch as changes occur that affect your selected services.

Step 3 Click **Next**.

The Historical Session wizard generates your historical session. Depending on the parameters selected and the size of your database, it may take several minutes to generate the historical session. When the session has been generated, the **Finish** button becomes available (see Figure 13-5).

Step 4 Click **Finish**.

Figure 13-5 Finish Screen in Historical Session Wizard

Once the system is finished generating the historical session, the Path Analyzer system resets your network environment to conditions as they existed during the specified period of time. For example, if the historical time period starts at 9 AM, Path Analyzer restores the system and Management Console to the historical state that existed on the selected date, just before 9 AM.

Using Controls of Historical Sessions

The buttons of the historical player enable you to play, pause, restart, step forward through, and stop a historical session. Table 13-1 describes each control.

The Historical Session controls are displayed in a toolbar under the Path Analyzer menu bar. Using the controls, you can play, stop, restart, step forward, or pause a historical sequence.

When you click the **Play** button, the historical sequence is replayed, and the Path Analyzer Management Console is set to the historical session. You can Start a Module in a Historical Session, page 13-11 to view persisted routing events as they are replayed in the Topology Viewer or Topology Browser, Event Log, or Service Monitor in your Path Analyzer Management Console.

Note All active historical session controls are displayed as red on a gray field. When buttons are active, you can click them to complete an action. Inactive historical session controls are displayed as dark gray on a gray field. When you click an inactive button, its associated action does not occur.

Table 13-1 Historical Session Controls

Click this button...	To complete this action...
	Starts to play the stream of historical events. Playing the historical session causes the Path Analyzer Server to restore and replay the set of events that were generated from historical routing updates persisted in the database.
	Pauses the stream of routing events until you click Play again.

Table 13-1 Historical Session Controls (continued)

Click this button...	To complete this action...
	Steps forward through portions of the historical sequence when no events were generated from routing messages. Replays the sequence from the point when events were generated again.
	Opens the Historical Session Restart wizard, in which you can select the same or a new set of services to run. Selecting a new set of services restarts the historical session from the beginning.
	Stops the stream of routing events from playing.

Set the Delay Between Routing Update Messages

While viewing a historical session, you can change the delay, in milliseconds, between routing update messages. However, you can only change the delay while your historical session is stopped or paused.

Step 1 Follow the procedure to Start a Historical Session, page 13-3. See Using Controls of Historical Sessions, page 13-7 for more information.

Step 2 Select the number of milliseconds to delay the historical session between routing update messages in the **Delay (ms)** field of the historical session controls.

If your session is currently playing, click the Pause button to activate the Delay (ms) field.

Navigating Between Historical Sessions and the Realtime Console

In addition to the realtime view of your Management Console, Path Analyzer allows you to run and switch between five simultaneous historical sessions. Using the Context Switcher feature, you can create historical sessions linked by entities or events, or set up independent, unrelated historical sessions.

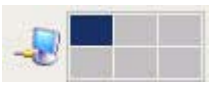
For example, to compare changes that affected a service at different times during a week, you can set up two or three historical sessions with different start times but replaying the same service selection. Or, you can set up one historical session to analyze the availability of routers, and a second to analyze event groups.

Using the Context Switcher to Switch Sessions

The taskbar contains a rectangular Context Switcher in the bottom right corner of your screen, divided into six squares. Clicking on a square toggles the Path Analyzer window to the session the square represents.

The upper left square in the Context Switcher represents your Path Analyzer realtime Management Console. In Figure 13-6, the user is currently in a realtime session:

Figure 13-6 Context Switcher with Realtime Session Selected



In Figure 13-7, the Context Switcher displays that the user is currently in the first generated historical session, and can switch back to the realtime Management Console by clicking the top left square.

Figure 13-7 Context Switcher with First Historical Session Selected

When in the realtime Management Console, clicking on the top middle square changes your view to the first historical session. The subsequent historical sessions are represented by each square going clockwise, in the order they were generated, as shown in Figure 13-8.

Figure 13-8 Context Switcher to Switch Between Sessions

Select a Module Window

The **Windows** menu at the top left of your Path Analyzer screen allows you to switch between specific modules in different historical and realtime sessions.

Select a Realtime Module Window From a Historical Session

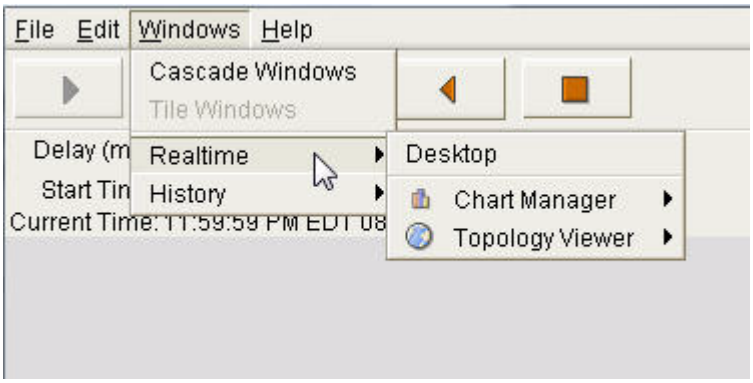
In the Path Analyzer menu bar as shown in Figure 13-9:

- Click **Windows > Realtime > Desktop** to run the selected realtime view of the Management Console.

or

- Click **Windows > Realtime > <module>** where <module> is replaced by the name of the Path Analyzer module. The selected module window appears in front of all other open windows.

Figure 13-9 Select a Realtime Window from Historical Session



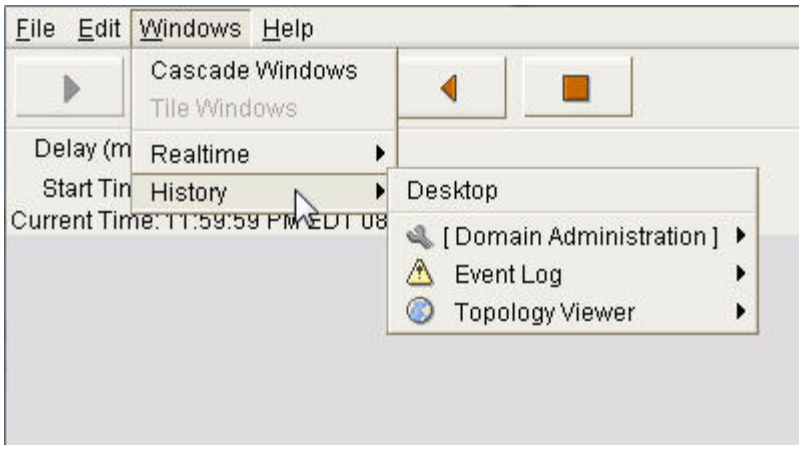
Select a Historical View of a Module

- Click **Windows > History** to run the selected historical view of the Management Console.

  or

- Click **Windows > History > <module>** where <module> is replaced by the name of the Path Analyzer Management Console module. For example, **Windows > History > Event Log** to switch to the historical session's open Event Log. Windows that have minimized appear in brackets, such as **Domain Administration** in Figure 13-10.

Figure 13-10 Select a Module in Historical Session



Analyzing Previous Network Conditions

After initializing a historical session, you can review previous network conditions by starting the Path Analyzer Topology Viewer, Topology Browser, Event Log, Service Monitor, and Domain Administration modules.

Start a Module in a Historical Session

To start a module in an historical session:

Step 1 Follow the procedure to Start a Historical Session, page 13-3.

Step 2 Click the Play button to start replaying historical events in the History Player.

See Using Controls of Historical Sessions for information about starting, stopping, restarting, and stepping forward through the sequence.

Step 3 Click the **Start** button In the Path Analyzer taskbar.

The Start menu appears.

