



## **Cisco Service Path Analyzer System Administration 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

Customer Order Number:  
Text Part Number: OL-12861-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0803R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

*Cisco Service Path Analyzer User Guide*

© 2008 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface ix**

Overview of Cisco Service Path Analyzer	ix
Audience	ix
Organization	x
Chapter-Level Organization	xi
Indicators	xi
Related Documentation	xi
Additional Technical References	xii
Support for Alarm Trigger Exporting	xiii
Obtaining Documentation, Obtaining Support, and Security Guidelines	xiv

---

## **CHAPTER 1**

### **Administering the Cisco Service Path Analyzer 1-1**

Getting Started with Administration	1-1
Initial Configuration and Reconfiguration Tasks	1-1
User Account Set Up and Maintenance Tasks	1-1
System Integration Tasks	1-2
Database Management Tasks	1-2
Component Removal Tasks	1-2
Upgrade Tasks	1-2
Troubleshooting Tasks	1-2

---

## **CHAPTER 2**

### **Preparing for Initial Configuration 2-1**

Preparation for Configuring your Cisco Service Path Analyzer System	2-1
Path Analyzer Initial Configuration Tasks	2-1
Using the Initial Configuration Task Checklist	2-1
Setting the Administrator's Environment	2-2

---

## **CHAPTER 3**

### **Configuring the Cisco Service Path Analyzer Server 3-1**

Configuring Interfaces and Network Information	3-1
The Configuration Tool	3-1
Initial Configuration: Network Information	3-2
Initial Configuration: Setting the Date and Time	3-4
Configuration Tool Command List	3-5
Reconfiguring a Path Analyzer Server	3-8

Start System Administration	3-9
<b>Start the Path Analyzer Server Configuration Wizard</b>	<b>3-9</b>

## CHAPTER 4

### **Installing the Management Console and Upgrading Your Cisco Service Path AnalyzerSystem** 4-1

Path Analyzer Installation and Upgrading Procedures	4-1
Reviewing Pre-Installation Requirements	4-1
Hardware Requirements	4-2
Software Requirements	4-2
Loading a New Software Release	4-2
Load a New Release	4-2
Downloading and Installing the Management Console (GUI)	4-3
Uninstalling the Management Console	4-3
Installing the GUI	4-3
Starting Path Analyzer	4-5
Upgrading Path Analyzer Software	4-5
Locating the Installation Files	4-5
Rebooting the Path Analyzer Server	4-6
Running the Installation Wizard	4-6
Starting Path Analyzer	4-10
Verify the Connection	4-10
Upgrading the Listeners	4-12

## CHAPTER 5

### **Configuring Domains for Your Enterprise** 5-1

Setting Up Autonomous Systems and Routing Domains	5-1
Divisions of Autonomous Systems	5-1
Customizing Router and Route Identifiers	5-2
Domain Administration Tasks Overview	5-3
Removing Unavailable Entities	5-3
Domain Administration	5-3
Start the Domain Administration Module	5-3
Assigning Names to Autonomous Systems and Routing Domains	5-3
Customizing the Name of Your Enterprise Network	5-4
Adding an Autonomous System	5-4
Changing the Name of an Autonomous System	5-5
Adding a Routing Domain	5-5
Changing the Name of a Routing Domain	5-6
Customizing Router Names	5-7
Options for Changing Router Names	5-7

Importing DNS Names and Applying them to Routers	5-7
Viewing Hostname Changes	5-8
Removing DNS Names	5-9
Changing Router Names	5-9
Managing Static Routes and Next-Hop Resolution	5-11
Static Routes and Next-Hop Resolution in Path Analyzer	5-12
Creating or Editing a Static Route	5-12
Configuring Next-Hop Resolution for a Static Route	5-15
Removing a Static Route	5-17
Viewing Properties of a Router	5-19
Managing VRF Tables	5-19
Importing VRF Tables Using XML Files	5-20
Removing Autonomous Systems and Routing Domains	5-21
Removing Autonomous Systems	5-21
Removing Routing Domains	5-22
Removing BGP or OSPF Entities	5-22
Remove BGP Entities	5-22
Remove OSPF Entities	5-23

## CHAPTER 6

### Configuring Listeners and Collectors 6-1

Enabling your Listeners to Collect Routing Data	6-1
Path Analyzer Components and Configurations	6-1
Path Analyzer Initial Configuration and Maintenance Tasks	6-1
Path Analyzer Components	6-1
Listener	6-2
Collectors	6-3
Path Analyzer Server	6-3
Clients Running the Management Console	6-3
Path Analyzer System Configurations	6-3
Single Autonomous System	6-4
Multiple Autonomous Systems	6-5
Adjacencies for OSPF or BGP Collection	6-5
Fault-Tolerant Configurations	6-10
Listener Availability	6-11
Listener Redundancy	6-12
Configuring Path Analyzer Appliances	6-13
Path Analyzer Initial Configuration Tasks	6-13
Path Analyzer Maintenance Configuration Tasks	6-13

Configuring the Listener Connection to the Path Analyzer Server	6-14
Adding a Listener	6-14
Reconfiguring a Listener	6-24
Configuring a Collector	6-25
Configuring an OSPF Collector	6-25
Adding a New OSPF Collector	6-25
Reconfiguring an OSPF Collector	6-35
Configuring a BGP Collector	6-35
Adding a New BGP Collector	6-35
Reconfiguring a BGP Collector	6-41
Viewing Appliance and Collector Configurations	6-42
Viewing Status and Statistics	6-42
View the Configuration Status of your System	6-42
View Path Analyzer Server Statistics	6-43
Removing Path Analyzer Components	6-49
Removing or Uninstalling Physical Components of Your System	6-49
Removing a Collector	6-50
Removing a Listener	6-50
Uninstalling the Management Console (Windows Users)	6-50
Uninstalling the Management Console (Unix-Bases System Users)	6-51

---

**CHAPTER 7**

<b>Setting Up and Maintaining User Accounts</b>	<b>7-1</b>
Managing Accounts of Path Analyzer Users	7-1
User Account Set Up and Maintenance Tasks	7-1
Path Analyzer Users	7-1
Administrator User Privileges	7-1
Power User Privileges	7-2
Limited User Privileges	7-2
Adding a New User Account	7-3
Changing Details of a User Account	7-5
Removing a User Account	7-6
TACACS+ Authentication	7-6
Add a Primary TACACS+ Server	7-7
Change a Primary TACACS+ Server	7-8
Disable a Primary TACACS+ Server	7-8
Enable a Primary TACACS+ Server	7-8
Secondary TACACS+ Server Tasks	7-9

**CHAPTER 8****Exporting Alarm Triggers 8-1**

- Viewing Path Analyzer Events that Trigger Alarms in your Network Management System (NMS) 8-1
  - Path Analyzer Alarm Integration Tasks 8-1
  - Path Analyzer Alarm Maintenance Tasks 8-1
  - Integrating Path Analyzer Alarm Triggers into Your NMS 8-2
- Configuring the Export of Alarm Triggers to a Syslog Host 8-2
  - Syslog Priority Levels Compared to Alarm Monitor Severities 8-2
  - Export to Syslog Destinations 8-3
  - For More Information about Syslog 8-4
- Configuring the Export of Alarm Triggers to an SNMP Agent 8-5
  - Export Alarm Triggers to an SNMP Agent 8-5
  - For more information about SNMP 8-6
- Reconfiguring a Syslog or SNMP Alarm Destination 8-7
  - Reconfigure an Existing Alarm Destination 8-7
- Removing an Existing Syslog or SNMP Alarm Destination 8-7

**CHAPTER 9****XML Configuration Files 9-1**

- XML Configuration Files 9-1
  - Why Use XML Configuration Files? 9-1
  - Exporting XML Configuration Files 9-1
  - Modifying XML Configuration Files 9-3

**CHAPTER 10****Maintaining Your Path Analyzer Database 10-1**

- Purging Your Path Analyzer Database 10-1
  - Data Management Tasks 10-1
- Starting the Data Management Administration Module 10-1
- Managing Your Data 10-2
  - Viewing Database Statistics 10-2
- Configuring a Purge 10-3
  - Scheduling a Periodic Purge 10-3
- Completing a Temporal Purge 10-7
- Canceling a Temporal Purge 10-8

**CHAPTER 11****System Diagnostics and Troubleshooting 11-1**

- Monitoring Performance 11-1
  - Statistics Graphs 11-1
  - Accessing Statistics Graphs 11-2
- Using System Diagnostics 11-3

Viewing System Diagnostics	11-3
Troubleshooting a Path Analyzer Appliance	11-5
Tools for Completing Troubleshooting Tasks	11-6
Troubleshooting a Collector	11-9
Verify the Configuration of a Collector Interface	11-9
View the OSPF or BGP Stack of a Collector	11-10
Verify Configured OSPF Neighbors	11-11
Analyze the Packet Stream of a Collector	11-13
Browse the LSA Database of an OSPF Collector	11-13
Browse the Route Database of a BGP Collector	11-15
Uploading Files	11-17
Upload Path Analyzer Files	11-17





## Preface

---

The *Cisco Service Path Analyzer System Administration Guide* provides system administrators with the information needed to configure and set up user accounts as well as reconfigure, upgrade, administer, maintain, and troubleshoot the Cisco Service Path Analyzer, once system installation has been performed.

For information about installing and connecting Cisco Service Path Analyzer appliances, see the *Cisco Application Deployment Engine 1010 and 2120 Appliance Hardware Installation Guide* or the *Cisco Application Deployment Engine 2130 and 2140 Appliance Hardware Installation Guide*.

## Overview of Cisco Service Path Analyzer

The Cisco Service Path Analyzer (hereafter referred to as Path Analyzer) enhances your current network management solution by adding the ability to identify, diagnose, and quickly resolve routing problems, thereby 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. The Path Analyzer delivers a new level of proactive maintenance by monitoring the IP level of the network for events and faults that remain undetected by existing network management systems.

## Audience

This guide is intended for the Path Analyzer System Administrator who is responsible for configuring, maintaining, and troubleshooting a Path Analyzer installation.

## Organization

Chapter Number	Chapter Title	Description
Chapter 1	<a href="#">Administering the Cisco Service Path Analyzer</a>	Outlines the sequence of steps involved in setting up a Path Analyzer system, from initial configuration to troubleshooting. Links to each section are provided.
Chapter 2	<a href="#">Preparing for Initial Configuration</a>	Setting up the administrative environment (hardware and software) before initial system configuration. A task checklist is provided.
Chapter 3	<a href="#">Configuring the Cisco Service Path Analyzer Server</a>	Using the Configuration Tool to configure IP interfaces on the Path Analyzer Servers and Listeners. Using the Path Analyzer Management Console to perform additional configuration tasks.
Chapter 4	<a href="#">Installing the Management Console and Upgrading Your Cisco Service Path Analyzer System</a>	Installing, starting, and logging into the Path Analyzer Management Console. Upgrading procedures for software and Listeners.
Chapter 5	<a href="#">Configuring Domains for Your Enterprise</a>	Setting up autonomous systems and routing domains, naming routers and providing route identifiers, managing static routes and next-hop resolution, managing associated administrative tasks.
Chapter 6	<a href="#">Configuring Listeners and Collectors</a>	Adding Listeners, configuring logical connections between the Path Analyzer Server and Listeners, and configuring connections between Collectors and router interfaces. Viewing Server, Listener, and Collector statistics. Removing Path Analyzer appliances.
Chapter 7	<a href="#">Setting Up and Maintaining User Accounts</a>	Viewing, adding, changing and removing user accounts.
Chapter 8	<a href="#">Exporting Alarm Triggers</a>	Exporting alarm triggers from the Alarm Monitor to an SNMP agent or a syslog host.
Chapter 9	<a href="#">XML Configuration Files</a>	Modify the Path Analyzer configuration using XML instead of the Management Console. Importing and exporting XML files.
Chapter 10	<a href="#">Maintaining Your Path Analyzer Database</a>	Exporting and purging the Path Analyzer database for optimal data storage and system performance.
Chapter 11	<a href="#">System Diagnostics and Troubleshooting</a>	Tips for diagnosing and troubleshooting your Path Analyzer system.

## Chapter-Level Organization

Each chapter is structured to provide you with the information you need to complete network management tasks using the 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.
- Graphical User Interface (GUI)—Screen captures and tables that describe the parts of each GUI form, tab, window or dialog box that you need to complete.

## Indicators



### Note

A note provides important information.



### Caution

A caution provides essential information that will prevent damage to the system, equipment, or data. The caution may apply to hardware or software.



### Warning

**A warning provides essential information about avoiding hazardous conditions that can cause personal injury, death, substantial property damage, or massive loss of data, if ignored.**

## Related Documentation

The *Cisco Service Path Analyzer System Administration Guide* is supported by the following related documents:

- *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 User Guide*—Provides information about the following topics:
  - Using the Path Analyzer Management Console.
  - Using the Topology Viewer to obtain a visual snapshot of your network.
  - Using the Event Monitor to view statistics about your network.
  - Using the Service Monitor to create and monitor network end users, departments and services, using visual representations.
  - Using the Real-time Topology Browser to view data about entities in your network.
  - Using Investigative Querying in the Topology Browser to query for specific BGP or OSPF route advertisements or OSPF interfaces.

- Using the Event Log to monitor network events.
- Using the Alarm Monitor to set alarms for network entities, receive notifications when changes occur, and view events that triggered alarms on the network.
- Using the Chart Manager to create charts that depict routers, routing trends, interfaces, and links that have an impact on activity in your network.
- Using the Report Manager to generate pre-defined reports that provide a high-level view of data.
- Using Schedule Manager to schedule charts and reports.
- Using the Supplementary Web Schedule Manager to view and manage schedules and completed tasks.
- *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:
  - Compatible hardware and software platforms.
  - System requirements.
  - Known and fixed software and documentation issues.

## Additional Technical References

The Path Analyzer supports networks that run Open Shortest Path First (OSPF) 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>

## 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: <http://www.rfc-editor.org/rfc/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>
- 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>

## Support for Alarm Trigger Exporting

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 8, “Exporting Alarm Triggers”](#).

## Syslog

For detailed information about the syslog protocol, see the following documents:

### On Supported Unix-Based Operating Systems

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

## From the IETF

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 Simple Network Management Protocol (SNMP) see:

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

# 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

## Administering the Cisco Service Path Analyzer

---

### Getting Started with Administration

The *Cisco Service Path Analyzer Administration Guide* provides information about the initial configuration of your Cisco Service Path Analyzer (hereafter referred to as Path Analyzer) system followed by user account management, and ongoing maintenance and administration.

This guide is divided into two main sections:

- Initial configuration—Chapters that cover initial and advanced configuration tasks.
- System administration—Chapters that describe the following administrator tasks:
  - Setting up and managing user accounts
  - Changing your system configuration by reconfiguring Listeners and Collectors
  - Upgrading your system components
  - Removing your system components

### Initial Configuration and Reconfiguration Tasks

- [Preparing for Initial Configuration, page 2-1](#)
- [Configuring the Cisco Service Path Analyzer Server, page 3-1](#)
- [Installing the Management Console and Upgrading Your Cisco Service Path Analyzer System, page 4-1](#)
- [Configuring Domains for Your Enterprise, page 5-1](#)
- [Configuring Listeners and Collectors, page 6-1](#)
- [Configuring the Listener Connection to the Path Analyzer Server, page 6-14](#)

### User Account Set Up and Maintenance Tasks

- [Setting Up and Maintaining User Accounts, page 7-1](#)
- [Adding a New User Account, page 7-3](#)
- [Changing Details of a User Account, page 7-5](#)
- [Removing a User Account, page 7-6](#)

## System Integration Tasks

- [Integrating Path Analyzer Alarm Triggers into Your NMS, page 8-2](#)
- [Configuring the Export of Alarm Triggers to a Syslog Host, page 8-2](#)
- [Configuring the Export of Alarm Triggers to an SNMP Agent, page 8-5](#)

## Database Management Tasks

- [Starting the Data Management Administration Module, page 10-1](#)
- [Managing Your Data, page 10-2](#)
- [Configuring a Purge, page 10-3](#)
- [Removing Autonomous Systems and Routing Domains, page 5-21](#)

## Component Removal Tasks

- [Removing a Collector, page 6-50](#)
- [Removing a Listener, page 6-50](#)
- [Uninstalling the Management Console, page 4-3](#)

## Upgrade Tasks

- [Upgrading Path Analyzer Software, page 4-5](#)

## Troubleshooting Tasks

- [Troubleshooting a Path Analyzer Appliance, page 11-5](#)
- [Troubleshooting a Collector, page 11-9](#)
- [Uploading Files, page 11-17](#)





## CHAPTER 2

# Preparing for Initial Configuration

---

## Preparation for Configuring your Cisco Service Path Analyzer System

The *Cisco Service Path Analyzer System Administration Guide* provides a set of procedures for basic configuration tasks that enable you to configure Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) quickly and start using it.

The following sections provide a checklist for you to follow during the initial configuration and explain how to set the Administrator's console and terminal emulation settings.

## Path Analyzer Initial Configuration Tasks

- [Using the Initial Configuration Task Checklist, page 2-1](#)
- [Setting the Administrator's Environment, page 2-2](#)

## Using the Initial Configuration Task Checklist

After rack-mounting and connecting your Path Analyzer appliances, use the following checklist to complete the initial configuration of the system.

Print the checklist and mark off each task as you complete it.

For information about rack-mounting and connecting your Path Analyzer appliances, see:

- *Cisco Application Deployment Engine 1010 and 2120 Appliance Hardware Installation Guide*, or
- *Cisco Application Deployment Engine 2130 and 2140 Appliance Hardware Installation Guide*

**Table 2-1 Initial Configuration Task List**

Task	Verified By	Date
Prepare for initial configuration by: <ul style="list-style-type: none"> <li>Connecting the administrator console to the Path Analyzer Server.</li> <li>Setting your virtual terminal emulator from the administrator console.</li> </ul>		
Start the Server Configuration Tool and set the IP interface of your Path Analyzer Server.  <b>Note:</b> Mandatory settings for each Eth( <i>n</i> ) interface include: IP Address, Subnet Mask, and Gateway.		
Install your Path Analyzer Management Console and log in.		
Start the System Administration utility.		
Configure one or more Autonomous System (AS) and OSPF domain.		
Configure one or more Listener.		
Configure one or more Collector.		
Start the Listener Configuration Tool and set the IP interface for each Listener. Repeat this procedure for each Listener in your system.  <b>Note</b> Mandatory settings for each Eth( <i>n</i> ) interface include: IP Address, Subnet Mask, and Gateway.		

## Setting the Administrator's Environment

In order to configure Path Analyzer, you must first connect an administrator's console. This can be done in two ways:

- Using a computer running a virtual terminal (vt100) emulator connected to the Path Analyzer appliance via a serial port, or
- Using a terminal and keyboard connected to the Path Analyzer appliance via a VGA port (terminal) and a USB port (keyboard).

Path Analyzer Servers and Listeners cannot be configured until their interfaces are assigned IP addresses, subnet masks, and gateways. Each Server and Listener in your network must be configured in this way.

For information about configuring a Path Analyzer Server, see [Configuring the Cisco Service Path Analyzer Server, page 3-1](#).

## Connect the Administrator Console (PC)

For information about connecting the Administrator Console, see:

- Cisco Application Deployment Engine 1010 and 2120 Appliance Hardware Installation Guide*, or
- Cisco Application Deployment Engine 2130 and 2140 Appliance Hardware Installation Guide*

## Connect the Administrator's Console (Terminal and Keyboard)

For information about connecting the Administrator Console terminal and keyboard, see:

- *Cisco Application Deployment Engine 1010 and 2120 Appliance Hardware Installation Guide*, or
- *Cisco Application Deployment Engine 2130 and 2140 Appliance Hardware Installation Guide*

## Set Your Virtual Terminal Emulator (for PC Connection Only)

For information about setting the Virtual Terminal Emulator, see:

- *Cisco Application Deployment Engine 1010 and 2120 Appliance Hardware Installation Guide*, or
- *Cisco Application Deployment Engine 2130 and 2140 Appliance Hardware Installation Guide*





## CHAPTER 3

# Configuring the Cisco Service Path Analyzer Server

---

## Configuring Interfaces and Network Information

Once you have connected the administrator's console to a Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) appliance (Server or Listener), you can begin configuring:

- IP addresses and subnet masks on all active Ethernet interfaces
- Speed and duplex settings on all active Ethernet interfaces
- Gateways for all active Ethernet interfaces
- Superior (privileged machine)
- System date and time

See [Initial Configuration: Network Information, page 3-2](#) to configure network information.

See [Initial Configuration: Setting the Date and Time, page 3-4](#) to set the date and time.

## The Configuration Tool

The Configuration Tool is a command line interface (CLI) utility tool available from both serial and VGA consoles. It is used for initial system setup and for system troubleshooting and recovery.

Once the Administrator's Console is booted, you see the following sequence of events:

- 
- Step 1** The BIOS Screen appears.
- Step 2** Kernel starts and mounts disks, showing boot messages.
- Step 3** The following text appears (Server version shown) followed by the setup prompt:

```
Server configuration (version R_1-0_0)
superior = 192.168.0.20
authport = 1050
comport = 1051
poll = 1200
ftphost =
```

```

ftpuser =

eth0 = 192.168.0.123/255.255.255.0 gw = 192.168.0.1 speed = auto/auto
speed = auto/auto

eth1 = 0.0.0.0/0.0.0.0 gw = 0.0.0.0 speed = auto/auto

useful commands

show          show configuration
configure     configure network,
configure all  configure everything
save          save changes
help          list of commands

setup> save

Wrote /etc/iptivia/firewall.cfg (superior = 192.168.0.20) Wrote
/etc/sysconfig/iptables Wrote /etc/iptivia/init_script.txt Wrote
/usr/share/iptivia/ftp Wrote /etc/sysconfig/network (gw =
192.168.0.1, gwdev = eth0) Wrote
/etc/sysconfig/network-scripts/ifcfg-eth0
(192.168.0.123/255.255.255.0)

Wrote /etc/sysconfig/network-scripts/ifcfg-eth1 (0.0.0.0/0.0.0.0)
Restarting other configtool instances

```

If you are connected to a Path Analyzer Server, as in the example above, you see two Ethernet interfaces (0 and 1).