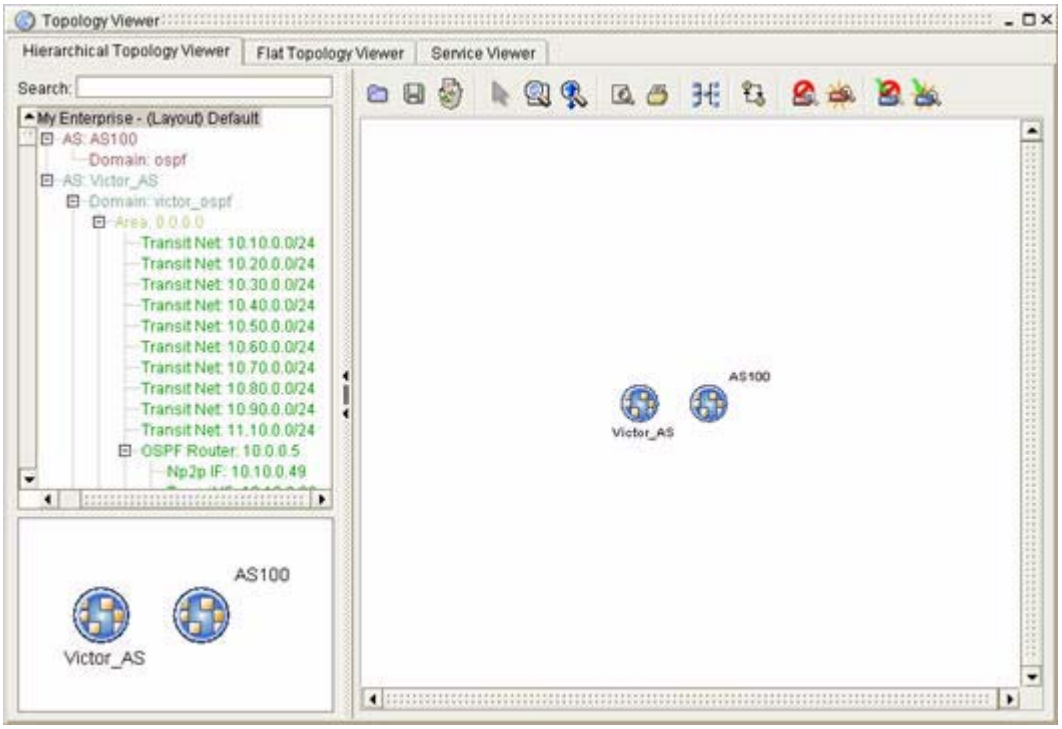
Step 4 Select one of the following modules from the menu:

- **Topology Viewer**
- **Service Monitor**
- **Topology Browser** > **Real Time** or **Topology Browser** > **Investigative**
- **Event Log**
- **Domain Administration**

The historical view of the module opens in the Path Analyzer Management Console. In addition to modules, you can select **Preferences** to change time formats, and you can obtain **Help**. See Set Preferences, page 1-24 and Using Help, page 1-36.

Review the Historical Topology

Figure 13-11 Topology Viewer in Historical Session



To review the historical topology:

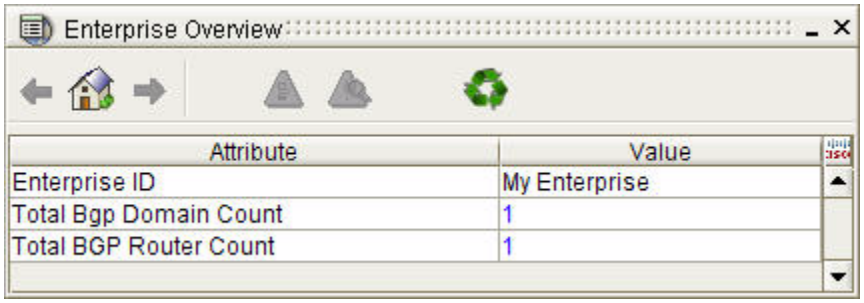
Step 1 Start the Topology Viewer during the historical session (see Figure 13-11) by selecting **Start > Topology Viewer**. See the procedure to Start a Module in a Historical Session, page 13-11 for more information.

Step 2 Scroll through the Topology Viewer and identify significant changes in the **Hierarchical Topology Viewer** tab, the **Flat Topology Viewer** tab, or the **Service Viewer** tab.

Step 3 Right-click a topology element and make a selection from the popup menu to obtain information about the topology element. See Viewing Metrics and Attributes, page 2-54 for more information on using the Topology Viewer.

Step 4 Start the historical Topology Browser by selecting **Start > Topology Browser > Real Time**. Click through Topology Browser dialog boxes to view information related to the selected topology element (see Figure 13-12). See Navigating in Topology Browser Dialog Boxes, page 2-48 for more detailed information on using the Real Time Topology Browser.

Figure 13-12 Real Time Topology Browser in Historical Session

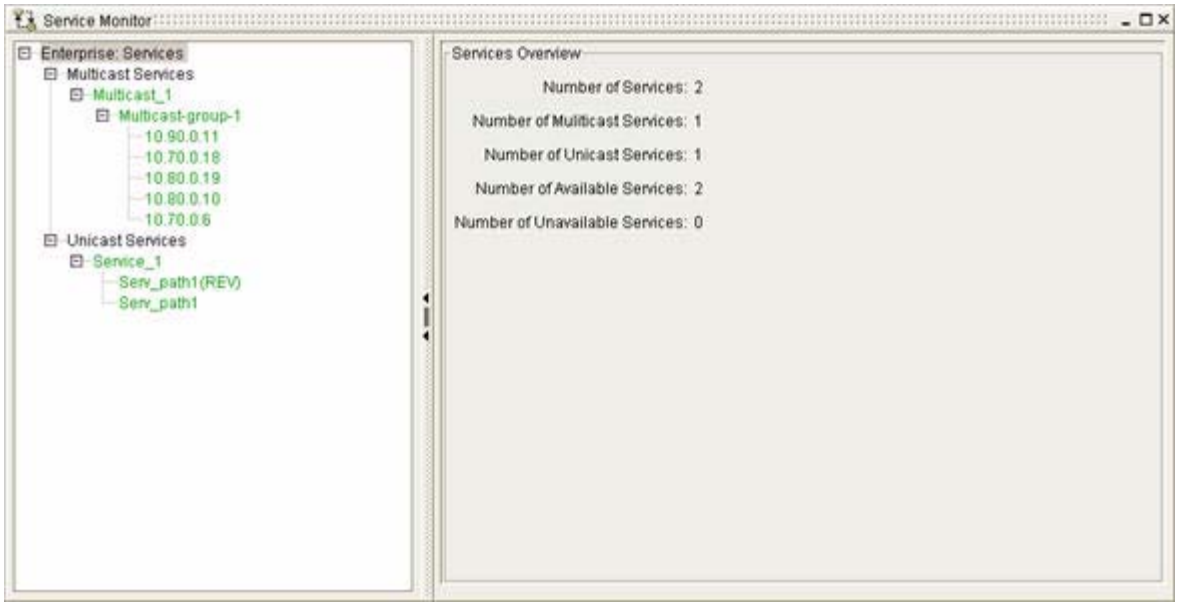


Step 5 Start the Topology Browser in investigative mode by selecting **Start** > **Topology Browser** > **Investigative**. In the Investigative Topology Browser wizard, you can query for specific attributes of OSPF interfaces, routes, and route advertisements, and BGP routes and route advertisements. For more information on using the Investigative Topology Viewer, see Querying for Network Elements (for OSPF Entities), page 2-82.

Find Information about Historical Service Paths

Start the Service Monitor during the historical session by selecting **Start** > **Service Monitor** (see Figure 13-13).