If you are connected to a Path Analyzer Listener, you see four Ethernet interfaces (0, 1, 2, and 3).

## Initial Configuration: Network Information

To configure the network information:

- 
- Step 1** Start by entering the `configure` command at the setup prompt.
  - Step 2** Enter a superior address.
    - For a Server, enter the IP address of the machine running the Path Analyzer GUI.
    - For a Listener, enter the IP address of the associated Path Analyzer Server.
  - Step 3** Enter the IP address, netmask, and gateway for the first interface you wish to use.
  - Step 4** Enter the speed/duplex for the first interface you wish to use. You can leave the default if you wish [0]  
auto/auto

- Step 5** Configure the remaining interfaces you wish to use.
- Step 6** Enter **save** to save your changes
- Step 7** Restart the network.
- 

A sample Server configuration is shown below.

```
setup> configure

Admin IP address (GUI access)
superior [0.0.0.0] 192.168.0.20

eth0 interface
Address [0.0.0.0] 192.168.0.123
Netmask [0.0.0.0] 255.255.255.0
Gateway [0.0.0.0] 192.168.0.1
    0 auto/auto
    1 10/half
    2 10/full
    3 100/half
    4 100/full
    5 1000/full

Speed/duplex [0]

eth1 interface
Address [0.0.0.0]

use 'save' to save changes
You also need to restart the network.
setup(save)>
```

In this example, only eth0 was configured.

At this point, no changes have been made to the system files. To save your changes, use the **save** command.

Notice that the prompt changes to `setup(save)>` to remind you that you have unsaved changes.

Next, save your changes.

```
setup(save)> save

Wrote /etc/iptables/firewall.cfg (superior = 192.168.0.20)
Wrote /etc/sysconfig/iptables
```

```
Wrote /etc/iptivia/init_script.txt
Wrote /etc/sysconfig/network (gw = 192.168.0.1, gwdev = eth0)
Wrote /etc/sysconfig/network-scripts/ifcfg-eth0
(192.168.0.123/255.255.255.0)
Wrote /etc/sysconfig/network-scripts/ifcfg-eth1 (0.0.0.0/0.0.0.0)
```

You need to restart the network to take changes into account:

```
setup(network restart)>
```

You see where each file is saved, and its corresponding values.

The final step is to restart the network and the Path Analyzer Server.

```
setup(network restart)>network restart
Shutting down interface eth0: [ OK ]
Shutting down interface eth1: [ OK ]
Shutting down loopback interface: [ OK ]
Setting network parameters: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: [ OK ]
Bringing up interface eth1: [ OK ]
setup> service restart

setup(service restart)>
Sending KILL signal to 27263
Stopping server (pid 27263.
Starting MySQL SUCCESS!
Starting server
setup>
```

Now you should be able to access your Path Analyzer appliance through the network.

## Initial Configuration: Setting the Date and Time

The **date** command displays the current system date and time. You can set the date and time manually or with Network Time Protocol (NTP).

### Setting the Date and Time Manually

Enter a new date and/or time as arguments to the **date** command:

```
setup> help date
date [MM/DD/YYYY] [hh:mm[:ss]]
setup> date 12:34
Current date: Jan 17 11:05:28 2007
```



```

New date: Jan 17 12:34:00 2007
setup> date 12:34:56
Current date: Jan 17 12:34:09 2007
New date: Jan 17 12:34:56 2007
setup> date 12/31/2011
Current date: Jan 17 12:36:40 2007
New date: Dec 31 12:36:40 2011
setup> date 12/31/2006 18:00
Current date: Dec 31 12:36:25 2011
New date: Dec 31 18:00:00 2006

```

## Setting the Date and Time Using NTP

If you have access to an NTP server, you can use it to set the correct date and time:

```

setup> ntpdate 192.168.1.11

17 Jan 11:28:50 ntpdate[8515]: step time server 192.168.1.11 offset
144.252415 sec

```



### Note

The **ntpdate** command calls the ntpdate system command, it does not configure the NTP server. To configure an NTP server, use the Path Analyzer GUI client.

If you have configured a DNS server on your Path Analyzer appliance, you can use host name with the ntpdate command. Otherwise, you must use an IP address. To configure a DNS server, use the Path Analyzer GUI client.

After completing these configuration tasks, refer to the Initial Configuration Checklist provided in [Preparing for Initial Configuration, page 2-1](#) before completing the next task, [Downloading and Installing the Management Console \(GUI\), page 4-3](#).

## Configuration Tool Command List

[Table 3-1](#) provides a complete list of Configuration Tool commands

**Table 3-1 Configuration Tool Command List**

Command	Usage and Description
configure	<b>Usage:</b> configure [all] Without argument, only the network is configured. With configure all, you can modify additional parameters, such as port numbers. Only use configure all if instructed by the Cisco support team.
date	<b>Usage:</b> date [MM/DD/YYYY] [hh:mm[:ss]] Without argument, shows the current date and time You can specify a date or time to set the clock to the desired value.

**Table 3-1 Configuration Tool Command List (continued)**

Command	Usage and Description
diag	<p><b>Usage:</b> diag [all hard sys proc rpm]</p> <p>The diag command calls the diagtool utility.</p> <p>Perform diagnostics:</p> <p>all</p> <p>Perform all diagnostic checks (default).</p> <p>hard</p> <p>Perform some hardware tests: machine type and CPU, temperature, voltages, power redundancy and RAID checks (if applicable).</p> <p>sys</p> <p>Current system check: Only memory occupation is tested at present.</p> <p>proc</p> <p>Verify that critical processes and services are running.</p> <p>rpm</p> <p>Verify files against RPM (Redhat Packet Maintenance) database.</p>
firewall	<p><b>Usage:</b> firewall [off reset status host]</p> <p>Controls the firewall rules.</p> <p>off</p> <p>Disable all rules; the firewall will be restarted if you restart the Path Analyzer service or reboot.</p> <p>reset</p> <p>Re-initialize rules as set by the Path Analyzer Server or Listener.</p> <p>status</p> <p>Display current rules.</p> <p>address</p> <p>Allow all connections from the given address; can be a host address (e.g.: 192.168.12.34), network address (e.g.: 192.168.0.0/16 or 192.168.0.0/255.255.0.0), or host name (if DNS is configured).</p>
help	<p><b>Usage:</b> help [command]</p> <p>Display help messages. When no command is given, displays the list of all commands.</p> <p>With a command, shows the usage.</p>

**Table 3-1 Configuration Tool Command List (continued)**

Command	Usage and Description
ifconfig	<b>Usage:</b> ifconfig [interface] Displays the output from the ifconfig system command. For display only; to configure network and other parameters, use configure.
ifdown	<b>Usage:</b> ifdown interface Brings a network interface down, using the ifdown system command.
ifup	<b>Usage:</b> ifup interface Brings a network interface up, using the ifup system command.
service	<b>Usage:</b> service start stop restart status Controls the Path Analyzer service.
log	<b>Usage:</b> log service syslog Displays Path Analyzer log and syslog.
network	<b>Usage:</b> network restart status Controls the network.
ntpdate	<b>Usage:</b> ntpdate host Ntpdate command synchronizes with an NTP server. If DNS is configured, you can specify a host name; otherwise, use an IP address.
ping	<b>Usage:</b> ping host Used to troubleshoot network connectivity problems. Ping command: sends 5 ICMP packets to the specified host. If DNS is configured, you can specify a host name; otherwise, use an IP address.
quit, exit, bye	Quit the configtool utility. If there are unsaved changes, a confirmation is required.  On the serial and VGA connections, configtool is executed by init, so quitting will result in configtool being restarted on the terminal. This is helpful if you wish to see the initial banner which shows the version information, or if you made changes that you do not want to save.  When started from a shell session, quit returns the user to the shell.
reboot, halt	<b>Usage:</b> reboot, halt Reboot or halt the system.  The Path Analyzer service is stopped during the system shutdown. A confirmation is requested before proceeding.

**Table 3-1 Configuration Tool Command List (continued)**

Command	Usage and Description
resetpass	<b>Usage:</b> resetpass Only available on a Server. Instructs the Path Analyzer Server to re-initialize the admin password. You need to save your changes and then restart the Path Analyzer service to reset the password.
resetssh	<b>Usage:</b> resetssh Disable AllowUsers in the sshd configuration. When combined with the firewall command, this command is used to access your machine when GUI access does not work.
save	<b>Usage:</b> save [force] Save changes to the system files. You may need to reboot or restart the network or Path Analyzer services to have the system take them into account. Use save force to force an update of the system files even if the configtool reports no changed variables.
show	<b>Usage:</b> show Shows the current configuration.
upgrade	<b>Usage:</b> upgrade URL Upgrades the machine from a Web server. The URL <u>must</u> start with <i>http://</i> and end with <b>iub</b> .
user	<b>Usage:</b> user add del list [user] Facilitates user management.
version	<b>Usage:</b> version Displays the version of Path Analyzer components.

## Reconfiguring a Path Analyzer Server

Additional configuration of the Path Analyzer Server can be completed directly from the Path Analyzer Management Console.

The following configuration tasks can be completed serially, in the following order, using the Path Analyzer Server Configuration wizard:

- [Configure Packet Marking Parameters, page 3-10](#)
- [Configure SNMP Trap/Polling Destination Parameters, page 3-11](#)
- [Set a System Login Banner, page 3-12](#)
- [Set System Users, page 3-13](#)
- [RADIUS Server Configurations, page 3-13](#)
- [DNS Server Configuration, page 3-15](#)

- [NTP Server Configuration, page 3-16](#)
- [OSPF Convergence Monitor Parameters, page 3-16](#)
- [Configure Web Server Parameters, page 3-17](#)
- [Setting Firewall Parameters, page 3-19](#)
- [Configure Access, page 3-20](#)

## Start System Administration

To start Path Analyzer system administration, click **Start > Administration > System** from the Path Analyzer taskbar.

The System Administration window appears.

## Start the Path Analyzer Server Configuration Wizard

This section details each screen of the Path Analyzer Server Configuration wizard.

To start the Path Analyzer Server Configuration wizard and configure additional Path Analyzer Server settings:

---

**Step 1** Go to the configuration tree in the left side of the window and select the Path Analyzer Server.

**Step 2** Go to the **Configuration** tab and click **Reconfigure**.

The Path Analyzer Server Configuration wizard starts, and displays the set Packet Marking Parameters screen (see [Figure 3-1](#)).

---

## Configure Packet Marking Parameters

**Figure 3-1** Packet Marking Parameters Screen in the Server Configuration Wizard

To configure packet marking parameters:

- 
- Step 1** Follow the procedure to [Start the Path Analyzer Server Configuration Wizard, page 3-9](#).
- Step 2** Select and complete the following options:
- **Ethernet Port**—Select a port from the drop-down box, which will mark all outgoing traffic.
  - **Protocol Port**—Select a protocol from the drop-down box, such as TCP or OSPF. This indicates the type of traffic you want to mark.
  - **Source Port**—Enter the source port to mark traffic originating from the Path Analyzer Server. Use the \* to indicate any source port.
  - **Destination Port**—Enter the destination port. Use the \* to indicate any destination port.
  - **DSCP Marking**—Differentiated Services Code Point Marking sets priorities for outgoing packets by marking them with specific DSCP numbers. These numbers can be associated with a specific group, department, or service (for example, customer service or voice service).
- Step 3** Click **Add**.
- The information appears on the table, and then it is set on the device.
- Step 4** Click **Next**.
- The SNMP Trap/Polling Destination Parameters screen appears (see [Figure 3-2](#)).
-

## Configure SNMP Trap/Polling Destination Parameters

**Figure 3-2** *SNMP Trap/Polling Screen in the Server Configuration Wizard*

Cisco Service Path Analyzer Server Configuration

### Cisco Service Path Analyzer Server Configuration Wizard

Please set the SNMP Trap/Polling Destination parameters.

☒ Do you want to enable SNMP Traps?

Monitor Java: yes ▼

Monitor Database: yes ▼

Monitor CPU/Disk: yes ▼

Monitor Collectors: yes ▼

Monitor Configuration: yes ▼

SNMP Version: v2c ▼

Trap Receiver:

Community: public

Port: 162

Location:

Contact:

☒ Do you want to enable SNMP Polling?

Community: public

< Back   Next >   Cancel

The SNMP Trap/Polling screen allows you to choose whether the Path Analyzer Server should generate and send SNMP traps to a network management system as well as receive them from the NMS.

To set SNMP trap/polling destination parameters:

- 
- Step 1** Click the check box **Do you want to enable SNMP Traps?**
- Step 2** Select and complete the following options to set the parameters for monitoring the device.
- **Monitor Java**—Selecting **Yes** enables the JAVA processes running on the Path Analyzer Server to be monitored. A trap is sent to the network management system if one of the JAVA processes goes down. The default is **Yes**.
  - **Monitor Database**—Selecting **Yes** enables the system to monitor the operation of the database. If the database goes down, the Path Analyzer server sends a trap to the network management system. The default is **Yes**.
  - **Monitor CPU/Disk**—Selecting **Yes** enables the system to monitor CPU use and disk space. The default is **Yes**.
  - **Monitor Collectors**—Selecting **Yes** enables the system to monitor any change in the state of the Collectors. The default is **Yes**.
  - **Monitor Configuration**—Selecting **Yes** enables the system to monitor any changes in the configuration. The default is **Yes**.
  - **SNMP Version**—Input the version of traps your SNMP management device should receive. The default setting is **SNMP v2c**.
  - **Trap Receiver**—Enter the destination that should receive the traps from the device.

- **Community**—Enter the appropriate string or password designated for receiving devices that use SNMP. The default setting is **Public**.
- **Port**—Enter the SNMP port to which the Path Analyzer Server sends traps. The default is **162**.
- **Location**—(Optional) You can enter the server name or the trap receiver the Path Analyzer Server uses.
- **Contact**—(Optional) You can enter the name of the network administrator or other individual responsible for managing Path Analyzer.

**Step 3** Click the check box to enable **SNMP Polling**.

**Step 4** Enter the appropriate string or password designated for the network management system or sending devices that use SNMP in the bottom Community field. The default setting is **public**.

**Step 5** Click **Next**.

The Set System Login Banner screen appears (see [Figure 3-3](#)).

## Set a System Login Banner

**Figure 3-3** System Login Banner Screen in the Server Configuration Wizard



The Set System Login Banner screen permits you to set up a banner that appears to system users (SSH) when they log in. You have any option to set up the banner and a box to enter the banner text.

To set a system login welcome message:

**Step 1** Click the check box and enter the banner text to be displayed to users when they log in. If you do not want to set a login message, leave the check box unchecked.

**Step 2** Click **Next**.

The Set System Users screen appears (see [Figure 3-4](#)).



## Set System Users

**Figure 3-4** System Users Screen in the Server Configuration Wizard

Cisco Service Path Analyzer Server Configuration Wizard

Please set System Users

☒ Do you want to enable System Users for SSH Access?

User Name	Password
cli	*****
admin	*****

Add Remove

User Name:

Password:

(Leave password field empty if you want to use Radius authentication.)

< Back Next > Cancel

The Set System Users screen enables you to create a password and user name for system users (SSH) who wish to access Path Analyzer.

To create system user accounts:

- 
- Step 1** Click the check box and enter the user name and password of each user in the appropriate field. If you do not want to create user accounts at this time, leave the check box unchecked.
  - Step 2** Click **Add** after each entry.  
The name and password appear in the box above.
  - Step 3** Click **Next**.  
The Configure RADIUS Server screen appears (see [Figure 3-5](#)).
- 

## RADIUS Server Configurations

The primary RADIUS (Remote Authentication Dial In User Service) Server authenticates Management Console access and SSH access to the Path Analyzer Server for system users. The secondary RADIUS Server acts as a backup for the primary server if the primary server does not respond with the appropriate access within the designated timeout period. The RADIUS checks that the user name and password information is correct, using the PAP authentication scheme.



### Note

The RADIUS authentication feature is disabled by default unless you deliberately turn it on.

**Figure 3-5** *RADIUS Settings in Server Configuration Wizard*

To configure RADIUS servers:

- 
- Step 1** To configure a primary RADIUS server, click the check box: **Do you want to enable RADIUS?**
- Step 2** To configure a secondary RADIUS server click the check box **Do you want to add a secondary RADIUS Server?**
- Step 3** Complete the Default User Type field under the first check box by selecting a user type (limited, admin, or power) from the drop-down menu. Path Analyzer creates a new account with this user type and associated user preferences when a new user logs in via the login screen of the Management Console.
- Step 4** Complete the remaining fields under both check boxes:
- **Hostname**—Enter the IP address or host name of the RADIUS Server that is used to authenticate users.
  - **Timeout(s)**—Accept the default timeout or enter a timeout period. The timeout period specifies number of seconds the Path Analyzer Server waits for a reply to a RADIUS request before retransmitting the request. The default is 15 seconds.
  - **Port Number**—The port number specifies the destination port. Enter the port number or accept the default.
  - **Secret Key**—Enter the secret key for the RADIUS Server. The secret key specifies the shared secret text string used between the Path Analyzer Server and the RADIUS Server, used to encrypt passwords and exchange responses.
- Step 5** Click **Next**.

The Set DNS Server screen appears (see [Figure 3-6](#)).

---

If RADIUS authentication is enabled, users are authenticated against RADIUS when they log in for the first time, unless they have already been explicitly added into the RD Management Console. See [Adding a New User Account](#), page 7-3.

During their first login, new users are automatically assigned the default type according to the default parameters previously configured in the Management Console. User access types can be changed (to “admin,” for example). See [Changing Details of a User Account, page 7-5](#).

Users added via the RD Management Console are set to authenticate locally. See [Adding a New User Account, page 7-3](#) to add users to the Management Console.

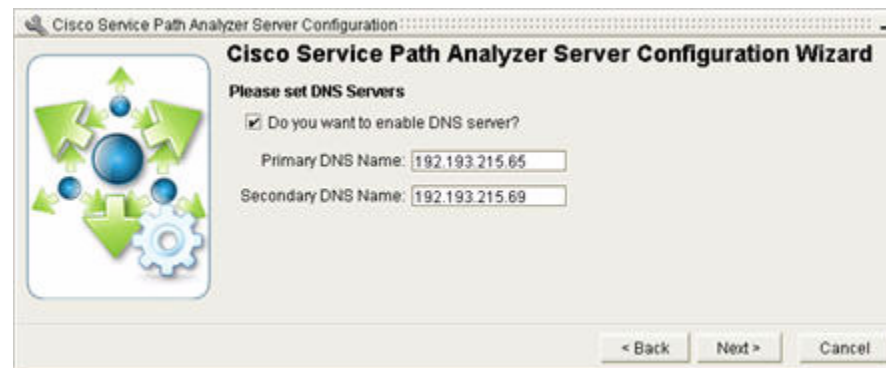
**Note**

The Serial Setup Tool can be used to reset the default password of the administrator’s account to admin.

The RADIUS authentication for systems users (SSH) is different. Once RADIUS is configured, all system users are authenticated against RADIUS. The local password will only be used if RADIUS is down.

## DNS Server Configuration

**Figure 3-6** DNS Server Settings in the Server Configuration Tool



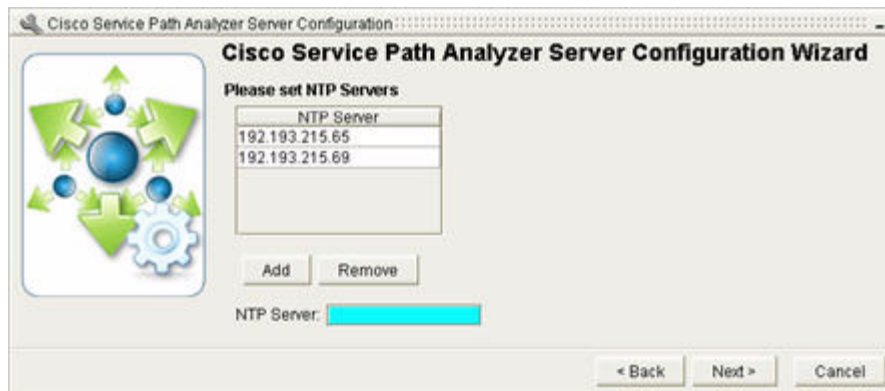
To enable a DNS server:

- Step 1** Click the check box **Do you want to enable DNS server?** and complete the following fields:
- Primary DNS Name—Enter the name or IP address of the primary DNS server.
  - Secondary DNS—In this optional field, enter the name or IP address of the backup DNS server.
- Step 2** Click **Next**.

The NTP Server Configuration screen appears (see [Figure 3-7](#)).

## NTP Server Configuration

**Figure 3-7** NTP Server Configuration Screen in the Configuration Tool



To enable an NTP server:

- 
- Step 1** Complete the NTP Server field by entering the IP address or DNS name of the NTP Server.
  - Step 2** Click **Add**.
  - Step 3** Click **Next**.