Figure 13-13 Service Monitor in Historical Session



To view historical service paths:

Step 1 View the creation of services and service paths. For more information, see Chapter 3, "Monitoring Unicast and Multicast Services".

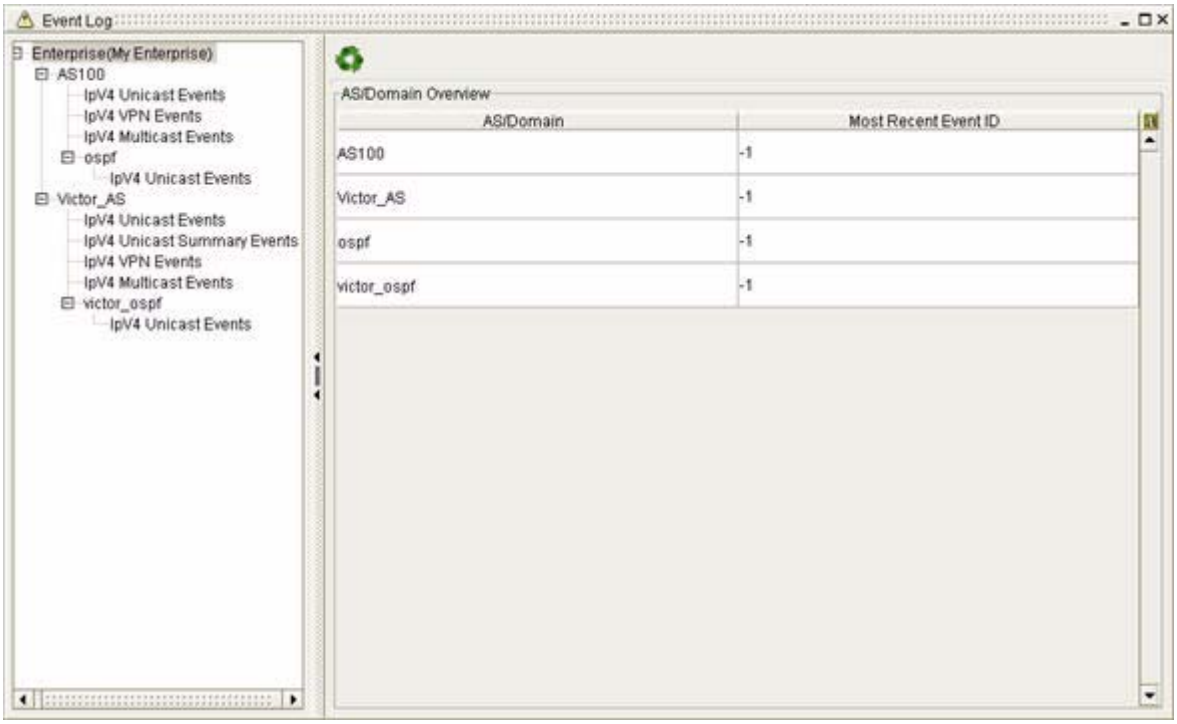
Step 2 Graphically view a service or service path on the Map. (For information, see Display Graphical Unicast Service, page 3-20 and Display Graphical Unicast Service Path, page 3-21.)

Identify the areas, as well as the date and time, that a service or any of its service paths deviated from its set baseline. For more information, see Managing Baselines of Service Paths, page 3-25.

Step 3 View the historical attributes of a service or service path.

Review Previous Events

Figure 13-14 Event Log in Historical Session



To review previous events:

Step 1 Start the realtime Event Log during the historical session by selecting **Start > Event Log** (see Figure 13-14).

Step 2 View the list of historical events and identify the dates and times of significant changes.

For example, determine which events occurred between `12:00` and `12:05` on a specific date that caused service path changes to display in the Service Monitor at the same time. See Working with Events, page 4-11 for more information.

View Historical Configurations and Domain Naming Assignments

Figure 13-15 Domain Administration in Historical Session

To view historical configurations:

Step 1 Start the Domain Administration module during the historical session by selecting **Start > Domain Administration**.

Step 2 Select the topmost level of the network hierarchy from the network hierarchy in the left side of the Domain Administration window (see Figure 13-15).

By default, this level is named **My Enterprise**. Your Path Analyzer system administrator may have changed the name.

Step 3 You can review domain administration at the enterprise, autonomous system, and domain level by selecting the applicable level in the network hierarchy on the left side of the screen.

At the top of the network hierarchy:

- Click the **Configuration** tab to view the name assigned to the network, and the autonomous systems configured for the network.
- Click the **Routers** tab to view router naming assignments. For information about naming assignments displayed in the Router Names tab, see Customizing Router Names on page 5-7 of the *Cisco Service Path Analyzer System Administration Guide*.
- Click the **Static Routes** tab to view the historical creation of static routes through parts of your network monitored by Path Analyzer.
- Click the **Next Hop Resolution** tab to view the historical configuration of a router as the next hop for a particular router. For information about configuring forwarding resolution, see Managing Static Routes and Next Hop Resolution on page 5-11 of the *Cisco Service Path Analyzer System Administration Guide*.

Step 4 Select an autonomous system under the highest level of your network.

For the selected AS:

- Click the **Configuration** tab to view Public or Private AS values, the autonomous system name, and the OSPF routing domains contained within the autonomous system. In addition, this tab displays BGP event summarization, master/slave flag, local VRF ID method, and VRF map method information.

- Click the **Router Names** tab to view DNS name assignments of routers imported in to Path Analyzer, and their sources. For information about configuring DNS name assignments in Path Analyzer, see Customizing Router Names on page 5-7 of the *Cisco Service Path Analyzer System Administration Guide*.

Step 5 From the network hierarchy, select an area from under an autonomous system.

For the selected routing domain:

- Click the **Configuration** tab to view the name.
- The **Router Names** tab, which is generally unpopulated in the historical session.

GLOSSARY

A

access router A router that passes data to and from a *Stub network*.

activity A measure of the amount of change to the network or aspects of the network. Catch-all category for all types of change including stability, availability, reachability, redundancy, loss, and growth. Activity level is determined by the number of events, atomic units of change, generated and stored by the system.

Address Resolution Protocol (ARP) A protocol that determines the Layer 2 Media Access Control (MAC) address of a network device from its network layer address, referred to as its Internet Protocol (IP) address, on a network segment.

advertisement An advertisement is a message that associates a route with a router. There are three types of events associated with advertisements:

- announcements that declare reachability
- changes that declare the modification of an attribute of the advertisement — metric, forwarding address, etc.
- withdrawals, which declare that a previously reachable route is no longer reachable.

OSPF route advertisements are deduced from *Link State Advertisement (LSA)*s, and are further classified into Stub, External, Type 3 and Type 4 summary advertisements. BGP advertisements are received directly and carry attributes such as community strings and next hop.

agent A software program that collects data from a designated source over a protocol, such as *Simple Network Management Protocol (SNMP)*, on a set, repetitive schedule.

alarm An automatic notification of changes in your network.

announcement An event indicating the availability of an advertisement. For example, an OSPF External route event advertising reachability of 1.2.3.0./25 from router 5.6.7.8.

application layer Layer 7 of the *Open Systems Interconnection (OSI) model*, which provides services to ensure communication between applications. Services include user and client authentication, confirmation that a destination application can be reached, and agreements between applications for protocol use, event structure, error recovery, data integrity, and privacy.

area A set of networks grouped together for administrative purposes within an *Autonomous System (AS)*. The topology of an area is hidden from the rest of the AS to reduce routing traffic. Routing within an area is determined by the area's topology, protecting the area from bad routing data. For more information, see http://www.ietf.org/rfc/rfc2328.txt.

Area Border Router (ABR) A router that has interfaces assigned to multiple areas.

Area-Internal View A Cisco Service Path Analyzer term that describes the router's view of a network area based on data received by an IP Listener or multiple IP Listeners assigned to the area.

Area Node A software component that logically connects to a router interface and identifies the area in which the interface is configured. (See *router interface*.) One area node is assigned to each router interface in the same area. For example, if a router has two interfaces in one area, the router is assigned only one Area Node.

Area Border Router (ABR) Area Border Routers (ABRs) have interfaces in more than one area. One area node is assigned to each interface that belongs to a different area. For example, if an ABR has one interface in Area 0 and two interfaces in Area 1, two area nodes are assigned to the ABR.

Autonomous System (AS) A single network or group of networks managed by an assigned network administrator and assigned a unique *Autonomous System Number* (ASN). Routers within an autonomous system use an interior gateway protocol to communicate route information to each other. An autonomous system comprises at least one routing *domain*.

Autonomous System Boundary Router (ASBR) Also, Autonomous System Border Router. An ASBR is a router that is connected to more than one AS, and that exchanges routing information with routers in other AS's. ASBRs typically run a non-IGP routing protocol (e.g., BGP), or use static routes, or both. An ASBR is used to distribute routes received from other AS's throughout its own AS.

AS Path *Autonomous System (AS)* path. An AS path is a list of each AS between a source and a destination router. AS paths are used by *Border Gateway Protocol (BGP)* to prevent routing loops. After each router makes a decision about the best route to a destination, it will send that route, or path information, along with accompanying distance metrics and path attributes, to each of its peers. As this information travels through the network, each router along the path prepends its unique AS number to a list of AS's in the BGP message. This list is the route's AS path. The AS path, when used in conjunction with an AS prefix, provides a unique one-way route through the network.

Autonomous System Number A globally unique number assigned to an *Autonomous System (AS)*.

availability A measure of the presence or readiness of a network device, or component such as an interface, link, network, service, or other network element. Availability is presented as the length of time the network or some aspect of the network was available or unavailable. In the Cisco Service Path Analyzer Topology Browser, availability is indicated by an "up" status; in the Topology Viewer, availability is indicated by blue or green coloration of a topology element.

Generally, an adjacency between two routers is available if the status is "up." A service is available if a path exists between all endpoints. A route is available if a router issues an advertisement for it, and a prefix is available if any router advertises a route to it.

B

backbone A high-capacity transmission channel within a network that carries data received from lower-capacity links.

backbone area An area used to interconnect other OSPF areas. The backbone area is referred to as Area 0. It has an Area ID of 0.0.0.0.

Backbone Router (BR) A router located in the backbone of a network. It normally carries a heavy volume of data across the network.

Backup Designated Router (BDR) A term used in OSPF routing to designate a secondary *Designated Router (DR)*, which takes over the responsibilities of the primary Designated Router (DR) in the event of a failure.

bandwidth The measure of the speed of data transmitted on a path from source to destination. Bandwidth may be measured in thousands of bits (kilobits) per second, millions of bits (megabits) per second, or billions of bits (gigabits) per second, depending on the medium and method of transmission.

baseline A designated route between the gateway (the first hop from the source of the transmission) and the destination.

big endian The *Network byte order* in which bits are arranged from smallest to largest in TCP/IP packet headers. In the big-endian arrangement, bits 0-7 are expressed first, followed by bits 8-15, then 16-23, then 24-31. See *little endian*.

black hole A term used to describe the lack of *reachability* of a routeable network address, usually within the scope of an autonomous system or the enterprise network. The network has a black hole if a given address has no route advertisements.

black hole list or blacklist A list of IP addresses known to be sources of *spam*. A blacklist is used to filter undesired traffic.

Border Gateway Protocol (BGP) The Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol. (See *Autonomous System (AS)*.) BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP's). Customer networks, such as universities and corporations, usually employ an *Interior Gateway Protocol (IGP)* such as RIP or OSPF for the exchange of routing information *within* their networks. Customers connect to ISP's, and ISP's use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Internal BGP (IBGP).

bound router A router configured with the *next hop* of a *static route*.

broadcast To send out a signal to all receivers at the same time. In broadcast networks using OSPF, the *Designated Router (DR)* connected to a switch in a Transit network broadcasts routing updates to all routers on the network.

broadcast storm An undesirable network condition in which a large-scale proliferation of packets occurs when multiple network hosts broadcast simultaneously.

C

call An action undertaken on a *circuit switched* telephone network that establishes a temporary, dedicated connection between the sender and the receiver for the duration of communications.

classification A type of chart provided in Cisco Service Path Analyzer Chart Manager. Classification charts graph data by the top entities that experience the most changes, or that have the largest impact on the network in the selected period of time. For example, the "Top Ten Flaky Interfaces" chart displays the ten interfaces with the most availability and metric changes over a user-defined time period.

circuit switched A network in which a circuit—a temporary, dedicated connection—is established between the sender and the receiver before initiating communications.

Classless Inter-Domain Routing (CIDR) A system of allocation of IP address space (represented as a prefix appended to a 32-bit IP address) intended to prevent the Internet from running out of IP addresses. Prior to CIDR, organizations were assigned an arbitrary block of IP addresses that allocated far more individual host addresses than the organization required.

Collector Cisco Service Path Analyze Collectors are the virtual routers that run inside each *Listener*. They form a adjacency with at least one router per OSPF or BGP domain, and they participate in routing activities without forwarding data. You are required to configure at least one Collector for each *Listener* in your system.

community string A password in the form of a character string shared by a *Simple Network Management Protocol (SNMP) agent*, such as a router configured with SNMP, or a host or system, such as a network management system (NMS).

conformance A binary state that is calculated as the Boolean AND of the conformance of all *service path*s associated with a *service*. A service is considered to be non-conforming when any of its associated service paths deviates from the set baseline. Also referred to as *conformity*.

conformity *conformance*

connectionless system A type of packet-switched network in which packets are routed from a source host to a destination host without prior arrangements or communication. Before sending data, the source and the destination do not share communications or establish a dedicated connection. Packetized data may follow a path across routers and through Transit networks. Connectionless systems do not provide:

- Guarantee of reaching the destination
- Mandated order or sequence
- Tracking mechanisms
- State information

If problems occur during transmission, the source host may attempt to resend the data several times. The *Internet Protocol (IP)* is one example of a connectionless protocol.

connection oriented system A system in which a direct, dedicated, and often temporary connection is established between the source and destination hosts before forwarding packetized data from the source to the destination. Packet headers enable switches to forward the packets on a hop-by-hop basis and to reconstruct the data at the destination point. Examples of connection-oriented systems include the Frame Relay networks, X.25 networks, and Asynchronous Transfer Mode (ATM) networks.

core A term used in Cisco Service Path Analyzer to categorize network entities for filtering and charting. Core entities reside in a single area of the network. Changes to core entities, referred to as core events, are limited to the area in which the core entity exists, and affect routing within the area. An example of a core entity is a router that has interfaces in only one area and sends packets one hop toward a destination within the area.

cost A single, dimensionless metric associated with the output side of a router interface, configured by a system administrator. An interface is more likely to be used to forward traffic if it has a lower cost than competing interfaces.

D

daemon A program that initiates a background process used to complete a system-related task.

data The main content of a packet of encoded information, as distinguished from control information.

datagram A Layer 3 connectionless packet.

data link layer Layer 2 of the *Open Systems Interconnection (OSI) model*. It provides reliable data transmission over a link or path in the network. The data link layer is subdivided into the Logical Link Control Layer and the *Media Access Control (MAC) Layer*.

dead router timer A router setting that tells the router how long to wait before it decides that a neighboring router is no longer functioning.

Designated Router (DR) A router in an *Open Shortest Path First (OSPF) Transit network* that establishes adjacencies with, broadcasts network link state advertisements to, and assists in the synchronization of all routers on the network. Every Transit network has a *Backup Designated Router (BDR)* that takes over the responsibilities of the DR if the DR becomes unavailable.

destination A host computer or device intended to receive a message or file from a source host.