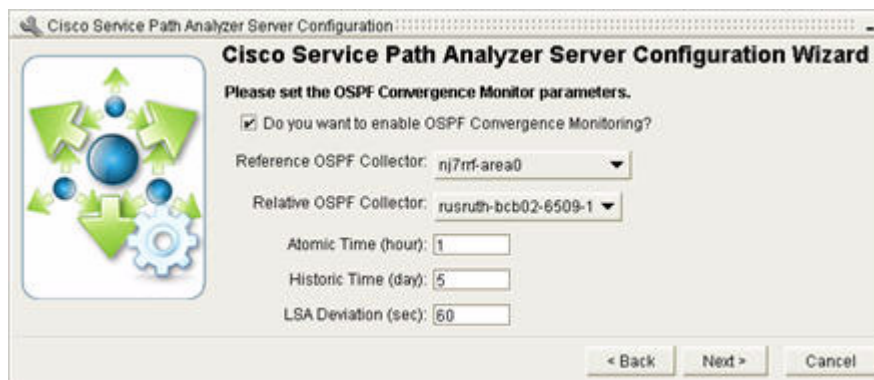
The OSPF Convergence Monitor Parameters screen appears (see [Figure 3-8](#)).

---

## OSPF Convergence Monitor Parameters

OSPF Convergence Monitors measures the propagation delay of OSPF LSAs across the network. To enable convergence measurements you must administer OSPF Collectors on two Listeners. (The first Collector is referred to as a Reference Collector, the second, a Relative Collector.) You should locate these Listeners in the same area and as far apart as possible to obtain the most accurate convergence data.

**Figure 3-8** OSPF Convergence Monitor Parameters



To set OSPF Convergence Monitoring:

- 
- Step 1** Click on the check box **Enable OSPF Convergence Monitoring?** and complete the following fields:

- Reference OSPF Collector—Select the Reference Collector from the drop-down menu.
- Relative OSPF Collector—Select the Relative Collector from the drop down-menu.

**Note**

Make sure that your Collectors are in the same domain and the same area. To obtain this information, click on the Collector name in the hierarchical menu on the left side of the System Administration screen and then select the **Configuration** tab.

Although all your Collectors will appear on the drop-down menu, you can only collect OSPF Convergence information from one area at a time. If you wish to check another area, you must run a process again with Collectors from that area.

- Atomic Time (hour)—Accept the default Atomic Time or enter the time period for recording OSPF Convergence periods. The default time is one hour; each OSPF log will record all convergence data in one-hour intervals.
- Historic Time (day)—Enter the amount of time the system should retain a historic record of each convergence measurement. The default setting is 5 days.
- LSA Deviation (sec)—Enter the time period within which the device should look for a matching LSA before discarding it. The default period is 60 seconds.

**Step 2** Click **Next**.

The Web Server Parameters screen appears (see [Figure 3-9](#)).

## Configure Web Server Parameters

**Figure 3-9** Screen for Configuring Web Server Parameters



This feature allows you to enable Web servers so users can access reports and Convergence logs from a browser-enabled computer without having to deploy the Path Analyzer Management Console.

The Web servers are enabled by default, so to leave them enabled, simply click **Next**:

- The Apache and TomCat Web servers are enabled.
- You can disable the Web servers if you do not want to allow HTTP access.
- The Set Certificate Parameters screen appears (see [Figure 3-10](#)).

You may need to request a certificate if you have not already received one from a certification authority. This is a three-step process which you initiate from the Path Analyzer Server Configuration wizard.

**Figure 3-10** Certificate Parameters on the Server Configuration Wizard

Cisco Service Path Analyzer Server Configuration Wizard

Please set Certificate Parameters

☐ Do you want to generate new Certificate request?

Step 1: Fill in the parameters to create a certificate request:

Country:

State:

Local:

Organization:

OU:

CN(required):

Email:

Step 2: Send the below certificate request to your authority:

Certificate Request

Step 3: Copy and paste the certificate from your authority:

Certificate

< Back   Next >   Cancel

To configure certificate parameters:

- 
- Step 1** Obtain a CSR (certificate request) for the Path Analyzer Server:
- Open the Path Analyzer Server Configuration wizard.
  - Access the Certification screen. Complete the following fields:
    - Country**—Enter the two-digit country code for your country.
    - State**—Enter the two-letter code for your state.
    - Local**—Enter your city or locality.
    - Organization**—Enter the name of your organization.
    - OU**—Enter your organization unit.
    - CN (required)**—Enter your server's DNS name or IP address.
    - Email**—Enter your e-mail address.
  - Click **Next** to send the request to the Server.
- Step 2** Obtain CSR from the Server:
- Access the Certification screen using the Path Analyzer Server Configuration wizard.
  - Find your CSR string in the Certificate Request field under **Step 2**.
  - Copy the CSR string and send it to the Certification Authority to obtain a Security Certificate.




- Step 3** Obtain the Certificate from the Certificate Authority:
- Paste the Certificate you receive into the **Certificate** field under **Step 3** on the same screen.
  - Click **Next** and validate the configuration to install the new certificate on the Path Analyzer Server.
- The Set Firewall Parameters screen appears (see [Figure 3-11](#)).

## Setting Firewall Parameters

You can activate a firewall to secure your Path Analyzer Server. Firewall rules specify the transmission criteria for all packets and targets. Packets that do not satisfy the firewall rules will be dropped. Decide which services you want to grant access to and then complete the following procedures:

**Figure 3-11** Firewall Settings Screen in Server Configuration Wizard



Cisco Service Path Analyzer Server Configuration

### Cisco Service Path Analyzer Server Configuration Wizard

Please set the Firewall setting parameters

☒ Do you want to enable Firewall?

Choose A Service

☐ Web Management Console

☐ SSH

☐ SPA Management Console

☐ SNMP

Allowed IP Addresses

Add Delete

☐ Prohibit the system from connecting to non-listed networks

Additional allowed Subnets:

Add Delete

**WARNING:** Be careful when assigning firewall rules. You may inadvertently block communications between Cisco Service Path Analyzer appliances. Add the IP addresses of any machines that require access to this Server, especially machines serving as Management Consoles.

To set firewall parameters:

- Step 1** The firewall is enabled by default; you can disable it by removing the check mark. Choose a service that the firewall should grant access to:
- Web Management Console
  - Secure Shell (SSH)
  - Path Analyzer Management Console

- Simple Network Management Protocol (SNMP) Console

**Step 2** Enter the IP addresses of the subnets that you want to grant access to via the specified service.

**Step 3** Click **Add**.

The information appears in the table, and then it is sent to the device.

The established connections are outbound connections. The Path Analyzer Server will be allowed to initiate outbound connections to any listed networks.

---

## Configure Access

To restrict access to a specific service, click the button next to the service you wish to restrict.

To prohibit the system from connecting to non-listed networks, check the **Prohibit the system from connecting to non-listed networks** checkbox.

To permit access to a specific service not listed on the screen:

---

**Step 1** Complete one of these options:

- uncheck the box next to **Prohibit the system from connecting to non-listed networks**,  
*or*
- enter the IP address of a specific subnet in the field next to **Add**.

**Step 2** Click **Add**.

The information appears in the above box. Repeat the process to define a connection with another subnet, or

**Step 3** Click **Next** to complete the Firewall configuration process.

**Step 4** Click **Finish** when the Server configuration is complete.

---

## To Override Default or Normal Settings

In the event that you encounter a configuration problem with the initial setup that you cannot resolve in the Management Console, you can use the Configuration Tool. You have a choice of the following commands:

- `firewall ip address`, or
- `firewall off`

The first command allows you to enter a network address (if you are connecting remotely). It permits you to make changes to the Path Analyzer Server.

The second command disables the firewall and allows you to make changes.

See [The Configuration Tool, page 3-1](#).



## Path Analyzer Server Port Assignments

Table 3-2 provides the default port settings for the Path Analyzer Server.

**Table 3-2**      *Default Ports Required for Path Analyzer Server*

Protocol/Port	Function
<b>TCP</b> 1050 Authentication port 1051 Connection port 1099 RMI port	Required Connection to management console
<b>TCP</b> 22 Secure shell 1061 Communication port	Required SSH connection
<b>TCP/UDP</b> 53 DNS <b>UDP</b> 123 NTP	Required Outbound
<b>TCP</b> 1812 RADIUS <b>TCP/UDP</b> 49 TACACS <b>UDP</b> 162 SNMP Trap	Optional Outbound
<b>UDP</b> 161 SNMP	Optional Inbound
<b>TCP</b> 80 Apache HTTP 80443 HTTPS	Optional Web interface

## Path Analyzer Listener Port Assignments

Table 3-3 provides the default port settings for the Path Analyzer Listener.

**Table 3-3** Default Ports Required for Path Analyzer Listener

Protocol/Port	Function
<b>TCP</b> 22 Secure shell 1061 Communication port	SSH connection
<b>TCP</b> 179 BGP	Required Outbound
<b>UDP</b> 123 NTP	
<b>TCP/UDP</b> 53 DNS	
<b>IP</b> 47 GRE 89 OSPF	
<b>TCP</b> 1812 RADIUS	Optional Outbound
<b>TCP/UDP</b> 49 TACACS	
<b>IP</b> 47 GRE 89 OSPF	Required Inbound
<b>UDP</b> 161 SNMP	Optional Inbound

## Firewall Rules Sample

The following is an example of the default rules that are added when you enable the firewall. Both the Server and Listener are shown.

### Path Analyzer Server

```
[root@i386-server-eth1 ~]# iptables -n -v -t filter --list
Chain INPUT (policy DROP 2 packets, 56 bytes)
```

target	prot	opt	in	out	source	destination
ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0
ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0

```

ACCEPT    tcp    --    *    *    192.168.25.102    0.0.0.0/0    tcp    dpt:80
ACCEPT    tcp    --    *    *    192.168.25.133    0.0.0.0/0    tcp    dpt:80
ACCEPT    tcp    --    *    *    192.168.25.102    0.0.0.0/0    tcp    dpt:443
ACCEPT    tcp    --    *    *    192.168.25.133    0.0.0.0/0    tcp    dpt:443
ACCEPT    tcp    --    *    *    192.168.25.102    0.0.0.0/0    tcp    dpt:1050
ACCEPT    tcp    --    *    *    192.168.25.133    0.0.0.0/0    tcp    dpt:1050
ACCEPT    tcp    --    *    *    192.168.25.102    0.0.0.0/0    tcp    dpt:1051
ACCEPT    tcp    --    *    *    192.168.25.133    0.0.0.0/0    tcp    dpt:1051
ACCEPT    tcp    --    *    *    192.168.25.102    0.0.0.0/0    tcp    dpt:1099
ACCEPT    tcp    --    *    *    192.168.25.133    0.0.0.0/0    tcp    dpt:1099
ACCEPT    tcp    --    *    *    192.168.25.0/24    0.0.0.0/0    tcp    dpt:161
ACCEPT    udp    --    *    *    192.168.25.0/24    0.0.0.0/0    udp    dpt:161
ACCEPT    tcp    --    *    *    192.168.25.102    0.0.0.0/0    tcp    dpt:22
ACCEPT    tcp    --    *    *    172.16.60.20      0.0.0.0/0    tcp    dpt:1061
ACCEPT    tcp    --    *    *    172.16.60.20      0.0.0.0/0    tcp    dpt:1099
ACCEPT    tcp    --    *    *    172.16.60.20      0.0.0.0/0    tcp    dpt:22
REJECT    tcp    --    *    *    0.0.0.0/0          0.0.0.0/0    tcp
flags:0x12/0x12 state NEW reject-with tcp-reset
DROP      tcp    --    *    *    0.0.0.0/0          0.0.0.0/0    tcp
flags:!0x16/0x02 state NEW
ACCEPT    all    --    *    *    192.168.25.102    0.0.0.0/0    state
ESTABLISHED
ACCEPT    all    --    *    *    192.168.25.133    0.0.0.0/0    state
ESTABLISHED
ACCEPT    all    --    *    *    192.168.25.0/24    0.0.0.0/0    state
ESTABLISHED
ACCEPT    all    --    *    *    1.1.0.0/16        0.0.0.0/0    state
ESTABLISHED
ACCEPT    all    --    *    *    172.16.10.100     0.0.0.0/0    state
ESTABLISHED
ACCEPT    all    --    *    *    192.168.25.25     0.0.0.0/0    state
ESTABLISHED
ACCEPT    all    --    *    *    192.168.25.254    0.0.0.0/0    state
ESTABLISHED
ACCEPT    all    --    *    *    172.16.60.20      0.0.0.0/0    state
ESTABLISHED

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
Chain OUTPUT (policy ACCEPT 4053 packets, 1398K bytes)

```

**Path Analyzer Listener**

```
[root@i386-listener-eth1 ~]# iptables -n -v -t filter --list
```

```
Chain INPUT (policy DROP 47 packets, 4048 bytes)
```

target	prot	opt	in	out	source	destination	
ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	
ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	
ACCEPT	tcp	--	*	*	192.168.25.102	0.0.0.0/0	tcp dpt:161
ACCEPT	udp	--	*	*	192.168.25.102	0.0.0.0/0	udp dpt:161
ACCEPT	tcp	--	*	*	192.168.25.0/2	0.0.0.0/0	tcp dpt:22
ACCEPT	89	--	*	*	10.10.0.0/16	0.0.0.0/0	
ACCEPT	47	--	*	*	10.10.0.0/16	0.0.0.0/0	
ACCEPT	tcp	--	*	*	172.16.60.2	0.0.0.0/0	tcp dpt:1061
ACCEPT	tcp	--	*	*	172.16.60.2	0.0.0.0/0	tcp dpt:1099
ACCEPT	tcp	--	*	*	172.16.60.2	0.0.0.0/0	tcp dpt:22
REJECT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp
flags:0x12/0x12 state NEW reject-with tcp-reset							
DROP	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp
flags:!0x16/0x02 state NEW							
ACCEPT	all	--	*	*	192.168.25.102	0.0.0.0/0	state
ESTABLISHED							
ACCEPT	all	--	*	*	192.168.25.0/24	0.0.0.0/0	state
ESTABLISHED							
ACCEPT	all	--	*	*	10.10.0.0/16	0.0.0.0/0	state
ESTABLISHED							
ACCEPT	all	--	*	*	172.16.10.100	0.0.0.0/0	state
ESTABLISHED							
ACCEPT	all	--	*	*	192.168.25.25	0.0.0.0/0	state
ESTABLISHED							
ACCEPT	all	--	*	*	192.168.25.252	0.0.0.0/0	state
ESTABLISHED							
ACCEPT	all	--	*	*	172.16.60.2	0.0.0.0/0	state
ESTABLISHED							
TCP-MD5	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
```