Distance Vector Protocol Routing protocols that use a distributed-processing approach to identify the shortest route between a path and a destination based on a distance vector algorithm. Routers enabled with a distance vector protocol such as Routing Information Protocol (RIP) calculate their routing tables, then send these tables to neighboring routers in the area. The receiving routers, in turn, calculate their routing tables until all routers determine the shortest path. Compare to a *link state protocol*, such as *Open Shortest Path First (OSPF)*.

distribution A term used in the Cisco Service Path Analyzer Report module to describe a classification of the data. For example, a Service Path Distribution chart shows both the level of service activity (for example, total number of service events), as well as how the activity level affected each member service path.

domain The scope of a single OSPF routed network. An OSPF domain is comprises at least one *area*.

down The state of a router, router interface, route, link, or network that has become unavailable due to a hardware or software issue. The down state indicates that the network element is not functioning properly. See also, *live* and *up*, for the contrasting state.

duration The length of time an entity is in a given state. In Cisco Service Path Analyzer, Duration charts show the cumulative time of a given network condition, such as availability. For example, the Duration of Service Availability chart shows the length of time a service was available within a specific period of time.

E

Enhanced Interior Gateway Routing Protocol (EIGRP) A proprietary routing protocol developed by Cisco in which each router stores a copy of its neighbor's routing table. If the router cannot identify a route from the local table, it queries all neighboring routers, which query their neighbors in turn until the route is discovered. Each router sends out periodic 'hello' packets to discover information about the state of neighboring routers. Routers keep backup routes (feasible successors) in their routing tables to speed network convergence in the event the successor route is no longer available.

enterprise The entire routeable network, comprising at least one *Autonomous System (AS)*.

entity Cisco Service Path Analyzer Reporting is based on entities and events. Entities are managed elements in the system, which persist through time, such as routers, interfaces and routes. An entity exists separately and independently and has the ability to communicate with other entities. For networks modeled after the Open Systems Interconnection (OSI) model, an entity is an element or item that exists within a subsystem and uses defined protocols to communicate with other entities

event An instantaneous change in the state or status of a network element, such as a router, Transit network, router interface, or route, usually recorded in a log and a database. An event may trigger other events to occur in response.

external route A route to a destination that resides outside an autonomous system. Advertised via *Open Shortest Path First (OSPF)* by an *Autonomous System Number*.

F

Fiber Distributed Data Interface (FDDI) A set of standards issued by American National Standards Institute (ANSI) and International Standards Organization (ISO) that provides specifications for data transmission on fiber optic lines in a local area network (LAN). Characteristics of FDDI networks include large geographic size, the ability to support thousands of users, similarity to the Token Ring protocol, and common use over the backbone of a Wide Area Network (WAN).

filter A process or device that screens network traffic for given characteristics, such as source address, destination address, or protocol. Filters can be used to collect information about traffic, or to discard selected packets.

flap Intermittent changes of state, from "available" or "up" to "unavailable" or "down," of a network entity such as a router, router interface, *path*, or *service* on or in your network.

flooding Broadcasting a *Link State Advertisement (LSA)* to all routers in an area. By flooding an LSA, a router can quickly distribute routing updates to every router, or *node* in a large network. *Open Shortest Path First (OSPF)* protocol uses flooding.

forwarding The task of a router to receive and then send an IP packet to one or more routers. The contents of the IP header within the packet enable the router to forward the packet to the correct destination.

fragment The result of *fragmentation*.

fragmentation The act of breaking up a single packet into multiple ones. Fragmentation is required when a packet is larger than the Maximum Transmission Unit (MTU) size designated for an interface. After fragmented packets are forwarded to the destination, they are reassembled.

frame A data packet of fixed or variable length, which has been encoded by a *data link layer* communications protocol for digital transmission over a node-to-node link.

frequency The number of times a network element changes state as a function of time. Frequency is a measure of stability. For example, frequency of service availability is the number of times a service becomes available or unavailable.

G

gateway A term that generally refers to a router. As a specialized networking term, gateway can also refer to a network device or software process that connects and enables communication between two or more systems that run different protocols. For example, a type of router that connects an autonomous system that runs *Border Gateway Protocol (BGP)* to an autonomous system that runs *Open Shortest Path First (OSPF)* protocol. One interface of the gateway supports BGP and receives transmissions from a BGP network. Another interface supports OSPF and sends the transmissions to an OSPF network.

generic router A term used to describe the mapping of routing protocol stacks to the physical device on which they run. Each Cisco Service Path Analyzer generic router has a one-to-one correspondence with its associated physical router, regardless of the number or type of protocol stacks that run on the physical router. For example, a router running an OSPF stack is associated with a single generic router in Cisco Service Path Analyzer. Likewise, a router running both OSPF and BGP stacks is also associated with a single generic router in Cisco Service Path Analyzer.

global view A Cisco Service Path Analyzer term used to describe the layout of the entire network topology built from data collected from IP Listeners installed in all areas of your network. The network topology is displayed in the Topology Viewer application.

growth The number of new IP addresses in the network as well as those that have been purged and then reappeared. Growth includes IP addresses of routers, interfaces, external prefixes, subnets, and other addressable components of the network.

H

header Supplemental data placed at the beginning of a block of data being stored or transmitted, which contain information for the handling of the data. The data following the header is often referred to as the “payload” or “body.” Layer 3 IP headers include items such as packet length, source address, destination address, time to live (TTL), type of service (TOS), and checksum, contained in sections of a packet. Packet headers provide instructions for routers about how to forward packets.

hello A special *packet* that routers on *Open Shortest Path First (OSPF)* networks send out periodically to establish and confirm adjacency relationships with other routers.

hello timer Router setting that controls how often a router sends out hello packets.

hop Transit of a data packet from one node to the next. As a packet is transmitted hop to hop, each intermediate router decrements its Time to Live (TTL) header setting by one. Routers drop packets with a zero TTL setting.

host See *node*.

hot-spot analysis A method for analyzing network data used by Cisco Service Path Analyzer Reporting that allows you to obtain information about a specific period of time or aspect of the network. Hot-spot reports contain Classification charts used to determine the most active elements in the network. These reports can be used as an entry point for a more comprehensive investigation through Historical Playback or Advanced Charting.

I

Internet Group Management Protocol (IGMP) IGMP is an Internet protocol used to manage the membership of Internet Protocol multicast groups.

inter-domain A term used to describe the aspect of the routing fabric that connects OSPF domains.

Internet Control Message Protocol (ICMP) ICMP is an Internet protocol that handles message control and error reporting between a generic device on the network, such as a host, and a gateway. One ICMP command, “ping,” sends a request for a response (“echo”) to the device you specify. If the remote device is available on the network, it responds with ICMP echo reply.

interface A point of interconnection between a terminal and a network, or between two networks.

Interior Gateway Protocol (IGP) A type of routing protocol used for sending data between routers with the same autonomous system. Two common Interior Gateway Protocols (IGP) are *Routing Information Protocol (RIP)* and *Open Shortest Path First (OSPF)*.

Internal Router (IR) A router that has all interfaces assigned to the same OSPF *area*.

Internet Engineering Task Force (IETF) In their own words (quoted from their Web site, www.ietf.org): “The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.The technical work of the IETF is done in its working groups, which are organized by topic into distinct areas (e.g., routing, transport, security, etc.). Correspondence is handled via mailing lists.

Internet Protocol (IP) IP is a network layer (Layer 3) protocol used for transmitting data across a packet-switched network like the Internet.

intra-domain Term used to describe the aspect of the routing fabric that connects areas within a domain.