```
Chain OUTPUT (policy ACCEPT 1845 packets, 760K bytes)
```

target	prot	opt	in	out	source	destination
TCP-MD5	all	--	*	*	0.0.0.0/0	0.0.0.0/0

Chain TCP-MD5 (2 references)





## CHAPTER 4

# Installing the Management Console and Upgrading Your Cisco Service Path Analyzer System

---

Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) is shipped with the software pre-installed. As part of the installation process, you will need to download the Management Console (GUI).

When a new release of the software becomes available, you will want to update your Path Analyzer software. A Cisco account representative will provide you with a CD containing an upgrade file.

All of these processes are explained in this chapter as well as the necessary pre-installation requirements for the Path Analyzer Management Console.



### Note

Except for upgrading the Path Analyzer Management Console, all upgrade tasks are reserved for Path Analyzer administrator users. Before you can begin updating and rebooting the Path Analyzer Server, you are prompted to log in using the Path Analyzer administrator user name and password.

## Path Analyzer Installation and Upgrading Procedures

- [Reviewing Pre-Installation Requirements, page 4-1](#)
- [Loading a New Software Release, page 4-2](#)
- [Downloading and Installing the Management Console \(GUI\), page 4-3](#)
- [Upgrading Path Analyzer Software, page 4-5](#)
- [Upgrading the Listeners, page 4-12](#)

## Reviewing Pre-Installation Requirements

The Path Analyzer Management Console provides a visual, real-time display of your network topology, router paths, events, and alarms.

## Hardware Requirements

Path Analyzer Management Console is meant to run on hardware with the following minimum specifications:

- Processor equivalent to 800 megahertz processing power. Recommended minimum: Intel® Pentium® Celeron® processor.
- 256 Megabytes of Random Access Memory (RAM) minimum.
- Graphics card that can achieve 1024 x 768 pixels.

## Software Requirements

Path Analyzer Management Console runs in the following operating environments:

- Microsoft Windows XP, NT, or 2000.
- Unix-based Operating Systems—Please check with your Cisco Technical Support representative for supported distributions.

## Loading a New Software Release

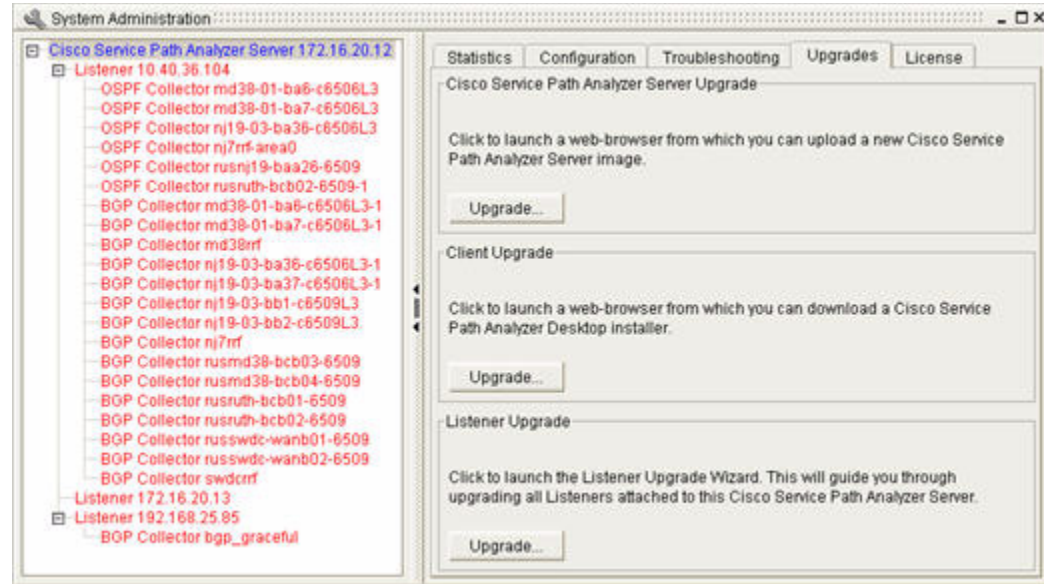
As new versions of Path Analyzer software become available, your Cisco account representative will provide you with a CD containing an upgrade file. To upgrade your system, you will need to load the upgrade software on a local PC or on a local or remote network server.

### Load a New Release

To load a new release of Path Analyzer:

- 
- Step 1** Insert the Path Analyzer upgrade CD in your CD-ROM or CD-RW drive. On many computers, the CD-ROM or CD-RW drive is configured as the D: or E: drive.
- Step 2** Copy the files to your hard drive or a local or remote network server.
- Path Analyzer software can now be installed from the System Administration window (see [Figure 4-1](#)) of the Administration Module.



**Figure 4-1 Path Analyzer System Administration Window**

## Downloading and Installing the Management Console (GUI)

Path Analyzer is accessed via the Management Console, which must first be downloaded and installed on a local machine, following these steps:

- [Uninstalling the Management Console, page 4-3](#)
- [Installing the GUI, page 4-3](#)
- [Starting Path Analyzer, page 4-5](#)

## Uninstalling the Management Console

If you are installing a new version of the Management Console it is advisable to first uninstall your current version. In Windows, this can be done using the Add or Remove Programs utility in the Control Panel. In Linux, you need to manually delete the directory in which the old version resides.

If you are unsure which version you are currently using, open the Management Console and select **Help/About Path Analyzer**. If you are installing a new version, the current version number is shown on the download page (see below).

## Installing the GUI

To install the Path Analyzer GUI:

- Step 1** Select the Microsoft Windows or Linux client on which you want to install the Path Analyzer Management Console, and start your Web browser.

**Step 2** Enter: *http://<IP\_Address>* in the Locator or Address field of your browser, where *<IP\_Address>* is the IP address, or hostname as a URL, of your Path Analyzer Server.

The Path Analyzer System Management Panel, Management Main Menu page is displayed in your Web browser.

**Step 3** Click **Download Management Console** on the Main Menu.

The User Login screen appears.

**Step 4** Log in to authenticate yourself as the system administrator:

- a. In the User Name field, enter the Path Analyzer administrator user name.
- b. In the Password field, enter the Path Analyzer administrator password.




---

**Note** Usernames and passwords are case sensitive.

---

**Step 5** Click **Login**.

The Manage Console Application screen appears.

**Step 6** Follow the numbered instructions on the screen and click on the **Windows** or **Linux** version of the Management Console application. The GuiInstall.exe screen appears.

**Step 7** Click **Save File**.

The file is downloaded to your machine.

**Step 8** Click on the downloaded **GuiInstall.exe** icon.

The Zero-G® InstallAnywhere® wizard begins installation of the Path Analyzer GUI. The wizard instructs you to complete the following steps:

- Introduction
  - Choose Install Folder
  - Choose Shortcut Folder
  - Pre-Installation Summary
  - Installing
  - Install Complete
- 



**Note**

---

Cisco recommends that you use the default settings of the installation wizard when you install the Path Analyzer Management Console. Using the default settings ensures that you can readily identify the location of your program folders and icons after the installation has been completed. However, the wizard also provides optional settings for you to select if you decide not to accept the default settings.

If you decide to cancel the installation at any point, click the **Cancel** button in the Introduction, Choose Install Folder, Choose Shortcut Folder, or Installing Path Analyzer pages of the installation wizard, then click **Quit** in the confirmation box, to stop the installation. If you click **Cancel**, then decide not to stop the installation, click **Resume** to continue the installation.

To revisit a previous page of the installation wizard, click **Previous** at any point during the installation prior to clicking **Install** in the Pre-Installation Summary page. Once you click **Install** in the Pre-Installation Summary page, the installation begins using your previous selections.

---

## Starting Path Analyzer

When the installation completes, the Path Analyzer icons will appear in the locations you selected during the installation process.

To open the Path Analyzer GUI, see the procedure to [Starting Path Analyzer, page 4-10](#).

## Upgrading Path Analyzer Software

If your Path Analyzer GUI is out of date, or a new version is available, you can upgrade the installation with the following procedures:

- [Locating the Installation Files, page 4-5](#)
- [Rebooting the Path Analyzer Server, page 4-6](#)
- [Running the Installation Wizard, page 4-6](#)

## Locating the Installation Files

To locate the installation files:

**Step 1** Select the Microsoft Windows or supported Unix-based Operating System client on which you want to install the Path Analyzer Management Console. Start your Web browser.

**Step 2** Enter: *http://<IP\_Address>* in the Locator or Address field of your browser, where *<IP\_Address>* is the IP address, or hostname as a URL, of your Path Analyzer Server.

The Path Analyzer System Management Panel, Management Main Menu page is displayed in your Web browser.

**Step 3** Click **Update Path Analyzer**.

The User Login screen appears in your Web browser.

**Step 4** Log in to authenticate yourself as the system administrator:

- a. In the User Name field, enter the Path Analyzer administrator user name.
- b. In the Password field, enter the Path Analyzer administrator password.



**Note** Usernames and passwords are case sensitive.

**Step 5** Click **Login**.

The Path Analyzer Server Update screen appears in your Web browser.



**Note** An administrator password is available from your Cisco Technical Support representative.

**Step 6** Click **Browse** to locate the installation file on your computer and click **Update**.

or

Enter the URL of a Web server where the installation file is located and click **Update**.

The message, “Uploading the image please wait,” appears. After the upload is complete, the Path Analyzer Server Upgrade, RD Server Software Upload page appears.

**Step 7** Click **Reboot Page**.

The User Login screen appears to authenticate you as the system administrator before rebooting the Path Analyzer Server.

## Rebooting the Path Analyzer Server

To reboot the Path Analyzer

**Step 1** In the User Login Screen, log in to authenticate yourself as the system administrator:

- a. In the User Name field, enter the Path Analyzer administrator user name.
- b. In the Password field, enter the Path Analyzer administrator password.



**Note** User names and passwords are case sensitive.

- c. Click **Login**.

The Path Analyzer System Reboot Panel, RD Server Reboot Panel appears.

**Step 2** Click **REBOOT Cisco Server**. Because rebooting temporarily interrupts the Path Analyzer Server, you are prompted to confirm your intention to reboot.

**Step 3** Click **Yes**.

The message “Rebooting now” is displayed.

**Step 4** Click **OK**.

The Web browser returns to the Path Analyzer System Management Panel while the Path Analyzer Server is rebooted.

## Running the Installation Wizard

To run the installation wizard:

**Step 1** From the Path Analyzer Management Console:

- a. Click **Start > Administration > System**.  
The Administration module appears.
- b. Select the **Upgrade** tab.
- c. Click **Upgrade** in the Client Upgrade field.

The Path Analyzer Management Console Update, Management Console Application page is displayed in a Web browser.

*or*

- Step 1** Click **Download Management Console** from the Path Analyzer System Management Panel, Management Main Menu page.
- Step 2** Select the desktop environment where you want to install Path Analyzer:
- In the Windows field, click the version link to install the Path Analyzer Management Console in the Microsoft Windows desktop environment.
  - In the Unix field, click the version link to install Path Analyzer in the Unix-based operating environment.
- Step 3** Click **Open** in the File Download dialog box.
- The Path Analyzer Zero-G® InstallAnywhere wizard-based installation for Microsoft Windows and Linux environments is started. Complete the steps provided in the wizard.
- Step 4** Run the installation wizard:
- In Microsoft Windows:**
- a. Click **Open** when you are prompted to Save or Open the file.
  - b. The Path Analyzer installation wizard for Microsoft Windows is started.
- The InstallAnywhere message box appears. As the program extracts the wizard, the message box informs you that InstallAnywhere is preparing to install.
- In a supported Unix-based Operating System:**
- a. Select **Open using an application**.
  - b. Click **Choose**.
  - c. Select a shell, such as `\bin\sh` or `\bin\bash`. At the command prompt, enter:  
`\bin\sh./GuiInstall.bin`
- The Download message appears as the installation wizard is downloaded.
- When the Path Analyzer Introduction page of the installation wizard appears, you can complete the installation.
- Step 5** Complete the wizard.
- For a fast installation, accept the default installation settings by clicking **Next** in each wizard screen.
- Step 6** Click **Done** in the Install Complete wizard page to end the installation.

**Note**

- Cisco recommends that you use the default settings of the installation wizard when you install the Path Analyzer Management Console. Using the default settings ensures that you can readily identify the location of your program folders and icons after the installation has been completed. However, the wizard also provides optional settings for you to select if you decide not to accept the default settings.
- If you decide to cancel the installation at any point, click the **Cancel** button in the Introduction, Choose Install Folder, Choose Shortcut Folder, or Installing Path Analyzer pages of the installation wizard, then click **Quit** in the confirmation box, to stop the installation. If you click **Cancel**, then decide not to stop the installation, click **Resume** to continue the installation.
- To revisit a previous page of the installation wizard, click **Previous** at any point during the installation prior to clicking **Install** in the Pre-Installation Summary page. Once you click **Install** in the Pre-Installation Summary page, the installation begins using your previous selections.

## Review the Introduction Page

To review the introduction page:

- 
- Step 1** Review instructions for using the wizard.
- Step 2** Click **Next**.
- 

## Choose Install Page Folder

To choose the installation folder:

- 
- Step 1** Click **Next** to accept the default setting:
- C:\Program Files\Path Analyzer
- or*
- Step 2** Click **Choose** and select a new folder in which to install Path Analyzer.



**Note** If you select a folder then decide that you would prefer to use the default setting, click **Restore Default Folder**.

---

- Step 3** Click **Next**.
- The Choose Shortcut Folder screen appears.
- 

## Complete the Choose Shortcut Folder Page

To accept the default setting:

- 
- Step 1** Select **In an existing Program Group**.
- Step 2** Ensure that Path Analyzer is selected.

*or*

---

To install the program shortcut in an existing program group other than the default:

- 
- Step 1** Select the program group from the **In an existing Program Group** field.
- Step 2** Select **Cisco > All Programs** after the installation completes, once the Path Analyzer icons appear in the program group you choose.
- 

*or*

To place the Path Analyzer icons in the Start menu:

---

**Step 1** Select **In the Start Menu**.

**Step 2** After the installation completes, the Path Analyzer icons appear in the Start menu.

---

*or*

To place the Path Analyzer icons on the Windows Management Console:

---

**Step 1** Select **On the Desktop**.

**Step 2** After the installation completes, the Path Analyzer icons and uninstall icon are displayed on your Microsoft Windows or Linux environment.

---

*or*

To place the Path Analyzer icons in the Quick Launch bar:

---

**Step 1** Select **In the Quick Launch Bar**.

**Step 2** After the installation completes, the Path Analyzer icons are displayed in the Quick Launch bar of your Windows environment.

---

*or*

To place the Path Analyzer icons in another Windows location:

---

**Step 1** Select **Other**.

**Step 2** Click **Choose**, then select the location for the icons from the Browse for Folder dialog box. After the installation completes, you can start Path Analyzer from the selected location.

---

*or*

To select and not create icons in a prominently displayed location of Windows:

---

**Step 1** Select **Don't create icons**.

**Step 2** Start Path Analyzer from Windows Explorer once the installation is complete:

**Step 3** Open **C:\Program Files\Path Analyzer** to locate the Path Analyzer icons.

**Step 4** Double-click the **Path Analyzer** icon.

**Step 5** Click **Next**.

---

## Complete the Pre-Installation Summary

To complete the pre-installation summary:

- 
- Step 1** Review the information listed on the Pre-Installation Summary page to ensure that your settings are correct.
- Step 2** Click **Previous** to return to a previous page of the wizard and make changes, if necessary.
- or*
- To continue with the installation, click **Install**.
- As the installation continues, the Installing Path Analyzer page appears. The wizard lists files in the order that they are installed. When the installation is complete, the Install Complete page appears.
- Step 3** Click **Done**.
- The installation is complete. The Path Analyzer icons are displayed in the location you selected during the installation process.
- 

## Starting Path Analyzer

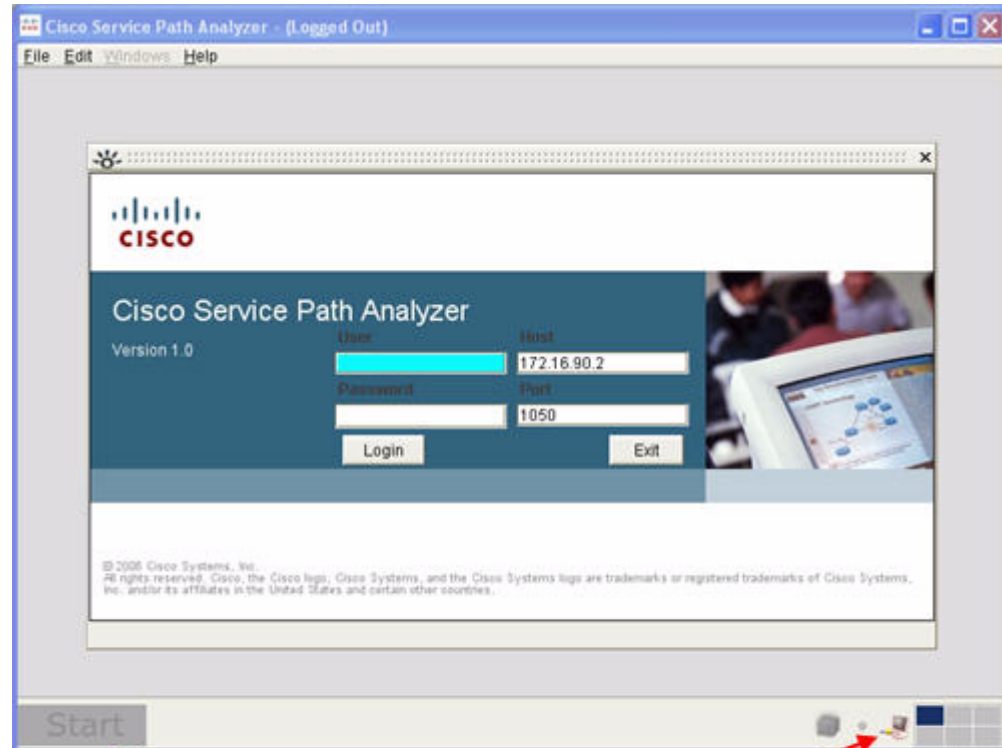
After installing Path Analyzer, verify your connection to the Path Analyzer Server by starting and logging into the Management Console. For detailed information about starting Path Analyzer in the Microsoft Windows or Linux operating environments, see Chapter 1, Getting Started, in the *Cisco Service Path Analyzer User Guide*.

For information about starting and using Management Console modules, see Working in the Management Console in Chapter 1 of the *Cisco Service Path Analyzer User Guide*.

## Verify the Connection

When you start Path Analyzer, the login screen appears, as shown in [Figure 4-2](#). The lower-right corner of the Management Console is displayed with a Disconnected icon, and the Path Analyzer taskbar is unavailable.



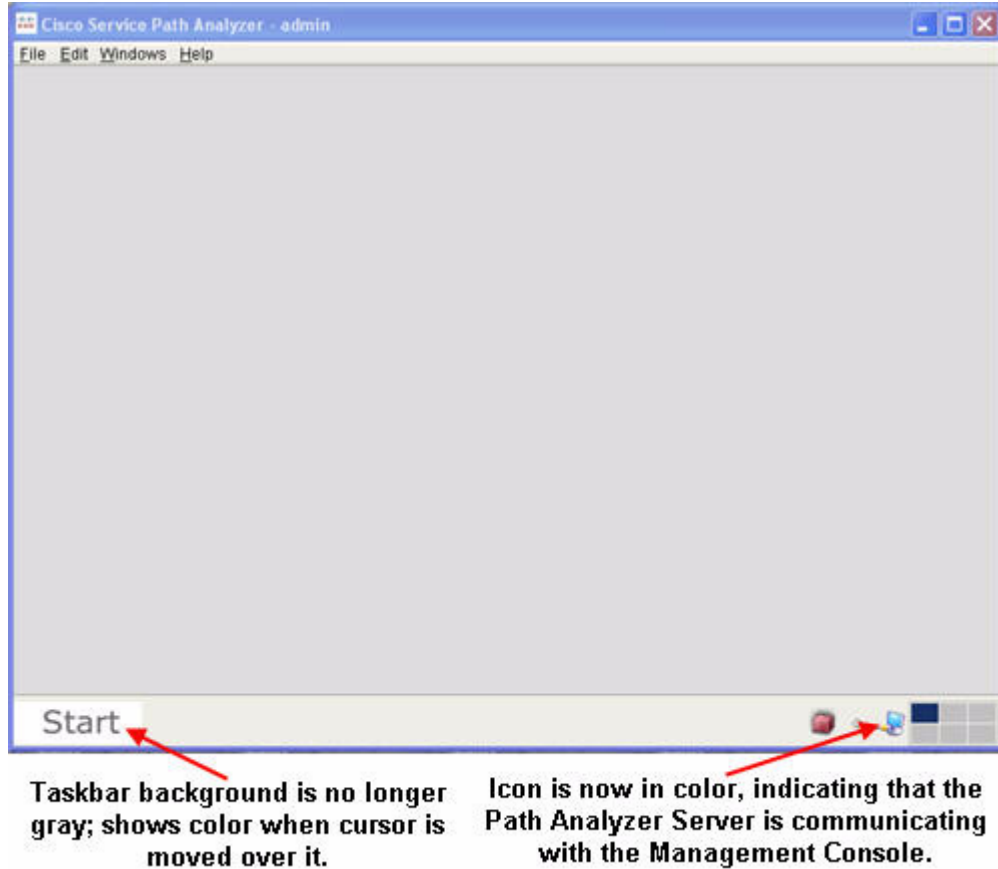
**Figure 4-2 Path Analyzer Management Console Before Login**

**"Grayed-out" taskbar indicates that the user is logged out.**

**"Grayed-out" icon indicates that the Path Analyzer Server is not communicating with the Management Console.**

Once you enter your user name and password, the Path Analyzer Management Console establishes a connection to the Path Analyzer Server.

After login, the lower-right corner of the Management Console is displayed with the **Connected** icon, and the Path Analyzer taskbar is active, as shown in [Figure 4-3](#).

**Figure 4-3** Path Analyzer Management Console after Login

## Upgrading the Listeners

Once you have installed the Management Console, you can upgrade the Listeners on your Path Analyzer System.

To upgrade a listener:

- 
- Step 1** Click **Start > Administration > System**. The System Administration window appears.
  - Step 2** Select the Path Analyzer Server from the configuration tree in the left side of the window.
  - Step 3** Select the **Upgrades** tab [Removing Path Analyzer Components, page 6-49](#) and click the **Upgrade** button under “Listener Upgrade”.

The Listener Upgrade Wizard starts (see [Figure 4-4](#)).

**Figure 4-4** Listener Upgrade Wizard



**Step 4** Click **Next**.

You will see a message, "Upgrading Listeners, please wait." When the process is complete, you will see a message, "Path Analyzer has successfully upgraded all your Listeners."

**Step 5** Click **Finish** to exit the Listener Upgrade Wizard.

See [Configuring a Collector, page 6-25](#) for information about configuring a Collector for each area of your network to be monitored.

---





## CHAPTER 5

# Configuring Domains for Your Enterprise

---

## Setting Up Autonomous Systems and Routing Domains

Your enterprise may consist of many autonomous systems, which are smaller, independent networks operating within your enterprise, which are managed by individual administrators. The routers carrying data to and from these autonomous systems deploy the same interior gateway protocol to direct data toward the destinations. However, each autonomous system may deploy different protocols to exchange data within its network.

The Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) Management Console provides an interface and the capabilities you need to assign names and configure autonomous systems and routing domains within your enterprise.

## Divisions of Autonomous Systems

Autonomous systems that use OSPF as the shared, interior routing protocol are formed of smaller, logical domains called areas. Exterior gateway protocols, (EGPs) such as Border Gateway Protocol, guide the movement of data between domains.

Viewing and managing the contents of your enterprise network in the Path Analyzer Management Console require you configure the following entities:

- Domains contained in the network. See [Assigning Names to Autonomous Systems and Routing Domains, page 5-3](#).
- IP interfaces between the Listeners and the Path Analyzer Server. See [Configuring the Listener Connection to the Path Analyzer Server, page 6-14](#).
- Virtual routers within each Listener that send routing data to the Path Analyzer Server. See [Configuring a Collector, page 6-25](#).



### Note

---

Assign names to autonomous systems and routing domains before configuring connections between Listeners and the Path Analyzer Server and setting up the collectors, virtual routers within each Listener.

---

At a later date, you can reconfigure routing domains on your network and add, change, or remove routing domains.

## Customizing Router and Route Identifiers

Additionally, you can complete the following tasks to change your view of the network elements in the Path Analyzer system:

- Assign unique names to routers to customize how they are displayed in the Path Analyzer Management Console. See [Customizing Router Names, page 5-7](#).
- Enable Path Analyzer to monitor static routes in your network.
- Help Path Analyzer to resolve next-hop IP addresses learned from routing protocols. Path Analyzer needs this information to display paths across your network.

### Router Names

In Path Analyzer, your routers are assigned two separate names:

- A *hostname* derived from Domain Name Service (DNS)—In Path Analyzer, routers keep the identifiers they are generally assigned on your network, including the router ID (an IP address).

**Note**

You can maintain DNS hostname translation conventions for routers in Path Analyzer by importing an `/etc/hosts` or similarly formatted file into the Domain Administration Module.

- A default *router name* is assigned by the Path Analyzer system to every router it discovers, and that name is displayed in the Management Console. This name is separate from and independent of the router's DNS hostname and equates to the router ID or the IP address of each OSPF or BGP router stack configured on a network device. Default router names are used exclusively in the Path Analyzer Management Console and are not visible in your other network management systems (NMS).

**Note**

You can create customized names for routers in the Path Analyzer Management Console by changing each router's name. If you want to display routers in the Topology Viewer, Event Log, and other Path Analyzer modules with their DNS hostname rather than a customized router name or an IP address, you can change the router's name to match its DNS hostname.

See [Customizing Router Names, page 5-7](#) for more information.

### Managing Static Routes and Next-Hop Resolution

The Domain Administration module deploys Path Analyzer to display the static routes that are configured in your network. See [Creating or Editing a Static Route, page 5-12](#).

You can also manage next-hop resolutions from your Path Analyzer system. See [Configuring Next-Hop Resolution for a Static Route, page 5-15](#).

### Managing VRF Tables

Virtual Routing and Forwarding (VRF) is a networking technology that supports multiple instances of a routing table within the same router at the same time. Because these routing tables are independent, the same or overlapping IP addresses can be used without conflicting with each other.

You can use the Domain Administration module to manage VRF tables within the Path Analyzer database. See [Importing VRF Tables Using XML Files, page 5-20](#) for more information.

For instructions on creating VRF XML files, see the *Cisco Service Path Analyzer User Guide*, Chapter 7: MP-BGP Instrumentation.

## Domain Administration Tasks Overview

- [Domain Administration, page 5-3](#)
- [Assigning Names to Autonomous Systems and Routing Domains, page 5-3](#)
- [Customizing Router Names, page 5-7](#)
- [Managing Static Routes and Next-Hop Resolution, page 5-11](#)
- [Managing VRF Tables, page 5-19](#)
- [Removing Autonomous Systems and Routing Domains, page 5-21](#)
- [Removing Routing Domains, page 5-22](#)
- [Removing BGP or OSPF Entities, page 5-22](#)

## Removing Unavailable Entities

The Domain Administration module also allows you to remove all of the routers or entities that have been physically removed from your network from the Path Analyzer Management Console.

## Domain Administration

Tasks you complete in the domain administration module include:

- Assigning names to the autonomous systems and routing domains of your network
- Customizing router names
- Configuring static routes in Path Analyzer
- Resolving next-hop addresses for the Path Analyzer system

## Start the Domain Administration Module

From the Path Analyzer taskbar, click **Start > Administration > Domain**.

The Domain Administration window appears. The left side of the window provides a tree in which you can organize the autonomous systems and routing domains that form your network.

After you assign names for these network components, they are displayed by name in the tree.

## Assigning Names to Autonomous Systems and Routing Domains

Networks, autonomous systems, and domains used in Path Analyzer can be added and named using the following procedures:

- [Customizing the Name of Your Enterprise Network, page 5-4](#)
- [Adding an Autonomous System, page 5-4](#)
- [Changing the Name of an Autonomous System, page 5-5](#)
- [Adding a Routing Domain, page 5-5](#)

## Customizing the Name of Your Enterprise Network

The tree in the left side of the Domain Administration window is assigned the default name “My Enterprise.” You can change this name to one of your choosing.

### Assign or Change the Enterprise Name

To assign the enterprise name, or change it:

- 
- Step 1** Click **Start > Administration > Domain** from the Path Analyzer taskbar.  
The Domain Administration window appears, showing a hierarchical view of your network.
- Step 2** Click the highest level of the network hierarchy. By default, it is labeled “My Enterprise”.  
The Configuration tab (of an Enterprise) appears.
- Step 3** In the Configuration tab, click **Reconfigure**.  
The Enterprise Configuration Wizard appears.
- Step 4** Click **Next**.
- Step 5** Enter a name for your enterprise in the Enterprise Name field. For example, you can enter the name of your corporation or division.
- Step 6** Click **Next**.
- Step 7** Click **Finish**.  
Path Analyzer processes the new enterprise identifier, then provides a message indicating that it was successfully created. The new name replaces the My Enterprise label at the highest level of the network hierarchy.
- 

## Adding an Autonomous System

You can enter an autonomous system of your network into the Path Analyzer Management Console and assign it a name.

You can also change the name of an autonomous system that you previously configured.

To add an autonomous system to your enterprise:

- 
- Step 1** Click **Start > Administration > Domain** from the Path Analyzer taskbar.  
The Domain Administration window appears, showing a hierarchical view of your network.
- Step 2** Click the highest level of the network hierarchy.



By default, this level of the hierarchy is labeled My Enterprise unless you assign or change the Enterprise Name.

#### Assign a New AS Name

**Step 3** Click **Add AS** in the Configuration tab.

The AS Configuration Wizard appears.

**Step 4** Enter a name for the autonomous system in the AS Name field.

**Step 5** Specify the AS Number (ASN).

- Enter the public ASN in the Public AS Number field.  
and, if required:
- Enter the private ASN in the Private AS Number field, if the autonomous system is a private autonomous system.

**Step 6** Leave the rest of the fields on this form with the default settings, unless you are using BGP Summarization, or a VPN.

**Step 7** Click **Next**.

The Committing AS message appears.

**Step 8** Click **Finish**.

Path Analyzer processes the autonomous system parameters, then provides a message indicating that the autonomous system was successfully created. The new name of the autonomous system is displayed in the network hierarchy.

---

## Changing the Name of an Autonomous System

To change the name of an autonomous system:

---

**Step 1** Select an Autonomous System from the Network Hierarchy.

**Step 2** Click **Reconfigure** in the Configuration tab.

The AS Configuration Wizard appears.

**Step 3** Enter a new name in the **AS Name** field.

**Step 4** Click **Next**. The Committing AS message appears.

**Step 5** Click **Finish**.

The new name appears in the network hierarchy.

---

## Adding a Routing Domain

Routing domains from your network can be named and entered into the Path Analyzer Management Console.

**Note**

In the current release of Path Analyzer, an autonomous system displayed in the network hierarchy can contain only one routing domain. If you attempt to add a routing domain to an autonomous system that already contains an OSPF domain, an error message is displayed.

To add a routing domain to Path Analyzer:

- 
- Step 1** Click **Start > Administration > Domain** from the Path Analyzer taskbar.  
The Domain Administration window appears, showing a hierarchical view of your network.
  - Step 2** Click an autonomous system in the network hierarchy.
  - Step 3** Click **Add Domain** in the Configuration tab.  
The Domain Configuration Wizard appears.
  - Step 4** (Optional) De-select the check box **Do not show this screen again** and click **Next**.  
The Domain Parameters screen appears.
  - Step 5** Enter a name for the routing domain in the Domain Name field.
  - Step 6** Click **Next**.
  - Step 7** Click **Finish**.  
Path Analyzer processes the domain name, then provides a message indicating that it was successfully created. The routing domain is displayed with the name in the network hierarchy.
- 

## Changing the Name of a Routing Domain

You can also change the name of a routing domain you previously configured.

To change the name of a routing domain:

- 
- Step 1** Select a routing domain listed under an autonomous system in the network hierarchy.
  - Step 2** Click **Reconfigure** in the Configuration tab.  
The Domain Configuration Wizard appears.
  - Step 3** (Optional) Click the **Do not show this screen again** check box.
  - Step 4** Click **Next**.  
The Domain Parameters screen appears.
  - Step 5** Enter a new name for the routing domain in the Domain Name field.
  - Step 6** Click **Next**.
  - Step 7** Click **Finish**.  
Path Analyzer processes the domain name, then provides a message indicating that it was successfully created. The routing domain is displayed with the new name in the network hierarchy.
-

# Customizing Router Names

From the Domain Administration module, you can:

- Import the DNS hostname translation file for routers on your network. This enables Path Analyzer to maintain the existing IP-address-to-hostname correlation.
- Change the default names of routers displayed in your Path Analyzer system.

When a Path Analyzer Listener discovers a router, it assigns a default router name that correlates with the IP address of each OSPF or BGP router stack installed on the network device.

These default router names are not displayed in modules of the Management Console unless you perform the following steps:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Navigate to <b>Start&gt; Preferences</b> .   |
| <b>Step 2</b> | Select <b>Router Name Format</b> under “Formats” in the left pane.                   |
| <b>Step 3</b> | Select <b>Append Generic Name</b> under “Select Format Modifiers” in the right pane. |
- 

However, you can manually change the default router name to an IP address, the Domain Name Service (DNS) name, or character string of your choice and set preferences for viewing the router name in the modules of the Path Analyzer Management Console.

For information about changing a router’s name, see [Changing Router Names, page 5-9](#).

For information about setting preferences for viewing router names in the Path Analyzer Management Console, see Set User Preferences on page 1-20 of the *Cisco ServicePath Analyzer User Guide*.

## Options for Changing Router Names

From the Path Analyzer Domain Administration module, you can customize router names in the following ways:

- Import an `/etc/hosts` file or other similarly formatted file that describes the Domain Name Service (DNS) correlation between the router ID and the host name of each router in your network.
- Select and change the router name of a particular router using the Router Configuration Wizard. You can set a new router name or replace the default router name with the router’s DNS host name.

Changes to router names are committed and persisted in the Path Analyzer Server’s database. After changing the name of a router, you can view the change in Path Analyzer modules, including router assignments in the Topology Viewer and Browser and event descriptions in the Event Log.

## Importing DNS Names and Applying them to Routers

To apply DNS names to routers:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Click <b>Start &gt; Administration &gt; Domain</b> from the Path Analyzer taskbar.<br><br>The Domain Administration window appears, showing a hierarchical view of your network. |
| <b>Step 2</b> | Expand the autonomous system that contains the routing domain you want to apply DNS names to in the network hierarchy.   |

- Step 3** Select the autonomous system or domain.
- Step 4** Click the **Router Names** tab. If an `/etc/hosts` file or other DNS hostname translation file was uploaded previously, its entries are displayed.
- Step 5** Start the Wizard:
- Click **Upload Wizard**.  
The Host File Upload Wizard appears.
  - (Optional) De-select the check box **Do not show this screen again** and click **Next**.  
The Select a File for Upload wizard page appears. It is similar to the Choose File or Choose dialog box of your operating system.
- Step 6** Locate the DNS Hostname Translation file:
- In the File Name field, enter the name of your `/etc/hosts` or other DNS host name translation file.  
*or*
  - Select a drive letter from the Look In field and browse for the host name translation file in the list of folders.
- Step 7** Click **Next**.  
The Review Entries wizard page appears.
- Step 8** Review the entries.
- If you are dissatisfied with the entries displayed:
    - Click **Back**.  
The Select a File for Upload wizard page is redisplayed.
    - From the list of folders, select another host name translation file.
    - Click **Next**.  
The Review Entries wizard page appears.
    - Click **Next** to approve the entries.
  - If you are satisfied with the entries displayed in the Review Entries wizard page, click **Next**.
- Step 9** Click **Finish** to complete the wizard.  
Router names from your host name translation file are accepted and displayed in the Router Names tab.
- 

## Viewing Hostname Changes

To view hostname changes in the Management Console after changing the host name translation file, open the Domain Administration module, select the domain in which changes occurred, and upload the file to the Path Analyzer Server.



### Note

- Router names are changed within Path Analyzer and are not propagated to your network management system (NMS).
- Default router names, assigned by Path Analyzer, are not displayed unless you select:  
**Append Cisco > Preferences**

**Router Name Format** (under “Formats” in the left-hand pane)

**Append Generic Name** (under “Select Format Modifiers” in the right-hand pane)

- The Path Analyzer Server does not retain a pointer to the `/etc/hosts` or similar hostname translation file.

## Removing DNS Names

To Remove DNS names:

- 
- Step 1** Click **Start > Administration > Domain** from the Path Analyzer taskbar.
- The Domain Administration window appears, showing a hierarchical view of your network.
- Step 2** Select the autonomous system or routing domain containing the router you want to remove the DNS name of from the network hierarchy.
- Step 3** Click the **Router Names** tab.
- Step 4** Click **Removal Wizard**.
- The Remove Entries Wizard page appears.
- Step 5** (Optional) De-select the check box **Do not show this screen again** and click **Next**.
- The Router Name Removal Wizard appears, showing a table of correlated IP address and router names.
- Step 6** Click the **check box next to the entry(s) you wish to remove** in the Select `/etc/host` mappings to remove table. A check mark is displayed in the check box of each selected entry.
- Step 7** Click **Next**.
- A message appears to inform you that the changes are committed to the Path Analyzer Server.
- Step 8** Click **Finish** to complete the wizard.
- Router names from your hostname translation file are accepted and displayed in the Router Names tab.
- 

## Changing Router Names

To change a router's name:

- 
- Step 1** Click **Start > Administration > Domain** from the Path Analyzer taskbar.
- The Domain Administration window appears, showing a hierarchical view of your network in the left side of the window.
- Step 2** Click the highest level of the network hierarchy.
- By default, this level of the hierarchy is labeled “My Enterprise” unless you [Assign or Change the Enterprise Name, page 5-4](#).
- Step 3** Click the **Routers** tab to display the tab's contents.
- Step 4** Select a router entry from the list.
- Step 5** Click **Edit**.

The Route Configuration Wizard appears.

**Step 6** (Optional) De-select the check box **Do not show this screen again** and click **Next**.

The Search for a Router wizard page appears.