IP multicast IP multicasting permits a one-to-many transmission, in contrast to unicast (one to one) or broadcast (one to all). IP datagrams are sent to a destination “host group” identified by single IP address (see *multicast address*). The membership of a host group is dynamic. Members may join or leave the group at any time. There is no restriction on the number or location of members in a host group.

IPV4 Internet Protocol Version 4. The fourth version of the *Internet Protocol (IP)* (see IETF RFC 791) and the most widely used (see also, *IPV6*). IPV4 uses 32-bit addresses.

IPV6 Internet Protocol Version 6. The sixth version of the Internet protocol (see IETF RFC 2460 has been designed to be the successor to IPV4. IPV6 uses 128-bit addresses, permitting many more IP addresses than IPV4.

J

K

KEEPALIVE message A type of message passed by one BGP speaker to a peer to maintain the communication channel.

L

link A connection between nodes over which data is transmitted.

link load The amount of data carried by a link, normally measured in bytes.

Link State Advertisement (LSA) The messages advertised by a router to other routers to provide information about network topology and how to route packets across an area, autonomous system, or multiple systems. Each LSA generates one or more events — changes that occur in your network. The *Internet Engineering Task Force (IETF) Open Shortest Path First (OSPF)* Work Group identifies the following seven types of Link State Advertisements.

- **Type 1, Router LSA**—Issued by a router to all other routers within a single area, this LSA describes the type of router and the state and cost of all the router's links in the area.
- **Type 2, Network LSA**—Issued by a *Designated Router (DR)* to all other routers within a single area, this LSA describes all routers attached to a Transit broadcast or non-broadcast, multi-access (NBMA) network.
- **Type 3, Summary LSA**—Issued by an *Area Border Router (ABR)* within a single area, describes a destination within the autonomous system, outside the area. Provides information about the advertising router and the destination network
- **Type 4, Summary LSA**—Issued by an ABR or combined ABR/ASBR within a single area, describes show to reach the advertised ASBR.
- **Type 5, External LSA**—Sent by an ASBR to all routers within an autonomous system. Provides information about destinations outside of the autonomous system.
- **Type 6, Multicast LSA**—Issued by a source router within an area. Informs multicast routers within the area about paths around routers that do not support multicasting, enabling automatic multicast transmission over the shortest paths to other multicast routers.
- **Type 7, Not So Stubby Area (NSSA) LSA**—Issued by a source router to other routers in the area about routes to a Stub network.

Listener A Cisco Service Path Analyzer Listener (or more specifically, a *Collector* within the Listener) forms an adjacency with a router on your network and obtains information about routing activities, the network topology, service paths, or routing events.

link state protocol A routing protocol that uses a distributed database approach and a link state algorithm to enable routers to distribute packets. Unlike a distance vector protocol, which requires all routers on the same network to recalculate their routing tables to determine the shortest path, a link state protocol requires routers to send out Link State Advertisements, informational communications about updates to parts of a router's routing table. When a router receives an LSA, it checks the LSA for corruption, then installs the LSA in its own link-state database and returns an acknowledgement that the LSA was received.

little endian *Network byte order* in which bits are arranged from largest to smallest in TCP/IP packet headers. In the little-endian arrangement, bits are expressed from 31 to 0. See *big endian*.

live A term generally applied to a router interface to indicate that it functions properly, completing normal and expected routing activities, such as packet forwarding. See *up* for a term that has the same meaning. See *down* for a term with the opposite meaning.

live interface A router interface that functions properly; receiving and forwarding packets in its assigned area. By subtracting the number of live interfaces from the total number of interfaces, you can determine the number of interfaces that are down (not functioning).

load The amount of data traffic carried by the link or network.

loss The number of times the relationship between elements on your network, such as an adjacency between routers, becomes unavailable or unreachable. For example, an adjacency loss is the number of times an adjacency between two routers becomes unavailable.

M

Maximum Transmission Unit (MTU) MTU refers to the size (in bytes) of the largest packet that an interface can pass onwards. The MTU for Ethernet is 1500 bytes.

Media Access Control (MAC) address The MAC address is the *physical* address of a network interface. A MAC address is hard-coded into the each specific interface device. (A network interface also has a *logical* address. For example, an IP address).

Media Access Control (MAC) Layer A subdivision of the *data link layer* that enables multiple computers to share the same lines of transmission. Widely used MAC protocols include Ethernet, FDDI, Token Bus, and Token Ring.

MP-BGP Multiprotocol *Border Gateway Protocol (BGP)*. BGP4 was originally designed to carry routing information for the IPv4 address family. The Internet Engineering Task Force (IETF) has extended BGP4 capability by standardizing multiprotocol extensions for BGP4. MP-BGP allows BGP to carry routing information for the multiple network layer protocols including IPV6, IPX, and VPN-IPV4.

multicast The communication between a source sender and multiple destination recipients.

multicast address Class D IP addresses are used for multicasting. In Internet standard dotted-decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. (Some of these addresses are reserved for special purposes.)

Multi-Exit Discriminator (MED) A BGP route attribute that tells the receiving BGP speaker how to weigh multiple occurrences of the same route.

multihomed Having multiple connections, denoted by IP addresses, to one or more networks.

N

network A network address within an OSPF domain. There are two types of networks: Transit and Stub. Network traffic is routed through a Transit network. A *Stub network*, or a subnet, is a sink in the network — traffic does not pass through. Routers advertise routes to Transit and Stub networks. Many routers form an adjacency with a Transit network. One router, the Designated Router (DR), is the elected advertiser for the network.

Network byte order The arrangement of bits in an IP packet header. All TCP/IP packet header bits are arranged in a manner referred to as *big endian*.

network convergence A state in which all routers on the same network have the same up-to-date knowledge of routing paths.

network layer reachability information (NLRI) The keywords that network administrators assign to routers to enable multicast or unicast forwarding. BGP-4 expresses NLRI as route prefixes. See http://rfc.net/rfc2283.html.

next hop An interface configured to receive packets from an originating router over a *static route*. The router configured with the next hop is referred to as the *bound router*.

node A connection point for data transmission. A node can be an end point for a data transmission or a redistribution point that processes or forwards transmissions to other nodes. A gateway node passes information between two networks.

node load The amount of data received by an end node or carried by a redistribution node to the next node in a path.

noise An unexpected and/or unwanted electrical or electromagnetic energy that interferes with a signal.

Non-Broadcast Multi-Access (NBMA) network A type of *Open Shortest Path First (OSPF)* network that is used to model network environments in multiple-access networks where there are no *broadcast* and *multicast* capabilities. In an NBMA network, OSPF routers send *hello* messages to each router on the network, one at a time, rather than multicasting the messages. In an NBMA network the *hello timer* is extended from 10 to 30 seconds and the *dead router timer* is extended from 40 to 120 seconds. Other OSPF network types are: *broadcast*, *point to point (P2P)*, and *point to multipoint*.

NP2P interface A numbered point-to-point interface. A point-to-point serial WAN link in which the interfaces are identified by IP addresses. Compare *UP2P interface*.

O

OPEN message A message from a BGP router that establishes an adjacency with its peer.

Open Shortest Path First (OSPF) A protocol that uses an algorithm to identify the shortest path (the path that traverses the least number of nodes), between source and destination. An OPSF Router represents the OSPF protocol specific stack running on a physical device within the network. The three types of events associated with an OSPF router are:

- discovery events that indicate that an OSPF router has been added to the network
- change events that indicate changes to the state of an OSPF Router, including availability, ABR status, etc.
- removal events that indicate when an OSPF router has been removed from the network.