**Step 7** Search for a Router:

**To view a list of all routers:**

- a. Without removing the wildcard asterisk (\*) displayed in the Router Name, DNS Name, and Router ID field, click **Next**.

*or*

**To search for a specific router:**

- a. Replace the wildcard asterisk (\*) with any of the following parameters:
  - In the Router Name field, enter the router name assigned by Path Analyzer, or enter the router ID.
  - In the DNS Name field, enter the DNS host name of the router, or enter the router ID.
  - In the Router ID field, enter the Router ID of the router in the form of an IP address.

**Step 8** Click **Next**.

The Select a Router to Edit wizard page appears.

**To view specific values in order to fill in the fields of the Search for a Router wizard page:**

- a. Move the Router Configuration Wizard window aside to view the Domain Administration module.
- b. Select the **Routers** tab.
- c. Select an entry from the list of routers, then click **View Details**.  
The Router Properties dialog box appears, showing the router name, DNS name, and Router ID in the uppermost section of the dialog box.
- d. Locate the information you need to complete the Search for a Router wizard page.
- e. Move the Router Configuration Wizard to the forefront to complete the fields.

**Step 9** Select the router you want to change from the list of routers.

**Step 10** Click **Next**.

The Select a Name for the Router wizard page appears.

**Step 11** Enter a new name for the router in the Select a name for this router field. Possible router names include:

- DNS host name of the router.
- Name that identifies the location of the router in the data center or lab, such as Router3Rack10Rm218.
- Name of the department or division to which the router belongs.
- Any unique name you want to assign the router within your Path Analyzer system.

**Step 12** Click **Next**.

**Step 13** Click **Finish** to complete the wizard.

The new router name is accepted.

---

# Managing Static Routes and Next-Hop Resolution

Routing protocols enable routers to dynamically learn how to reach destinations within the same network or external networks. As routes change, the router learns and adjusts in real-time.

However, depending on network conditions between the route's source and destination, it may be more efficient to manually configure a static, unchanging route than to allow the router to dynamically learn the route using its routing protocol.

Similar to an express train that bypasses stops and brings passengers directly to a destination, the static route passes packets to a interface on a router one hop from the destination, bypassing high-cost, or unroutable intervening hops.

You can configure static routes when you want to force data to take a known, lower-cost path to a destination, or when a router:

- Cannot dynamically learn a lower-cost or better route to a destination. This situation occurs when a router cannot learn about routes received on an interface configured with a different protocol.
- Cannot determine the route to a destination due to an intervening firewall or Network Address Translation (NAT) appliance.
- Forwards unroutable packets.

For example, router 192.168.2.10 dynamically learns the route 192.168.11.0/24 from its routing protocol. This prefix is recorded in the routing table of 192.168.2.10.

When 192.168.2.10 receives packets destined for a host in the 192.168.11.0/24 network, it passes packets over the learned route, shown in [Figure 5-1](#).

The four long arrows represent the four hops that the packets traverse from router 192.168.2.10 to 192.168.0.5, which forwards data to the destination host. If each hop has a value of 4, the cost value to reach the destination will equal 16.

**Figure 5-1** Path of Learned Route

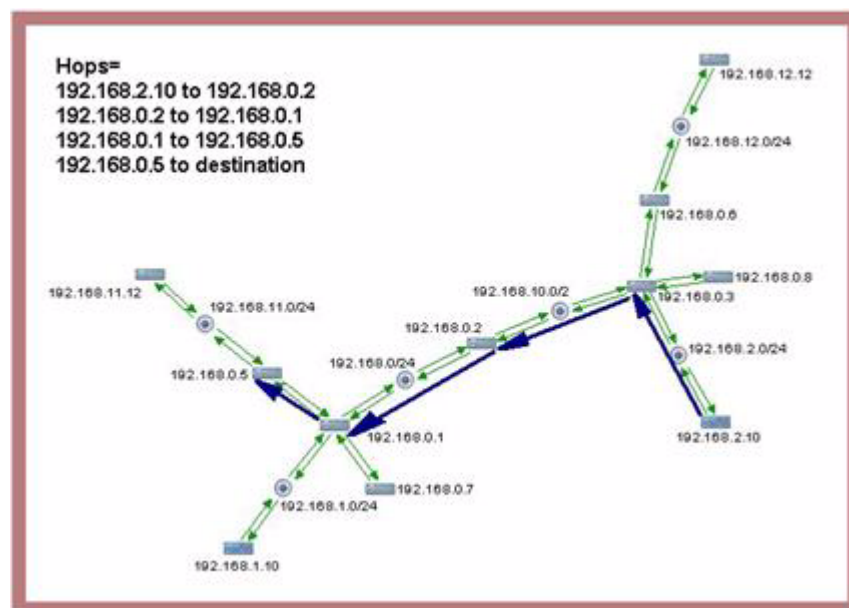
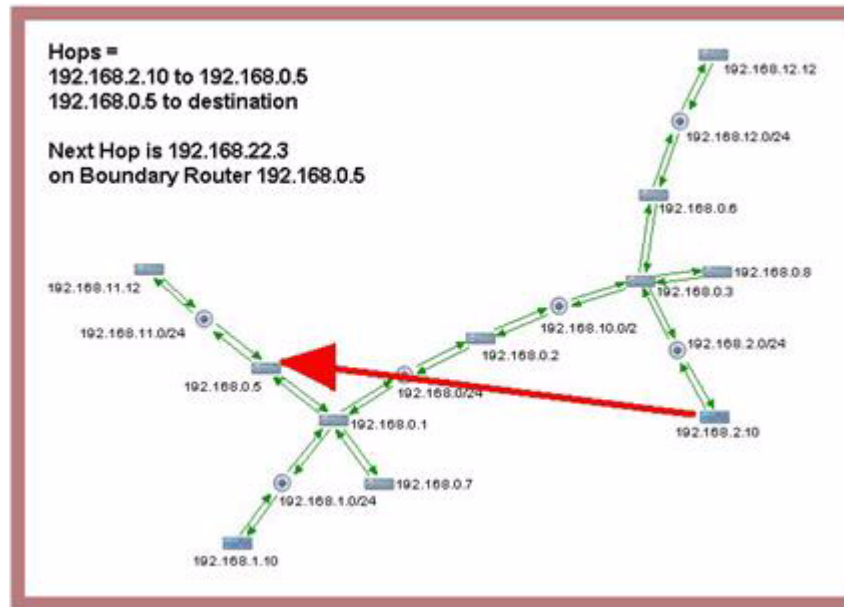


Figure 5-2 shows the path between router 192.168.2.10 and router 192.168.0.5 after configuring a static route.

**Figure 5-2 Path of Static Route**



Packets are expressly forwarded from 192.168.2.10 to an interface, 192.168.22.3, on 192.168.0.5, and bypass intermediate routes. The interface, 192.168.22.3, is referred to as the *next hop*. Router 192.168.0.5 is referred to as the *bound router*, which is the physical router configured with the logical next hop on the static route.

In addition to reducing the number of hops traversed, the static route lowers the cost of reaching the destination by half, to 8.

## Static Routes and Next-Hop Resolution in Path Analyzer

If routers in your network are configured with static routes, Path Analyzer requires the following information:

- Router on which the static route is configured.
- Static route, such as 10.10.0.0/16.
- Next hop of the static route.

## Creating or Editing a Static Route

To create or edit a static route:

- 
- Step 1** Determine the static route you want to create in Path Analyzer:
- Start the Topology Viewer.
  - Identify the router to which you will add the static route.



- c. Locate the network in which the destination host resides.
- d. Right-click the router located one hop before the destination network. This router is the bound router for the static route.
- e. Click **Show Attributes** if the router has only one designated interface and note the IP address of the interface you will assign to be the next hop for the static route.

or

- Start the Static Routes Wizard to locate and edit an existing static route.

**Step 2** Start the Static Routes Wizard:

- a. Click **Start > Administration > Domain**. The Domain Administration window appears, showing a hierarchical view of your network.
- b. Click the highest level of the network hierarchy.
- c. By default, this level of the hierarchy is labeled “My Enterprise” unless you [Assign or Change the Enterprise Name, page 5-4](#).
- d. Click the **Static Routes** tab. The content of the Static Routes tab appears.
- e. Click **Edit**.

The Static Route Configuration Wizard starts, showing the Search for a Router wizard page (see [Figure 5-3](#)).

**Figure 5-3 Search for a Router Screen in Static Route Configuration Wizard**



**Step 3** Search for a Router

**To view a list of all routers:**

- a. Click **Next** without removing the wildcard asterisks (\*) displayed in the Router Name, DNS Name, and Router Id field. The Select a Router to Edit wizard page appears.

or

**To search for a specific router:**

- a. Replace the wildcard asterisk (\*) with any of the following parameters:
  - In the Router Name field, enter the router name assigned by Path Analyzer, or enter the router ID.
  - In the DNS Name field, enter the DNS host name of the router, or enter the router ID.

In the Router ID field, enter the Router ID of the router in the format of an IP address. The Select a Router to Edit wizard page appears (see [Figure 5-4](#)).

**Static Route Configuration Wizard**

Select a router to edit...

OSPF Do...	OSPF Rout...	AS	BGP Router	Name
...	...	AS100	172.31.15.1	172.31.15.1
33464-Area0	169.185.96.61	...	...	169.185.96.61
33464-Area0	169.185.96.62	...	...	169.185.96.62
33464-Area0	169.185.96.63	...	...	169.185.96.63
33464-Area0	169.185.96.64	...	...	169.185.96.64
2911-Area0	192.193.250.201	AS2911	192.193.250.201	192.193.250.201
2911-Area0	192.193.250.200	AS2911	192.193.250.200	192.193.250.200
2911-Area0	192.193.252.244	AS2911	192.193.252.244	192.193.252.244
2911-Area0	192.193.252.243	...	...	192.193.252.243
2911-Area0	192.193.252.242	...	...	192.193.252.242
2911-Area0	192.193.252.241	...	...	192.193.252.241
2911-Area0	192.193.252.54	...	...	192.193.252.54
2911-Area0	192.193.252.53	...	...	192.193.252.53
2911-Area0	192.193.252.52	...	...	192.193.252.52
2911-Area0	192.193.252.43	...	...	192.193.252.43
2911-Area0	192.193.252.40	...	...	192.193.252.40
2911-Area0	192.193.252.39	...	...	192.193.252.39
2911-Area0	192.193.252.38	...	...	192.193.252.38
2911-Area0	192.193.252.11	...	...	192.193.252.11
2911-Area0	192.193.252.9	...	...	192.193.252.9
2911-Area0	192.193.252.2	...	...	192.193.252.2
2911-Area0	192.193.252.1	...	...	192.193.252.1
2911-Area0	192.193.251.252	...	...	192.193.251.252
2911-Area0	192.193.251.251	...	...	192.193.251.251
2911-Area0	192.193.251.246	...	...	192.193.251.246
2911-Area0	192.193.251.245	...	...	192.193.251.245

< Back      Next >      Cancel

**Step 5** Click **Next**.

**Figure 5-5** *Edit This Router's Static Routes Screen in Static Route Configuration Wizard*



- Enter the prefix of the static route in the Route field, in the format of an IP address and subnet mask prefix. Example: 10.10.1.0/24
- Enter the IP address of the interface configured to be the next hop from the router that originates the static route in the Next Hop field.
- Click **Add**.

If you configure a duplicate static route, an error message appears.

If you configure multiple static routes and decide not to commit one, or mistype the route, select the route from the list and click **Remove**.

**Step 7** Click **Next**.

**Step 8** Click **Finish** to complete the wizard.

---

## Configuring Next-Hop Resolution for a Static Route

After adding a static route to Path Analyzer or editing an existing static route, set the bound router ID and indicate the state of the static route.

To configure a next-hop resolution for a static route:

---

**Step 1** Select Resolution Settings of the Static Route:

- a. Click **Start > Administration > Domain**. The Domain Administration window appears, showing a hierarchical view of your network.
- b. Click the highest level of the network hierarchy. By default, this level of the hierarchy is labeled My Enterprise unless you [Assign or Change the Enterprise Name, page 5-4](#).
- c. Click the **Next Hop Resolutions** tab.

The Next-Hop Resolutions tab appears, showing the following information:

- Router—IP address or host name of the router configured with the static route.
  - Next Hop—IP address of the next hop, the interface on the bound router that directly receives forwarded data from the originating router over the static route.
  - Bound Router—Router ID of the physical router configured with the next hop.
  - Confirmed—Indicates whether a static route is configured for the router.
  - Description—Provides a description of the static route, if one was provided when the static route was created.
  - Routable—Indicates whether the path to the next hop is available, enabling data to be forwarded to the next hop.
- d. Select an entry from the list to change its next-hop resolution settings.
  - e. Click **Edit**. The Next-Hop Resolutions Configuration Wizard appears.
  - f. (Optional) De-select the check box **Do not show this screen again** and click **Next**. The Search for a Router wizard page appears.

**Step 2** Find one or more routers by router name to change next hop resolution settings.

**To view a list of all routers:**

- Click **Next** without removing the wildcard asterisks (\*) displayed in the Router Name, DNS Name, and Router Id field. The Select a Router to Edit wizard page appears.

*or*

**To search for a specific router:**

- Replace the wildcard asterisk (\*) with any of the following parameters:
  - In the Router Name field, enter the router name assigned by Path Analyzer, or the router ID.

- In the DNS Name field, enter the DNS host name of the router, or enter the router ID.
- In the Router Id field, enter the Router ID of the router, in the format of an IP address. The Select a Router to Edit wizard page appears.

**Step 3** Click **Next**.

**Step 4** Select the router entry you want to change from the list of routers.

**Step 5** Click **Next**.

**Step 6** Select an entry to edit From the list of next-hop resolution entries.

**Step 7** Click **Next**.

The Select the Bound Router wizard page appears.

**Step 8** Select one of the following options for the bound router:

- **Keep the existing router**—Keeps the current bound router as the next hop from the originating router.
- **Undefined**—Indicates that the bound router for the next hop is undefined.
- **One of the following candidates**—Provides a list of potential bound routers. Select one of the listed routers.
- **None of the above**—Provides options for selecting a specific router.

**Step 9** Click **Next**.

If you select any of the following settings, the Enter Additional Properties for the Next-Hop Resolution wizard page appears:

- Keep the existing router
- Undefined
- One of the following candidates

**Step 10** Continue the wizard to [Set Additional Properties: on page 5-17](#).

If you select None of the above, the Search for a Router to Bind To wizard page appears. [Search for a Router: on page 5-16](#) to bind to, select the router, then continue the wizard to [Set Additional Properties: on page 5-17](#).

**Step 11** Search for a Router:

**To view a list of all routers:**

- Click **Next** without removing the wildcard asterisks (\*) displayed in the Router Name, DNS Name, and Router Id field. The Select a Router to Edit wizard page appears.

*or*

**To search for a specific router:**

- Replace the wildcard asterisk (\*) with any of the following parameters:
  - In the Router Name field, enter the router name assigned by Path Analyzer, or the router ID.
  - In the DNS Name field, enter the DNS host name of the router, or enter the router ID.
  - In the Router Id field, enter the Router ID of the router, in the format of an IP address. The Select a Router to Edit wizard page appears.

**Step 12** Click **Next**. The Enter Additional Properties for the Next-Hop Resolution wizard page appears.

**Step 13** Select an entry to edit from the list of Next Hop Resolution Entries.

**Step 14** Click **Next**.

The Enter Additional Properties for the Next-Hop Resolution wizard page appears.

**Step 15** Set Additional Properties:

- a. Select **Yes** or **No** in either of the following fields:
  - **Routable**—Indicates to Path Analyzer how the selected router forwards packets to the next hop on the bound router. The default setting is **Yes**.
    - **Yes**—Prompts Path Analyzer to forward packets to the next hop directly, without forwarding to any intervening OSPF routers.
    - **No**—Prompts Path Analyzer to forward packets to OSPF routers between the originating router and the bound router via a dynamic or static route.
  - **Confirmed**—Indicates whether the bound router for the static route has been identified within Path Analyzer. The default setting is **No**.
    - **Yes**—Indicates that you have approved the bound router.
    - **No**—Indicates that you have to select a router to bind to the next hop.
- b. Enter a description of the forwarding resolution settings in the Description field.

**Step 16** Click **Next**.

**Step 17** Click **Finish** to complete the wizard.

---

## Removing a Static Route

To remove a static route:

**Step 1** Click **Start > Administration > Domain**.

**Step 2** Select the **Static Routes** tab.

**Step 3** Click **Edit**.

The Static Route Configuration Wizard starts, showing the Search for a Router Wizard page (see [Figure 5-6](#)).

**Figure 5-6** Search for a Router Screen in Static Route Configuration Wizard

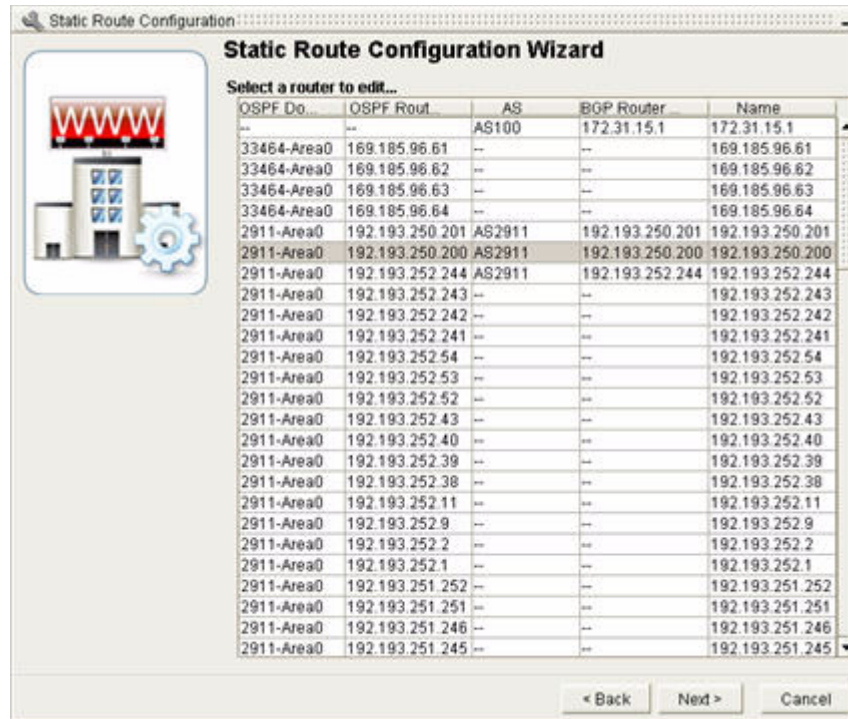


**Step 4** Search for a Router

To view a list of all routers:

- a. Click **Next** without removing the wildcard asterisks (\*) displayed in the Router Name, DNS Name, and Router Id field. The Select a Router to Edit wizard page appears (see [Figure 5-7](#)).

**Figure 5-7** Select a Router to Edit Screen in Static Route Configuration Wizard



or

To search for a specific router:

- Replace the wildcard asterisk (\*) with any of the following parameters:
  - In the Router Name field, enter the router name assigned by Path Analyzer, or the router ID.
  - In the DNS Name field, enter the DNS host name of the router, or enter the router ID.
  - In the Router Id field, enter the Router ID of the router, in the format of an IP address. The Select a Router to Edit wizard page appears.

**Step 5** Select the router entry you want to edit from the list of routers.

**Step 6** Click **Next**.

The Edit This Router's Static Routes wizard page appears (see [Figure 5-8](#)).

**Figure 5-8** *Edit This Router's Static Routes Screen in Static Route Configuration Wizard*



- Step 7** Enter Definitions of the Static Route
- Enter the prefix of the static route in the Route field, in the format of an IP address and subnet mask prefix. Example: 10.10.1.0/24
  - Enter the IP address of the interface configured to be the next hop from the router that originates the static route in the Next Hop field.
- Step 8** Click **Remove**. A message appears to indicate that your changes are saved successfully.
- Step 9** Click **Finish**.  
The static route is removed from your Path Analyzer system.

## Viewing Properties of a Router

To find out information about a router's configuration:

- Step 1** Click **Start > Administration > Domain**.
- Step 2** Select the **Routers** tab.
- Step 3** Select a router entry from the list in the Routers tab.
- Step 4** Click **View Details**.  
The Router Properties dialog box appears, showing the Router ID, DNS name, or user-defined name in the uppermost section of the dialog box.

## Managing VRF Tables

To manage VRF tables, you must first import them into Path Analyzer as XML.



## Importing VRF Tables Using XML Files

The VRF Configuration Wizard lets you add, remove, and change VRF definitions within the Path Analyzer database. VRF tables are imported using XML files. See *Creating VRF XML files* in Chapter 7, *MP-BGP Instrumentation*, in the *Cisco Service Path Analyzer User Guide*.

To import VRF tables:

- 
- Step 1** Click **Start > Administration > Domain**.
- The Domain Administration window appears, showing a hierarchical view of your network.
- Step 2** Select the autonomous system for which you want to manage VRFs.
- The Configuration tab should be open on the right side of the screen.
- Step 3** Click **Manage VRFs** at the bottom of the Configuration tab.
- The VRF Configuration Wizard displays.
- Step 4** (Optional) De-select the check box **Do not show this screen again** and click **Next**.
- The Please Select the XML File wizard page appears (see [Figure 5-9](#)).

**Figure 5-9** Select XML File Screen in VRF Configuration Wizard



- Step 5** Navigate to the network location where you have stored your VRF XML files and click on the name of the XML file you wish to import.
- Step 6** Click **Next**.
- The Select Type of Import screen appears (see [Figure 5-10](#)).



**Figure 5-10** Select Type of Import Screen in VRF Configuration Wizard

- Step 7** Select one of the following radio buttons and click **Next**.
- **Add to Existing Configuration**—The VRFs in your XML file will be added to those already in the database.
  - **Update the Existing Configuration**—The VRFs in your XML file will update existing VRFs that have the same IDs.
  - **Remove the Existing Configuration**—Your XML file will remove specific VRFs, identified by ID).
  - **Import Configuration from Scratch**—The VRFs in your XML file will replace all those currently in the database.

You will receive a notification that the update is in process.

- Step 8** When the update is complete, click **Next**.

- Step 9** Click **Finish** to complete the wizard.

## Removing Autonomous Systems and Routing Domains

As part of effective data management, you can remove selected autonomous systems or routing domains and purge the Path Analyzer database of related data.

### Removing Autonomous Systems

To remove an Autonomous System:

- Step 1** Click **Start > Administration > Domain**.  
The Domain Administration window appears.
- Step 2** Select the autonomous system you want to remove from the network hierarchy.  
The Configuration tab (of an Autonomous System) appears.
- Step 3** Click **Remove** in the Configuration tab.

A message appears to inform you that removing the selected autonomous system also removes all Collectors, OSPF domains, and alarms associated with the selected autonomous system.

**Step 4** Click **Yes** to confirm that you want to remove the autonomous system and purge related data.

**Step 5** Click **Finish** to complete the purge.

The autonomous system is removed from the network hierarchy in the Domain Administration window. All data related to the autonomous system is purged from the Path Analyzer database.

---

## Removing Routing Domains

To remove a Routing Domain:

---

**Step 1** Click **Start > Administration > Domain**.

The Domain Administration window appears.

**Step 2** Select the domain you want to remove from the network hierarchy.

The Configuration tab (of a Domain) appears.

**Step 3** Click **Remove** in the Configuration tab.

A message appears to inform you that removing the selected domain also removes all Collectors, alarms, and services associated with the selected domain.

**Step 4** Click **Yes** to confirm that you want to remove the domain and purge related data.

**Step 5** Click **Finish** to complete the purge.

The domain is removed from the network hierarchy in the Domain Administration window. All data related to the domain is purged from the Path Analyzer database.

---

## Removing BGP or OSPF Entities

Removing a router or subnet from your enterprise network causes its icons and other related data to be displayed as unavailable in the Topology Viewer and other Path Analyzer modules. The Domain Administration module provides the Entity Removal Wizards, which allow you to remove views of unavailable BGP or OSPF entities per selected autonomous system or routing domain.

### Remove BGP Entities

To remove BGP entities:

---

**Step 1** Click **Start > Administration > Domain**.

The Domain Administration window appears.

**Step 2** Select the autonomous system you want to remove an entity from in the network hierarchy.

The Configuration tab (of an Autonomous System) appears.

**Step 3** Click **Remove Entities** in the Configuration tab.

The BGP Entity Removal Wizard appears.

- Step 4** The initial wizard page explains that the wizard will guide you through the batch removal of selected entities. Click **Next**.
- To prevent this page from displaying every time you start the wizard, select: **Do not show this screen again**.
- The Select Entities to Remove wizard page appears.
- Step 5** Select the entity or entities you want to remove in the Entity table. A check mark is displayed in the check box of each selected entity.
- Step 6** Click **Next**.
- Step 7** Click **Finish** to complete the removal of selected entities.
- The selected entities are removed from modules of the Path Analyzer Management Console. All data related to each entity is purged from the Path Analyzer database.
- 

## Remove OSPF Entities

To remove OSPF entities:

- 
- Step 1** Click **Start > Administration > Domain**.
- The Domain Administration window appears.
- Step 2** Select the domain you want to remove an entity from in the network hierarchy.
- The Configuration tab (of a Domain) appears.
- Step 3** Click **Remove Entities** in the Configuration tab.
- The OSPF Entity Removal Wizard appears.
- Step 4** The initial wizard page explains that the wizard will guide you through the batch removal of selected entities. Click **Next**.
- To prevent this page from displaying every time you start the wizard, select: **Do not show this screen again**.
- The Select Entities to Remove wizard page appears.
- Step 5** Select the entity or entities you want to remove in the Entity table. A check mark is displayed in the check box of each selected entity.
- Step 6** Click **Next**.
- Step 7** Click **Finish** to complete the removal of selected entities.
- The selected entities are removed from modules of the Path Analyzer Management Console. All data related to each entity is purged from the Path Analyzer database.
-





## CHAPTER 6

# Configuring Listeners and Collectors

---

## Enabling your Listeners to Collect Routing Data

After configuring the IP interface of your Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) Server and installing the Path Analyzer Management Console, you are ready to preconfigure connections between the Listener and the Path Analyzer Server and configure the Collectors internal to the Listener.

Before describing the administration procedures involved in connecting Listeners and Servers, it is useful to understand the components that comprise a Path Analyzer system, how these components work together, the different configurations that are possible, and the reasons for using each configuration.

## Path Analyzer Components and Configurations

- [Path Analyzer Components, page 6-1](#)
- [Path Analyzer System Configurations, page 6-3](#)
  - [Single Autonomous System, page 6-4](#)
  - [Multiple Autonomous Systems, page 6-5](#)
- [Fault-Tolerant Configurations, page 6-10](#)

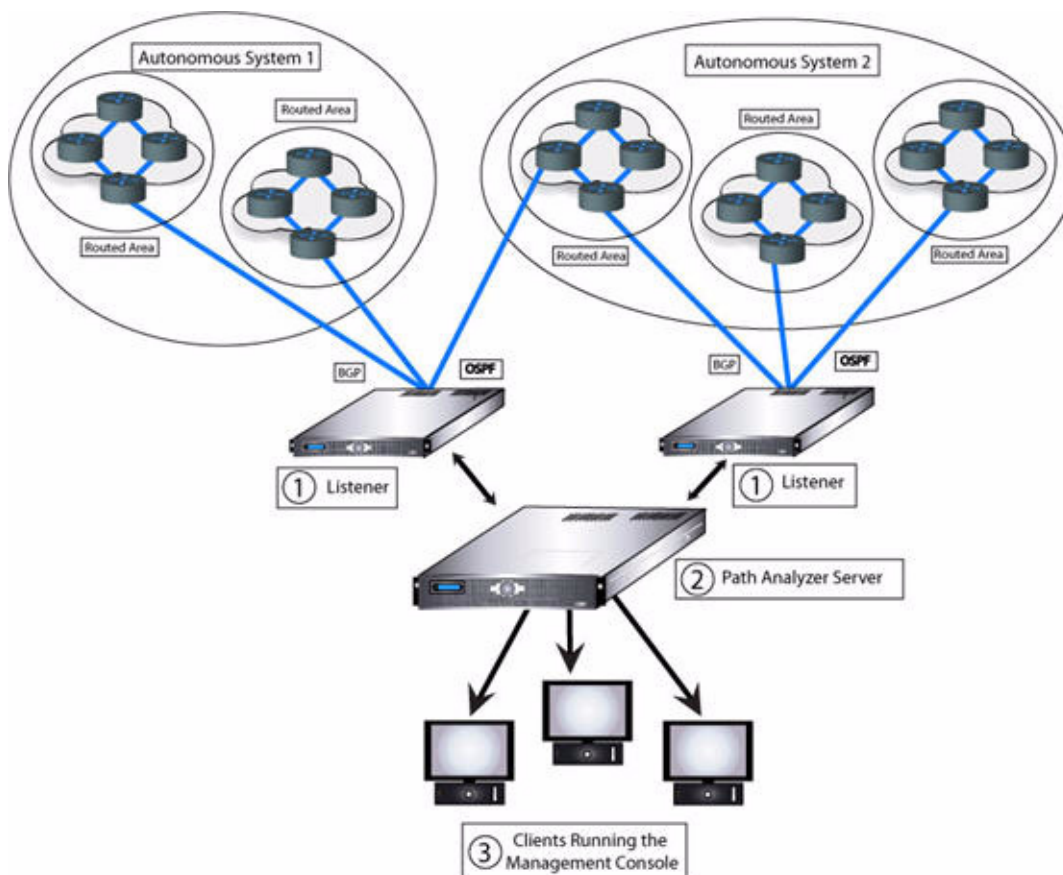
## Path Analyzer Initial Configuration and Maintenance Tasks

- [Configuring Path Analyzer Appliances, page 6-13](#)

## Path Analyzer Components

Your Path Analyzer system consists of the following components, as illustrated in [Figure 6-1](#):

- [Listener, page 6-2](#) (1)
- [Path Analyzer Server, page 6-3](#) (2)
- [Clients Running the Management Console, page 6-3](#) (3)

**Figure 6-1** Components of the Path Analyzer System

## Listener

The Listener appliance has the following functions:

- Captures routing updates from your network by forming an adjacency with a router in one or more Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) routing domains.
- Forwards routing data to the Path Analyzer Server.

For Listener hardware specifications and additional information, see:

- *Cisco Application Deployment Engine 1010 and 2120 Appliance Hardware Installation Guide*, or
- *Cisco Application Deployment Engine 2130 and 2140 Appliance Hardware Installation Guide*

## Listener Port Configurations

Your Path Analyzer system contains a 4-port Listener. The Path Analyzer Listener provides two direct 10/100/1000 Base-T connections, plus two additional 10/100/1000 connections through the PCI interface. A Listener can monitor routing in up to four autonomous systems or OSPF areas.

## Collectors

Collectors are the virtual routers that run inside each Listener. They form an 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.

## Path Analyzer Server

The Path Analyzer Server has the following functions:

- Creates a composite, real-time view of the network, which can be viewed via the Path Analyzer Management Console.
- Stores and makes available current and historical data about alarms, events, network topology, and paths, which can be viewed via the Path Analyzer Management Console
- Provides applications that enable the configuration and management of Listeners and Collectors.
- Provides a Web-based interface in which you can upgrade your Path Analyzer appliances and Management Console.

For Path Analyzer Server hardware specifications and additional information, see:

- *Cisco Application Deployment Engine 1010 and 2120 Appliance Hardware Installation Guide*, or
- *Cisco Application Deployment Engine 2130 and 2140 Appliance Hardware Installation Guide*

## Clients Running the Management Console

Path Analyzer clients provide:

- A visual display of routing and service data across multiple autonomous systems and OSPF areas.
- A view of your network's topology, displayed as a hierarchy of autonomous systems comprised of logical routing domains and elements including routers, subnets, interfaces, and routes.
- A view of your network's services; the flow of business-critical data to your applications and end users.
- A view of your network's changes, called events, that occur on your network, and the root causes of these events.
- The ability to set customized alarms on sequences of events.
- The ability to develop customized charts and reports that can be used to detect routing trends.

## Path Analyzer System Configurations

Your Path Analyzer system configuration is determined by your team and your Cisco Customer Support Representative. Configurations are customized for your organization and network, based on the following requirements:

- Complexity of your network
- Geographical distribution of your network components
- System redundancy and failover requirements

- Protocols running within and between autonomous systems

The following sections describe supported configurations.

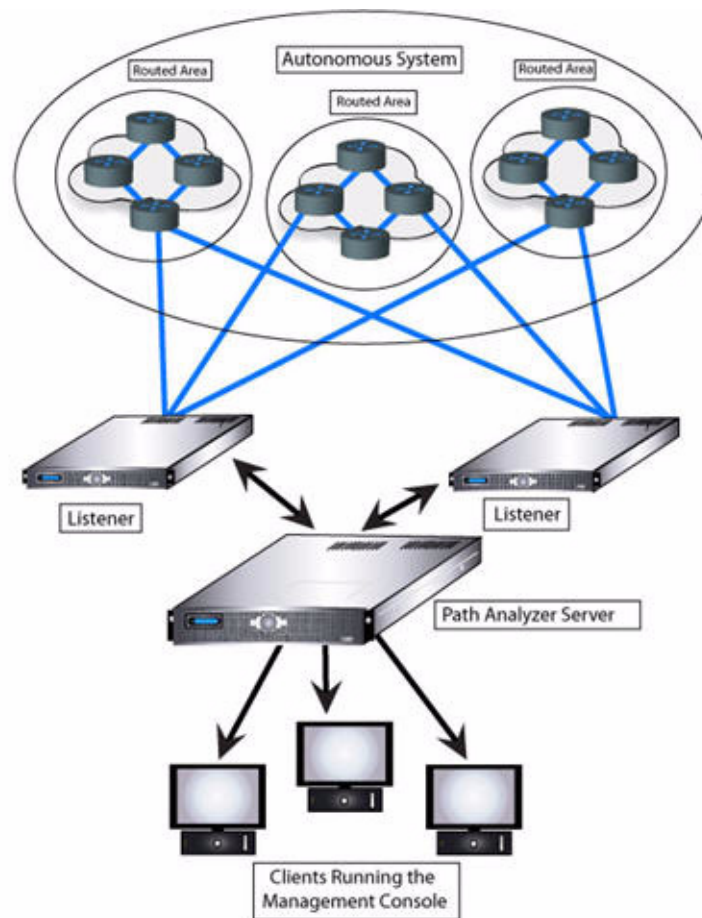
## Single Autonomous System

You can monitor routing activities within and between logical routing domains of a single autonomous system. Through an adjacency with an OSPF-enabled router or a BGP speaker, Listeners can collect and forward routing messages to the Path Analyzer Server.

In a single routing domain, Cisco recommends a redundant configuration of two or more Listeners with at least one virtual connection to the Path Analyzer Server. In the event of a power outage or a hardware problem on one Listener, the second Listener seamlessly maintains the connection. For information about redundant, failover configurations, see [Fault-Tolerant Configurations, page 6-10](#).

Figure 6-2 shows a redundant configuration within a single autonomous system.

**Figure 6-2** Redundant Listeners in an OSPF Routing Domain



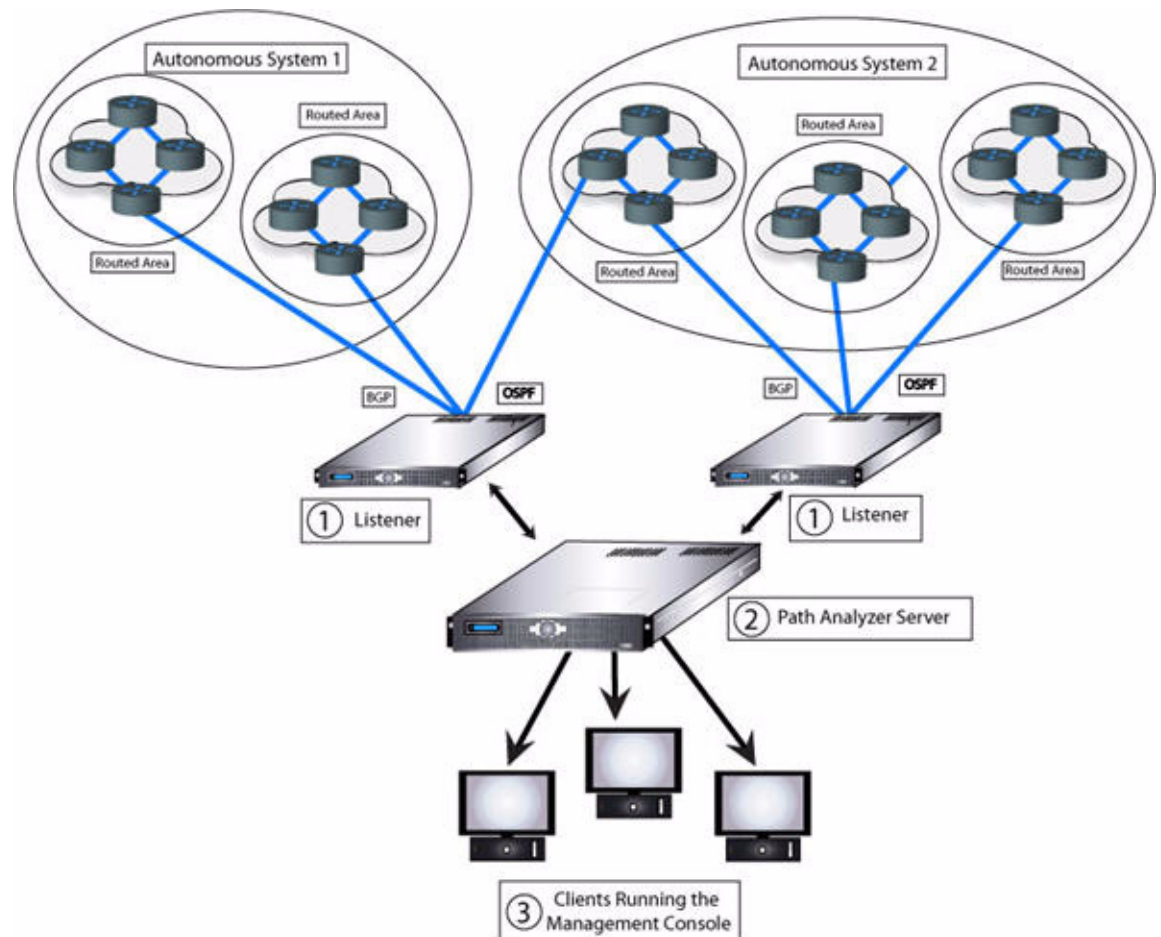


## Multiple Autonomous Systems

In a configuration that spans multiple autonomous systems, Listeners form adjacencies with external BGP (eBGP) speakers to collect routing information between autonomous systems. Within an autonomous system, Listeners form adjacencies with OSPF routers or interior BGP (iBGP) speakers.

Figure 6-3 shows a multiple autonomous systems.

**Figure 6-3** *OSPF and BGP Adjacencies in Multiple Autonomous Systems*



## Adjacencies for OSPF or BGP Collection

Adjacencies configured between Listeners and OSPF or BGP routers enable Path Analyzer to receive and generate an end-to-end view of routing activities across your network. The following sections explain possible configurations of adjacencies for OSPF and BGP collection.

## Configuring OSPF Adjacencies

Routers in an OSPF routing domain, called an area, continuously exchange routing updates in Link State Advertisements (LSAs). Continued updating ensures that all routers in an area have information recorded in their routing tables about all possible routes to destinations.

Due to the shared nature of OSPF updates, one adjacency between a Listener and an OSPF router provides Path Analyzer with complete visibility of routing activities in an area.

Path Analyzer supports the following types of connections to configure an adjacency between a Listener and an OSPF router:

- [Direct Adjacency](#), page 6-6
- [Generic Routing Encapsulation \(GRE\) Tunnel](#), page 6-7

### Direct Adjacency

To form an OSPF adjacency, you can physically or virtually connect a Listener to the OSPF interface of a router. Physical connections are formed by connecting one end of an Ethernet cable to a port on the Listener and connecting the other end to the port of a local router.

- Virtual adjacencies are formed by connecting a Listener to a Layer 2, or
- Layer 2/Layer 3 switch that carries packets between the Listener and the adjacent OSPF router. Multiple switches can reside between a Listener and the adjacent OSPF router.

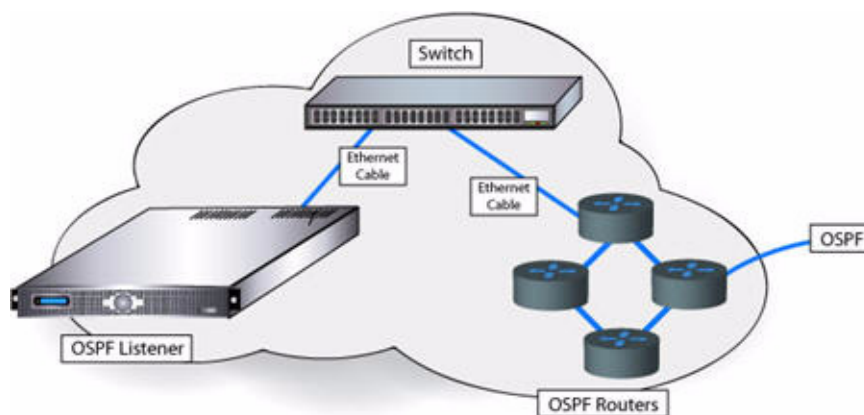


#### Note

Due to the size and geographical distribution of large networks, Listeners generally are not co-located with adjacent routers, and virtual connections are used.

[Figure 6-4](#) shows an example of a virtual connection formed between a Listener and a router through an Ethernet switch.

**Figure 6-4**      *Adjacency Between OSPF Listener and Router through Ethernet Switch*



[Table 6-1](#) explains the benefits of forming a direct adjacency between a Listener and an OSPF router.

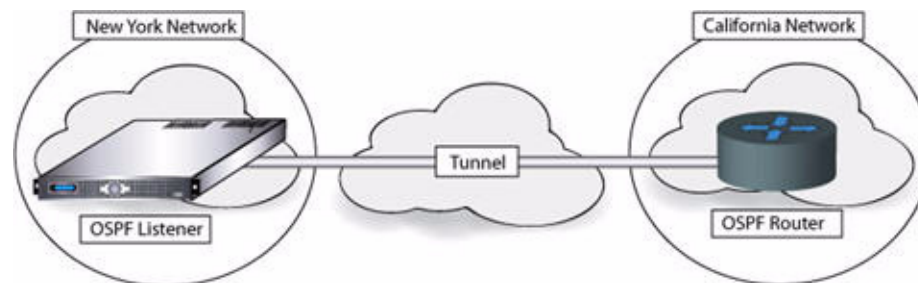
**Table 6-1** *Deployment Criteria Analysis for a Direct Adjacency*

Criteria	Description
<b>Advantages</b>	
System Reliability	Provides fewer points of failure between the OSPF router and a Listener.
Ease of Deployment	Requires no configuration changes on the OSPF router. Configuration of Listener ports is required. For information about configuring ports, see <a href="#">Configuring the Listener Connection to the Path Analyzer Server, page 6-14</a> .
Network Visibility	Provides immediate visibility into local OSPF routing.
Overhead	Enables Listeners to receive routing updates instantly without placing additional load on the network.
<b>Disadvantages</b>	
Ease of Device Management	Requires additional Listeners for visibility into remote OSPF areas, which increases the number of Listeners to maintain.
Cost	Adding Listeners increases system cost.

### Generic Routing Encapsulation (GRE) Tunnel

When a Listener and OSPF router are located too far away in the network to form a direct adjacency, Path Analyzer connects the devices through a GRE tunnel. The Listener and OSPF router exchange GRE packets, which are IP packets encapsulated within a larger packet for fast traversal through intermediate routers (the ‘tunnel’).

[Figure 6-5](#) shows how a GRE tunnel is used to form an adjacency between a Listener in New York and an OSPF router in California. Packets are exchanged between the Listener and router through the tunnel, which may comprise many intervening switches and routers.

**Figure 6-5** *Adjacency Formed Through a GRE Tunnel*

[Table 6-2](#) explains the benefits of an adjacency formed through a GRE tunnel.

**Table 6-2**      *Deployment Criteria for a GRE Tunnel*

Criteria	Description
<b>Advantages</b>	
Remote Visibility	Enables remote deployment of Listeners. Instrumentation of geographically-distributed OSPF areas using a single Listener appliance.  <b>Note:</b> Deployment requires a GRE tunnel configuration on the OSPF router. One static tunnel must be configured per OSPF area. Firewalls require a GRE tunnel-friendly configuration.
Ease of Device Management	Enables network visibility through a single Listener, resulting in fewer appliances to maintain.
Cost Savings	Keeps system costs down by enabling visibility into multiple OSPF areas through one Listener.
<b>Disadvantages</b>	
System Reliability	Introduces a single point of failure by using one Listener to monitor multiple OSPF areas. Problems on the path between the Listener and the adjacent OSPF router can prevent the Listener from collecting routing updates.
Overhead	Places additional load on network resources as OSPF routing updates are passed through the GRE tunnel to the Listener.

For detailed information about configuring a GRE Tunnel, see [Configuring a Collector, page 6-25](#).

## Configuring BGP Adjacencies

Routers in a BGP routing domain exchange packets over TCP port 179 to form an adjacency, update routing tables, and maintain the connection.

Path Analyzer supports the following types of connections to configure an adjacency between a Listener and a BGP router:

- [BGP Collection via TCP on a Shared Subnet, page 6-8](#)
- [BGP Collection via TCP Over the Network, page 6-9](#)

### BGP Collection via TCP on a Shared Subnet

When you plan to co-locate or instrument the Listener in the same part of the network as its BGP peer, you can form an adjacency between the devices on a shared subnet.

[Figure 6-6](#) shows an adjacency formed through a Layer 2 switch. The Listener and BGP peer exchange routing data over TCP/IP.

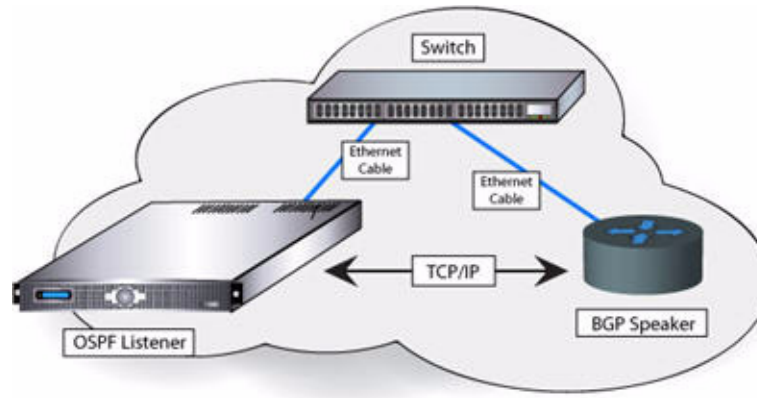
**Figure 6-6 BGP Collection over a Shared Subnet**

Table 6-3 explains the benefits of BGP collection over a shared subnet.

**Table 6-3 Deployment Criteria Analysis for BGP Collection Over a Shared Subnet**

Criteria	Description
<b>Advantages</b>	
System Reliability	Provides fewer points of failure between BGP speaker and Listener.
Ease of Deployment	Requires no configuration changes on the BGP speaker. Configuration of Listener ports is required. For information about configuring ports, see <a href="#">Configuring the Listener Connection to the Path Analyzer Server, page 6-14</a> .
Network Visibility	Provides immediate visibility into the BGP routing domain.
Overhead	Enables Listeners to receive routing updates instantly without placing additional load on the network.
<b>Disadvantages</b>	
Ease of Device Management	Requires additional Listeners for visibility into remote BGP networks, which increases the number of Listeners to maintain.
Cost	Adding Listeners increases system cost.

### BGP Collection via TCP Over the Network

When a Listener and BGP speaker are located too far away in the network for collection to occur over TCP on the same subnet, Path Analyzer establishes the adjacency via TCP over your enterprise network or across the Internet.

Figure 6-7 shows an example of this configuration.

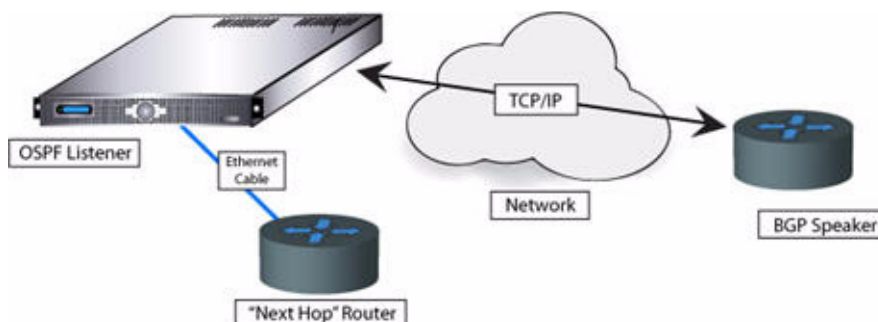
**Figure 6-7 BGP Collection via TCP/IP over the Network**

Table 6-4 explains the benefits of BGP collection over the network.

**Table 6-4 Deployment Criteria for BGP Collection Over the Network**

Criteria	Description
<b>Advantages</b>	
Remote Visibility	Enables remote deployment of Listeners. Instrumentation of geographically distributed BGP networks using a single Listener appliance.
Ease of Device Management	Enables network visibility through a single Listener, resulting in fewer appliances to maintain.
Cost Savings	Keeps system costs down by enabling visibility into multiple BGP networks through one Listener.
<b>Disadvantages</b>	