Open Systems Interconnection (OSI) model The OSI Model is a standard model used to simplify the design of networks. OSI divides network protocols into seven layers. The first four layers relate to the transmission of messages to or from users. The lower three layers relate to the handling of messages passed through host computers or routers. OSI defines the following seven layers:

- **Layer 7. Application Layer**—Despite the name, this layer does not concern itself with specific applications but with providing network services to applications. For example, if you want to access the World Wide Web you need to invoke application layer functions to send and receive HTML pages. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.
- **Layer 6. Presentation Layer, or Event Structure Layer**—Provides a variety of coding and conversion functions that are applied to application layer data to ensure that information sent from the application layer of one system would be readable by the application layer of another system. Presentation layer coding and conversion schemes include common data representation formats, conversion of character representation formats, common data compression schemes, and common data encryption schemes.
- **Layer 5. Session Layer**—Coordinates session and connection dialogs between applications at each end of a transmission. Establishes, manages, and terminates communication sessions.
- **Layer 4. Transport Layer**—Accepts data from the session layer and segments the data for transport across the network. Generally, the transport layer is responsible for making sure that the data is delivered error-free and in the proper sequence. Flow control generally occurs at the transport layer. The transport protocols used on the Internet are *Transmission Control Protocol (TCP)* and *User Datagram Protocol (UDP)*.
- **Layer 3. Network Layer**—Manages the routing and forwarding of packets between source and destination with a focus on finding the fastest path for a packet. The network layer defines the logical address of a destination, which differs from its *Media Access Control (MAC) address*.
- **Layer 2. Data-link Layer**—Provides reliable transit of data across a physical network link. Different data link layer specifications define different network and protocol characteristics, including physical addressing, network topology, error notification, sequencing of frames, and flow control. Physical addressing (as opposed to network addressing) defines how devices are addressed at the data link layer.
- **Layer 1. Physical Layer**—The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems. Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors.

P

packet A unit of data intended for transmission between a source and a destination node on a packet-switched network. In general, the term packet applies to any message formatted as a packet, while the term *datagram* is generally reserved for the packets of an unreliable service. A reliable service is one where the user is notified if delivery fails.

packet switched Describes a network in which units of data called packets are distributed from a source to a destination. Packet-switched systems may be *connection oriented systems* or connectionless.

path The entire route from a source host to a destination host within an area, between areas, or across more than one *Autonomous System (AS)*.

pathway A specific sequence of hops and links between a source and a destination. A path that branches at any hop can have more than one pathway.

persistent Stored in a database. Changes to persistent objects are recorded in the database over time.

point to multipoint Connections between three or more routers on an OSPF network in which one router sends hello packets and simultaneously forms an adjacency with the other routers.

point to point (P2P) A connection between two routers on an OSPF network. Routers exchange hello packets and establish adjacencies over numbered interfaces or unnumbered interfaces. See *NP2P interface* and *UP2P interface*.

port A TCP/IP transport layer (Layer 4) header field found in TCP and UDP headers. Ports are numbers used to identify a specific process. For example, HTTP is associated with port 80.

prefix Routeable address space within the enterprise network. Types of prefixes include:

- Core prefix — Address space located within an OSPF domain.
- External prefix — Address space located outside the OSPF domain.
- BGP prefix — Address space that is located outside the autonomous system.

propagation A term used in Path Analyzer to categorize network entities for filtering and charting. Propagated entities correspond to router advertisements within an area of a *core* event that occurred in another area. For example, one type is a peripheral entity is an *Area Border Router (ABR)* that sends packets between areas.

protocol convergence Protocol convergence is defined for the OSPF and BGP protocols. In both cases, it measures the amount of time separating the receipt of a given protocol event at two distinct instrumented routers. For OSPF, LSAs are the relevant protocol events, while route advertisements are used for BGP.

Q

Quality of Service (QoS) A resource reservation control mechanism that provides different priorities to different users or data flows or guarantees a certain level of performance. Quality of Service guarantees are important if the network capacity is limited, especially for real-time streaming multimedia applications, for example voice over IP and IP-TV, since these often require fixed bit rate and are delay sensitive.

R

RAID Redundant Array of Independent Drives (or Disks). A method of data storage that divides and/or replicates data among multiple hard drives. RAID systems are used to increase data reliability and/or input/output performance.

reachability Routing updates flow through the hierarchy, creating a connected fabric of routeable network addresses. Reachability is the term used to describe the accessibility of an address within a specific scope of the network.

A router is reachable within an area if there is an established adjacency connecting it to the area. A router is reachable within the enterprise network if it is reachable within the area *and* there is a route advertised for it throughout the enterprise.

Route reachability is scoped by a specific advertising router. Prefixes are scoped at the AS level. A prefix is reachable if any router within the AS advertises a route for it. A core prefix is reachable if any router advertises a route to it. A BGP and external prefix is reachable if any router advertises a specific or less specific route to it. A service path destination is reachable if there is a path from the source to the destination.

Reachability is a boolean — something is either reachable or not. Stability (see *stability*) is the number of times reachability changes; *availability* is the length of time something was reachable or not reachable.

redundancy Redundancy exists when one appliance can reach another over more than one path. Service paths are redundant if there is more than one way of getting from the source to the destination (that is, the path branches at some point). A prefix is redundant if more than one router advertises a route for it (either specific or less specific). Redundancy is not defined for route advertisements.

route A route is associated with a routing domain and indicates reachability to a set of IP addresses, indicated by an associated prefix.

- An ASBR advertises a route that is external to the OSPF domain.
- An ABR advertises a route (or summarized route) between OSPF areas.
- A BGP router advertises a route external to its AS system.

There are three types of routes: OSPF Core Route, OSPF External Route and BGP Route.

- A Core Route is a set of IP addresses that are internally reachable within an OSPF Domain through a Stub advertisement or transit interface.
- An External Route is similar but reachable outside of the OSPF Domain.
- A BGP Route typically represents reachable address space in a neighboring autonomous system.

route advertisement A message a router sends to other routers to communicate reachability for a given *prefix*.

route reflector Hardware or software that enables a BGP router to advertise (reflect) the best path to a destination to other routers in the network. Route reflectors reduce the amount of data passed between routers by:

- minimizing the number of update messages transmitted within an autonomous system.
- decreasing the amount of data contained in each message.
- freeing a single router from forwarding the entire routing table to all BGP routers within an autonomous system.

route summarization The consolidation of advertised addresses so that a single summary route is advertised. Used to reduce the number of entries in routing tables.

router A network device or software that determines the next node to forward a packet toward its destination.

router interface The part of a router assigned to receive packets from and send packets to routers and networks within a specific area.

Routing Information Protocol (RIP) A *Distance Vector Protocol* developed for managing router information in small, contained networks. RIP requires that neighboring routers share their forwarding tables to achieve an ideal state of *network convergence*. RIP measures the distance between routers by the number of hops — node to node transversals that a packet makes between source and destination — to determine the best direction in which to forward a packet.

RIP requires a designated router to send its entire forwarding table to the closest neighboring router every 30 seconds. The neighboring router updates its own forwarding table with the one it receives from the designated router, then passes the information to its next neighbor. Routers continue to pass the full forwarding table update from neighbor to neighbor.

RIP is considered an effective solution for small homogeneous networks. For larger, more complicated networks, RIP's transmission of the entire routing table every 30 seconds can place excessive traffic on the network.

routing table aggregation See *Classless Inter-Domain Routing (CIDR)*.

S

session A sequence of interactions or communications that occur after a source or sender initiates a request for communication or data transfer to a destination or receiver. Sessions occur in a *connection oriented system* and some *C*s, such as SSH, Telnet, and File Transfer Protocol (FTP).

service In Cisco Service Path Analyzer terminology, a service is a collection of *paths* that are critical to the reliability, stability, and availability of the application.

service path A construct within Cisco Service Path Analyzer used to monitor end-to-end connectivity between a source (first hop router) and a destination (some IP address). Service paths are used to monitor critical information flows within a network, allowing the user to track the availability and conformity to a predetermined baseline.

service path deviation A service path is said to deviate if the chain of routers used to forward packets between a source and destination is not the same as the baseline, a preconfigured set of routers, representing the "correct" hops in the path. If the service path does adhere to the predetermined chain of hops, it is said to "conform" to the baseline.

Simple Network Management Protocol (SNMP) A set of protocols used to manage networks using network management systems. Participating network devices are installed with software agents, which provide information about the state of the device to requesting systems. The attributes of SNMP-compliant devices are defined and stored as managed objects in a virtual information database called a Management Information Base (MIB).

SNMP Agent See *agent*.

single-homed Having one connection to a network.

source A computer or device that initiates a connection or sends a message or file to a recipient at a *destination*.

spam The indiscriminate transmission of unwanted e-mail solicitations.

speaker Another term for a router. BGP speakers exchange updates to their routing tables over the *Border Gateway Protocol (BGP)*.

Source Specific Multicast (SSM) Source Specific Multicast is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created.

stability The number of times a network element changes in *reachability*. Route stability refers to the *availability* of a route advertisement and the number of times it has changed. Service stability refers to the availability of the service, conformance to its engineered path, and the number of times it has changed. Metric stability refers to the number of times the metric has changed for an advertised route or physical interface.

static route A route configured manually by a network administrator. Static routes used fixed paths rather than routes derived automatically using routing protocols (called “adaptive routing”). With static routes, when there is a change in the network or a failure occurs between two statically defined nodes, traffic will not be rerouted. See also *bound router* and *next hop*.

Stub area A type of area that has no destinations in another *Autonomous System (AS)*. Type 3 Summary routes, Type 4 Summary routes, or External routes are not broadcast in a Stub area.

Stub interface A router interface that connects to a Stub network.

Stub network A network that allows traffic to flow only to and from directly connected systems or devices. Stub networks do not allow data to pass through the network.

Stub route A path between a router and a Stub network.

Stub router A router that connects and transmits data to and from a Stub network

subnet mask A 32-bit address mask used to indicate the bits of an IP address that are being used for the subnet part of the address. That is, they distinguish host bits from network bits.

summarization See *route summarization*.

switch A network device that channels incoming data packets from one or more input ports to a specific output port that forwards data toward its intended destination. In a *connection oriented system*, such as the telephone network, one or more switches set up a temporary, dedicated connection for an exchange between two or more parties. In an Ethernet-based, Frame Relay local area network (LAN), a switch determines which output port to forward data from based on the *Media Access Control (MAC) address* in each incoming message frame.

In a packet-switched wide area network (WAN) such as the Internet, a switch determines which output port to forward data out of based on the destination IP address provided in each packet. Many switches act as *router*s

syslog A UNIX-based logging system used to manage messages and information generated by the kernel, applications, and utilities. Syslog includes a *daemon*, a set of library routines, and the `logger` command that enables users to submit log entries. Syslog saves programmers from the tedium of writing log files and allows system administrators to control logging functions.

Cisco Service Path Analyzer system administrators can export alarm triggers to syslog. For information, see Exporting Alarm Triggers in the *Cisco Service Path Analyzer System Administration Guide.*

T

.TCP segment A unit of data that *Transmission Control Protocol (TCP)* sends to *Internet Protocol (IP)*.

Time To Live (TTL) A field within an IP header that specifies how many hops the packet should travel before being discarded.

topology A description of the physical arrangement of network devices that form an autonomous system. Topologies are described by their geometric shape, such as a ring or a star.

topology element A depiction of an autonomous system, area, router, or other network element as it appears in the Cisco Service Path Analyzer Topology Viewer and Topology Browser modules.

tracking A type of chart provided in Cisco Service Path Analyzer Charting. Tracking charts graph data over a continuous time period. Unlike a *trending* chart, a tracking chart shows when something happened to a network element. The x-axis shows a continuous time period. The y-axis either shows a state transition value or the number of entities in a given state. For example, the y-axis can show state transitions in availability or unavailability for a given service, or the number of services that are available at any given point in time.

Transmission Control Protocol (TCP) A Transport Layer (Layer 4) protocol and one of the major protocols on the Internet (TCP/IP). TCP established a full-duplex virtual connection between two endpoints to ensure the reliable delivery and proper sequencing of packets.

TCP also distinguishes data to allow multiple connections by concurrent applications (for example, a Web server and an e-mail server running on the same host). TCP is the intermediate layer between the Internet Protocol (IP) below it, and an application above it. Many popular applications use TCP including the World Wide Web, FTP, and Secure Shell. Compare *User Datagram Protocol (UDP)*.

Transit interface A router interface that connects to a Transit network.

Transit network A network that provides interconnectivity among a set of routers.

trending A type of chart provided in Cisco Service Path Analyzer Charting that tracks event volume by plotting the number of occurrences in each subinterval of time. This type of chart highlights peak periods of instability and indicates the type(s) of events responsible. An example of a trend chart is an "OSPF Core Route Activity Chart," which displays the hourly number of Core Route Availability, Core Route Unavailability, and Core Route Redundancy events plotted over an entire week.

trigger 1. (n) A single event or sequence of events that causes an alarm to be activated in Alarm Monitor. A trigger corresponds to at least one event, as one or more events can activate an alarm.

For example, a flap alarm set on a P2P interface is triggered after the interface changes state from "down" to "up" a specified number of times within a set period of time. (In Alarm Monitor, you set the number of times and the period of time.) Each change of state from "down" to "up" is an event that contributes to triggering the alarm. For each triggered alarm, Alarm Monitor and the Alarm Log display the last ten triggers.

2. (v.) The action of a trigger activating an alarm.

U

unicast The transmission of data between one sender (source) and one receiver (destination) over a network.

up The state of a router, router interface, route, link, or network that indicates it functions properly, fulfilling its role in the network by completing normal and expected routing activities. See *live* for a term that has the same meaning. See *down* for a term with the opposite meaning.

UP2P interface An unnumbered point-to-point interface. A point-to-point serial WAN link in which the interfaces are not assigned permanent IP addresses. Instead, a Management Information Base (MIB) number is assigned. Compare *NP2P interface*.

UPDATE message A BGP message a router sends to its peer to update its routing table with new and changed routes.

User Datagram Protocol (UDP) UDP is a Transport Layer (Layer 4) communications protocol that offers limited service but low overhead when messages are exchanged between computers in an IP network. UDP is an alternative to *Transmission Control Protocol (TCP)* but it does not guarantee reliability or ordering in the way that TCP does. Datagrams may arrive out of order or in duplicate, or not arrive at all. UDP is faster and more efficient than TCP, at least for applications that do not need guaranteed delivery.

V

virtual link A connection formed between two geographically dispersed network devices through a switch.

VPN Virtual Private Network. A VPN uses shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer 2 Tunneling Protocol (L2TP). VPNs support remote access and private data communications over public networks.

VRF Virtual Routing and Forwarding (also referred to as *VPN* Routing and Forwarding). A VRF is a "logical" router. It consists of routing tables, a forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the routing table. VRFs allow multiple instances of a routing table to exist within a router and work simultaneously. This permits network paths to be segmented without using multiple devices, thereby increasing network security and eliminating the need for encryption and authentication. VRF technology is most commonly used in the ISP marketplace, particularly in *VPN* configurations.

W

withdrawal Refers to the removal of an advertisement from a router's routing table.

X

XML Extensible Markup Language. The Extensible Markup Language (XML) is a subset of SGML (Standard General Markup Language). A markup language combines text and extra information about the text such as its structure or appearance. The most commonly used markup language is HTML (Hypertext Markup Language), used extensively on the World Wide Web. XML is used within Cisco Service Path Analyzer for a variety of purposes including importing and configuration data, installing VRF definitions, and creating tags used to mark identify and/or remove events.

Y

Z