System Reliability	Introduces a single point of failure by using one Listener to monitor multiple BGP networks. Problems on the path between the Listener and the adjacent BGP speaker can prevent the Listener from collecting routing updates.
Overhead	Places additional load on network resources as BGP routing updates are passed through the network to the Listener.

## Fault-Tolerant Configurations

Path Analyzer Listeners are available in four-port configurations, enabling connections to up to four network areas.

To maintain the availability of Listener connections to the Path Analyzer Server and to your network, Path Analyzer offers the following fault-tolerant configurations:

- [Listener Availability, page 6-11](#)
- [Listener Redundancy, page 6-12](#)

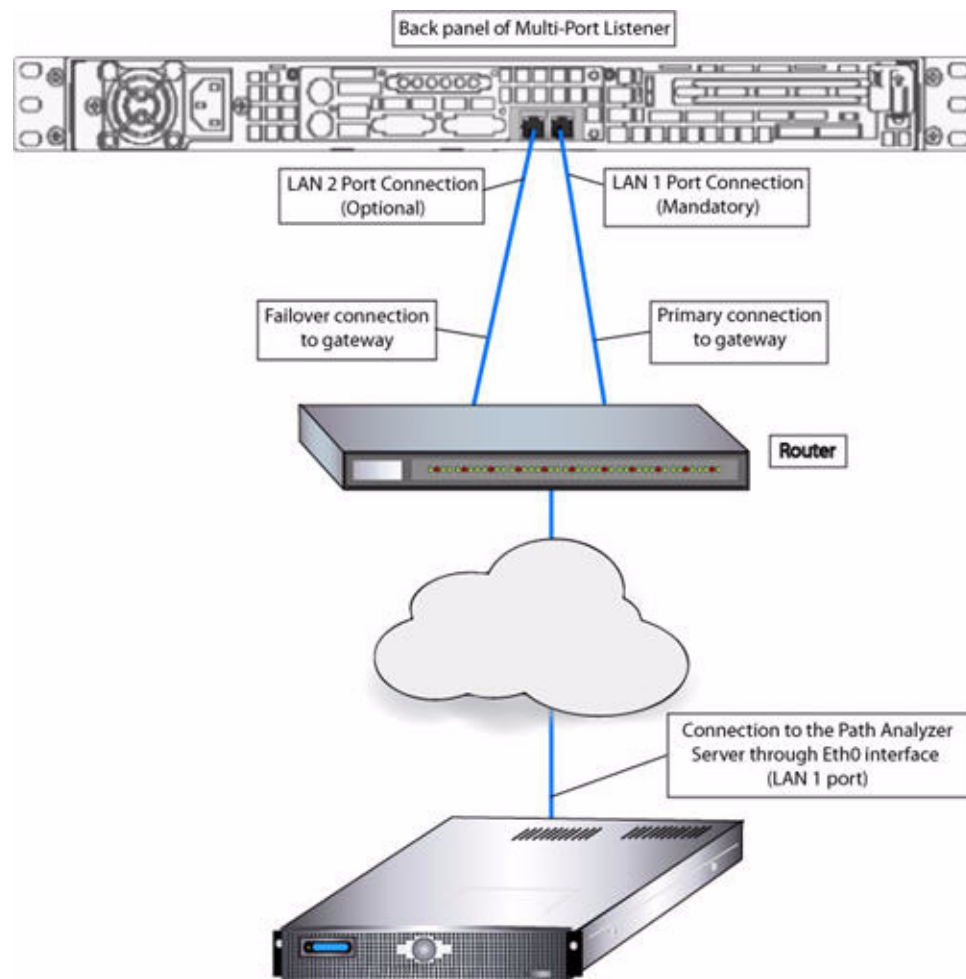
## Listener Availability

In a fault-tolerant configuration with Listener Availability, redundant connections between a Listener and a gateway ensures that your connection to the Path Analyzer Server is maintained if a port on the Listener becomes unavailable.

Maintaining connectivity to your Path Analyzer Server is essential to provide you with a real-time view of your network in the Path Analyzer Management Console.

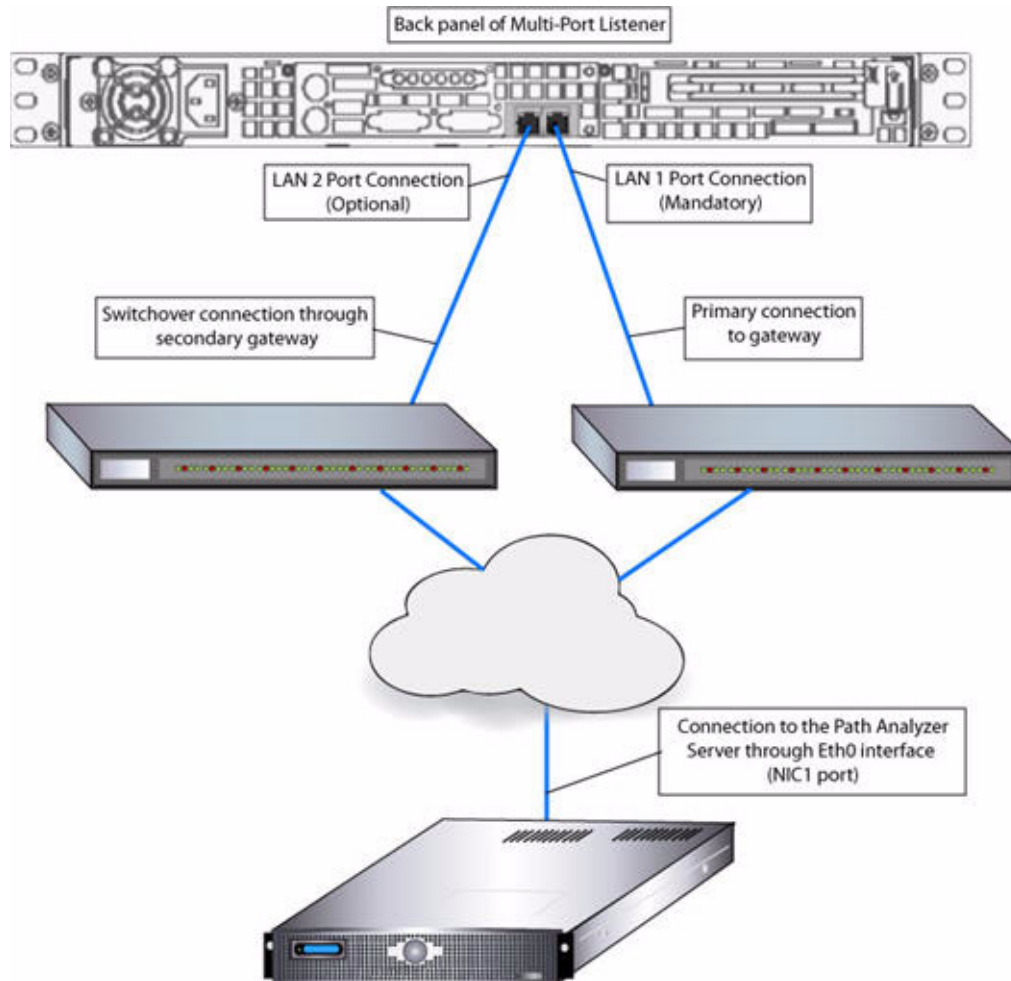
Figure 6-8 shows the configuration of redundant connections between the Multi-Port Listener and a gateway.

**Figure 6-8** *Listener Availability*



In Figure 6-9, if the connection between LAN1 and the default gateway becomes unavailable, connectivity is maintained by the second connection between the LAN2 port and the additional gateway.



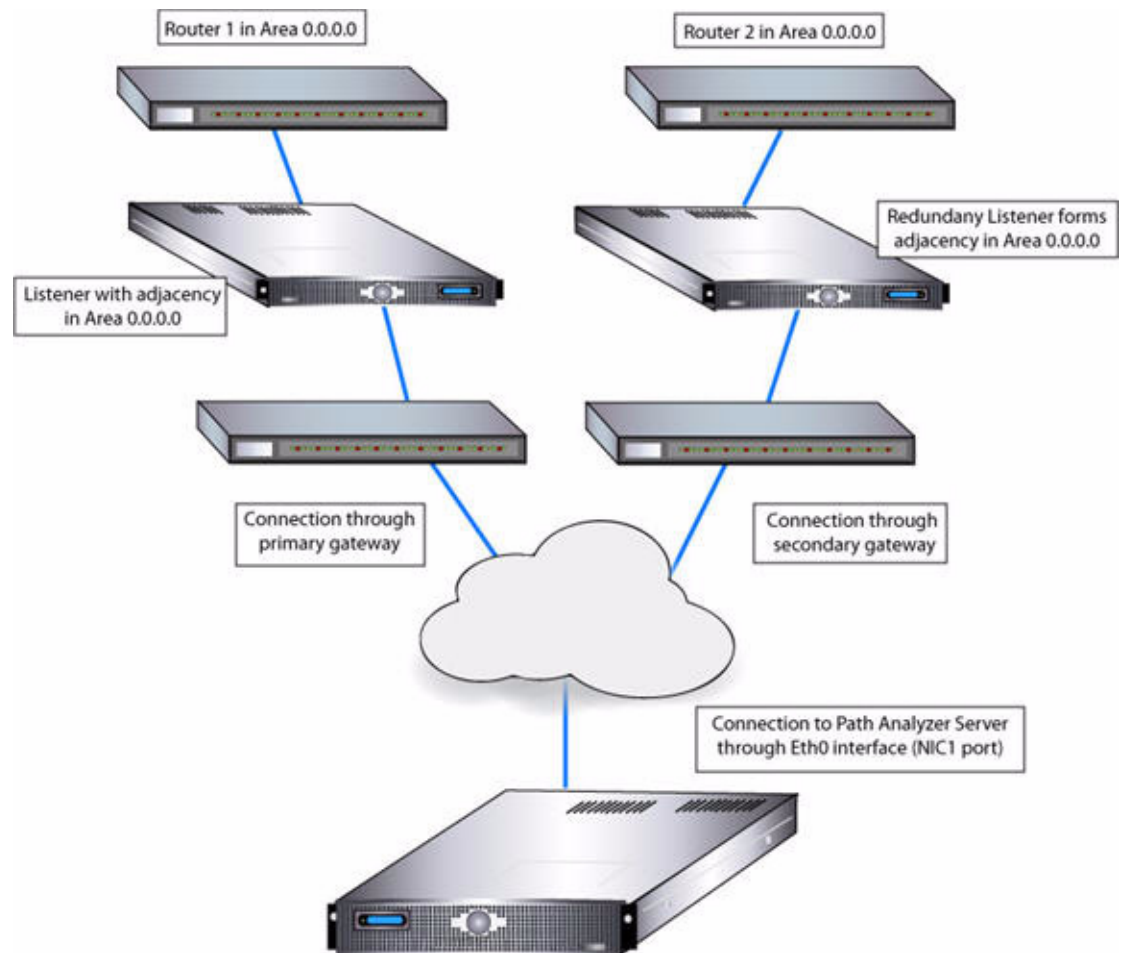
**Figure 6-9** Listener Availability with Multi-Gateway Connectivity

## Listener Redundancy

In a fault-tolerant configuration with Listener redundancy, one primary Listener and at least one backup Listener are connected to different routers or gateways in the same area. The primary Listener actively forwards routing information to the Path Analyzer Server. If either the primary Listener or its adjacent router become unavailable, the secondary Listener automatically continues to receive and forward routing information.

[Figure 6-10](#) shows a configuration with Listener Redundancy and Availability with Multi-Gateway Connectivity.



**Figure 6-10 Listener Redundancy and Multi-Gateway Availability**

## Configuring Path Analyzer Appliances

The following sections describe the tasks required to preconfigure Listeners and Collectors in a new Path Analyzer system. After the initial configuration, you can use the same set of procedures to add new Listeners and Collectors or change your configuration.

### Path Analyzer Initial Configuration Tasks

- [Configuring the Listener Connection to the Path Analyzer Server, page 6-14](#)
- [Configuring a Collector, page 6-25](#)

### Path Analyzer Maintenance Configuration Tasks

- [Reconfiguring a Listener, page 6-24](#)
- [Reconfiguring an OSPF Collector, page 6-35](#)

- [Reconfiguring a BGP Collector, page 6-41](#)
- [Statistics Tab, page 6-43](#)
- [Removing a Collector, page 6-50](#)
- [Removing a Listener, page 6-50](#)
- [Uninstalling the Management Console \(Windows Users\), page 6-50](#)
- [Uninstalling the Management Console \(Unix-Bases System Users\), page 6-51](#)

## Configuring the Listener Connection to the Path Analyzer Server

Through a physical or IP-based connection to the Path Analyzer Server, Listeners provide the Path Analyzer Server with real-time information they gather from adjacent routers.

After adding a Listener to your system in the System Administration module, see [Configuring a Collector, page 6-25](#).

### Adding a Listener

When you add a Listener to Path Analyzer, you must complete the following steps:

- [Starting System Administration, page 6-14](#)
- [Starting the Listener Configuration Wizard, page 6-14](#)
- [Entering Basic Settings, page 6-15](#)
- [Configuring a Backup IP Address, page 6-16](#)
- [Configuring Packet-Marking Parameters, page 6-16](#)
- [Configuring SNMP Trap/Polling Destination Parameters, page 6-17](#)
- [Set a System Login Banner, page 6-18](#)
- [Set System Users, page 6-19](#)
- [Configuring RADIUS Servers, page 6-20](#)
- [DNS Server Configuration, page 6-21](#)
- [NTP Server Configuration, page 6-22](#)
- [Setting Firewall Parameters, page 6-22](#)
- [Configure Access, page 6-23](#)
- [To Override Default or Normal Settings, page 6-24](#)

### Starting System Administration

To start system administration, click **Start > Administration > System** from the Path Analyzer taskbar. The System Administration window appears.

### Starting the Listener Configuration Wizard

To start the Listener Configuration wizard:

- 
- Step 1** Select the Path Analyzer Server you want to connect the Listener to from the configuration tree in the left side of the window.
- Step 2** Select the **Configuration** tab and click **Add Listener**.  
The Listener Configuration Wizard starts.
- Step 3** (Optional) Click the **Do not show this screen again** check box.
- Step 4** Click **Next**.  
The Do you want to use an existing Listener as a template? screen appears. Select one of the following options:
- **Yes**—Use the configuration of an existing Listener as a template for creating a new one.
  - **No**—Create a new Listener without an existing configuration as a basis.
- Step 5** Click **Next**.  
The Set Basic Parameters screen appears. If you selected “No” on the previous screen, the fields are blank. If you selected “Yes,” the screen shows the default values for the new Listener. You can delete the default values and enter new values, or you can accept the default settings.
- 

## Entering Basic Settings

To enter basic settings in the Listener Configuration wizard:

- 
- Step 1** Enter configuration settings for the new Listener:
- a. Enter the IP address or host name of the Listener interface that connects to the Path Analyzer Server in the Address field. This interface forms the primary connection to the Path Analyzer Server.
  - b. Select **Up** in the Admin State field to enable the connection between the Listener and the Path Analyzer Server.



### Note

You can disable the connection between a Listener and the Path Analyzer Server if an event occurs that requires you to remove a Listener from your network, or if your Listener cannot be reached by the Path Analyzer Server.

---

- c. Enter the Listener TCP port used to communicate with the Path Analyzer Server in the Port field.  
The default TCP Port is 1061.
- d. Enter the number of milliseconds that must elapse before the Path Analyzer Server polls the Listener to ensure connectivity in the Poll Period field.  
The default Poll Period is 30,000 milliseconds (30 seconds).
- e. Enter the number of milliseconds that must elapse before the Path Analyzer Server attempts to re-establish a connection with a Listener if disconnection occurs in the Retry Period field.  
The default Retry Period is 60,000 milliseconds (60 seconds).
- f. Enter a character string that describes the location of the Listener in the Location field.  
Example:  
**Bldg 201 Closet 2 Rack 1 Shelf 3**

**Step 2** Click **Next**.

The Backup IP Addresses screen of the Listener appears, in which you can configure backup, or failover, addresses that the Path Analyzer Server can use to reach the Listener if the primary address of the Listener becomes unavailable.

## Configuring a Backup IP Address

To configure a backup IP address in the Listener Configuration wizard:

**Step 1** Enter a backup IP address or host name for the Listener in the blue field of the Backup IP Addresses screen.

**Step 2** Click **Add**.

The IP address appears in the Backup IP Addresses table. You can have up to five failover connections with the Path Analyzer Server.

**Step 3** Click **Next**.

The Packet Marking Parameters screen appears (see [Figure 6-11](#)).

## Configuring Packet-Marking Parameters

**Figure 6-11** Packet-Marking Parameters Screen

To configure packet-marking parameters in the Listener Configuration wizard:

**Step 1** Select and complete the following options:

- Ethernet Port—Select a port from the drop-down box. This port will mark all outgoing traffic.

- Protocol Port—Select a protocol from the drop-down box, such as TCP or OSPF. This indicates the type of traffic you want to mark. If you want to mark BGP packets, select TCP.
- Source Port—Enter the source port for the Listener you are configuring.
- Destination Port—Enter the destination port for the traffic.
- DSCP Marking—Differentiated Services Code Point Marking sets priorities for outgoing packets by marking them with specific DSCP numbers. These numbers (0-63) can be associated with appliances or services, such as a particular server or customer service.

**Step 2** Click **Add**.

The information will appear on the table. When the wizard is finished, DSCP settings in the table are installed in the device.

**Step 3** Click **Next**.

The SNMP Trap/Polling Destination Parameters screen appears (see [Figure 6-12](#)).

**Figure 6-12** *SNMP Settings in Listener Configuration Wizard*

The screenshot shows the 'Listener Configuration Wizard' window. The title bar says 'Listener Configuration'. The main title is 'Listener Configuration Wizard'. Below the title, it says 'Please set the SNMP Trap/Polling Destination parameters.' There are two main sections. The first section is for SNMP Traps, with a checked box 'Do you want to enable SNMP Traps?'. Below this are dropdown menus for 'Monitor Java:' (set to 'yes'), 'Monitor CPU/Disk:' (set to 'yes'), and 'SNMP Version:' (set to '2c'). There are text input fields for 'Trap Receiver:' (highlighted in blue), 'Community:' (set to 'public'), 'Port:' (set to '162'), 'Location:', and 'Contact:'. The second section is for SNMP Polling, with a checked box 'Do you want to enable SNMP Polling?' and a 'Community:' field set to 'public'. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

## Configuring SNMP Trap/Polling Destination Parameters

The SNMP Trap/Polling Destination Parameters screen allows you to configure the Listener to generate and send SNMP traps to a network management system. You can also choose whether the Listener should respond to polls from the network management system.

To configure SNMP trap/polling destination parameters in the Listener Configuration wizard:

**Step 1** Click the check box to enable SNMP traps.

**Step 2** Select and complete the following options to set the parameters for monitoring the device.

- **Monitor Java**—Selecting “yes” enables the monitoring of Java processes running on the Listener. A trap is sent to the network management system whenever a Java process goes down. The default setting is **yes**.
- **Monitor CPU**—Selecting “yes” enables the system to monitor the Listener’s CPU usage. If the usage exceeds a pre-defined setting, the Listener sends a trap to the network management system. The default setting is **yes**.
- **SNMP Version**—Enter the version of traps your SNMP management device should receive. The default setting is **SNMP v2c**.
- **Trap Receiver**—Enter the destination that should receive the traps that the device sends.
- **Community String**—Enter the appropriate community string or password designated for receiving devices that use SNMP. The default setting is **public**.
- **Port**—Enter the SNMP port that the Listener uses to send traps. The default setting is **162**.
- **Location**—(Optional) Enter the name of the server or the trap receiver where the Listener is deployed.
- **Contact**—(Optional) Enter the name of the network administrator or other individual responsible for managing Path Analyzer.

**Step 3** Click the **Do you want to enable SNMP Polling?** check box to enable SNMP polling.

**Step 4** Enter the appropriate community string or password designated for sending devices that use SNMP In the Community text box. The default setting is **public**.

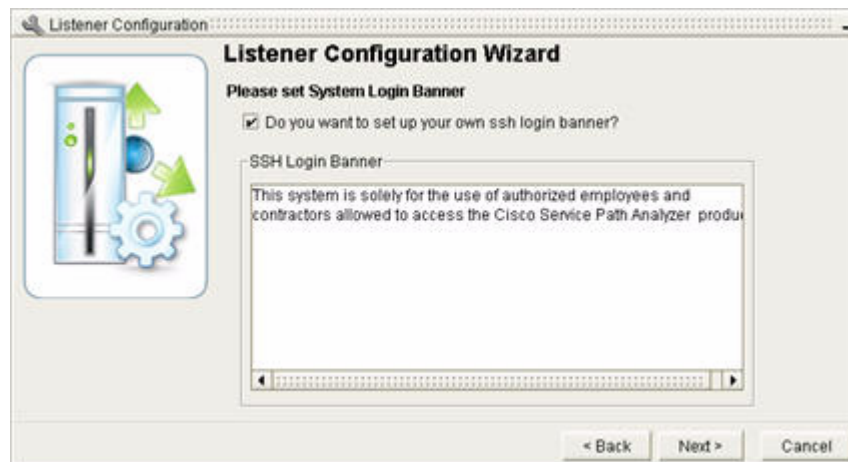
**Step 5** Click **Next**.

The System Login Banner screen appears (see [Figure 6-13](#)).

## Set a System Login Banner

The System Login Banner screen will permit you to set up a banner that is displayed to system users (SSH) when they log in. You have any option to set up the banner and you can enter the banner text.

**Figure 6-13** System Login Banner Screen



To set a system login banner in the Listener Configuration wizard:

- Step 1** Click the check box and enter the banner text to be displayed to users when they log in. If you do not want a system login banner, do not select the check box.
- Step 2** Click **Next**.
- The System Users screen appears (see [Figure 6-14](#)).

**Figure 6-14 Set System Users Screen**



## Set System Users

The System Users screen will enable you to create a password and user name for system users (SSH) who wish to access Path Analyzer.

To set system users in the Listener Configuration wizard:

- Step 1** Click the check box If you wish to enable system users (SSH).
- Step 2** Enter the user name and password of each user in the appropriate field.
- Step 3** Click **Add** after each entry.
- The name and password will appear in the box above.
- Step 4** Click **Next**.
- The Configure RADIUS Server screen appears (see [Figure 6-15](#)).

**Figure 6-15** Settings for Primary and Secondary RADIUS Servers.

## RADIUS Server Configurations

The primary RADIUS (Remote Authentication Dial In User Service) Server authenticates Management Console access and SSH access to the Listener for system users. The secondary RADIUS Server acts as a back up for the primary server and takes over the authentication process if the primary server does not respond with the appropriate access within the designated timeout period. The RADIUS checks that the user name and password information is correct using the PAP authentication scheme.

The RADIUS authentication feature is disabled by default, unless you turn it on.

## Configuring RADIUS Servers

To configure RADIUS servers in the Listener Configuration wizard:

- Step 1** To configure a primary RADIUS server, click the check box: **Do you want to enable RADIUS?**
- Step 2** To configure a secondary RADIUS server click the check box **Do you want to add a secondary RADIUS Server?**
- Step 3** Select a user type (limited, admin, or power) from the Default User Type field under the first check box. Path Analyzer creates a new account with this user type and associated user preferences when a new user logs in via the login screen of the Management Console.
- Step 4** Complete the remaining fields under both check boxes:
  - **Hostname**—Enter the IP address or host name of the RADIUS Server that is used to authenticate users.
  - **Timeout(s)**—Accept the default timeout or enter a timeout period. The timeout period specifies the number of seconds the Path Analyzer Server waits for a reply to a RADIUS request before retransmitting the request. The default is 15 seconds.
  - **Port Number**—The port number specifies the destination port. Enter the port number or accept the default.



- **Secret Key**—Enter the secret key for the RADIUS Server. The secret key specifies the shared secret text string used between the Path Analyzer Server and the RADIUS Server, used to encrypt passwords and exchange responses.

**Step 5** Click **Next**.

The DNS Server screen appears (see [Figure 6-16](#)).

If RADIUS authentication is enabled, users are authenticated against RADIUS when they log in for the first time, unless they have already been explicitly added into the RD Management Console. See [Adding a New User Account](#), page 7-3.

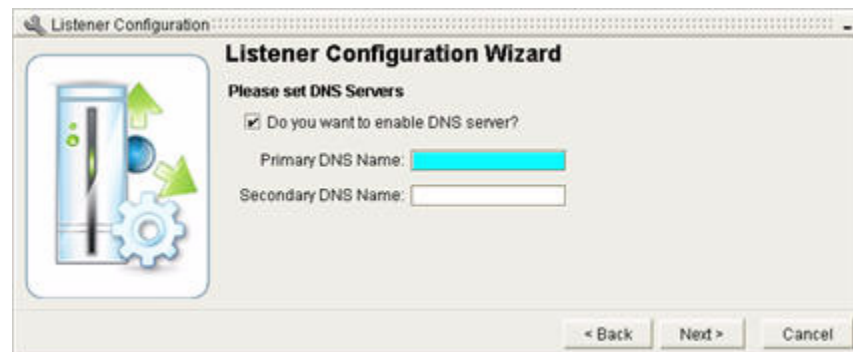
During their first login, new users are automatically assigned the default type according to the default parameters previously configured in the Management Console. User access types can be changed (to “admin,” for example). See [Changing Details of a User Account](#), page 7-5.

Users added via the RD Management Console are set to authenticate locally. See [Adding a New User Account](#), page 7-3 to add users to the Management Console.

The RADIUS authentication for systems users (SSH) is different. Once RADIUS is configured, all system users are authenticated against RADIUS. The local password will only be used if RADIUS is down.

## DNS Server Configuration

**Figure 6-16** Set DNS Servers



To configure a DNS server in the Listener Configuration wizard:

**Step 1** Click the check box **Do you want to enable DNS server?** and complete the following fields:

- **Primary DNS Name**—Enter the name or IP address of the primary DNS server.
- **Secondary DNS**—In this optional field, enter the name or IP address of the backup DNS server.

**Step 2** Click **Next**.

The Configure NTP Server screen appears (see [Figure 6-17](#)).

## NTP Server Configuration

**Figure 6-17** Set NTP Servers



To configure an NTP server in the Listener Configuration wizard:

- 
- Step 1** To enable an NTP server, enter the IP address or DNS name of the NTP Server in the **NTP Server** field.
  - Step 2** Click **Add**.
  - Step 3** Click **Next**.

The Set Firewall Parameters screen appears (see [Figure 6-18](#)).

---

## Setting Firewall Parameters

You can activate a firewall to secure your Path Analyzer Server. Firewall rules specify the transmission criteria for all packets and targets. Packets that do not satisfy the firewall rules will be dropped. Decide which services you want to grant access to and then complete the following procedures:

**Figure 6-18** Settings for Firewall

The screenshot shows the 'Listener Configuration Wizard' window. On the left is an icon of a server with a green arrow pointing up and a gear. The main title is 'Listener Configuration Wizard'. Below it, the text says 'Please set the Firewall setting parameters'. There is a checked checkbox 'Do you want to enable Firewall?'. To the right of this is a section 'Choose A Service' with four radio buttons: 'SSH', 'SNMP', 'OSPF', and 'GRE'. To the right of this is a text box labeled 'Allowed IP Addresses' with 'Add' and 'Delete' buttons below it. Below the 'Choose A Service' section is a checked checkbox 'Prohibit the system from connecting to non-listed networks'. Below this is a note: 'Note: If this box is checked, ALL BGP connections will be blocked'. Below the note is a text box labeled 'Additional allowed Subnets' with 'Add' and 'Delete' buttons below it. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

To set firewall parameters in the Listener Configuration wizard:

- 
- Step 1** The firewall is enabled by default; you can disable it by removing the check mark. Choose a service that the firewall should grant access to:
- Web Management Console
  - Secure Shell (SSH)
  - Path Analyzer Management Console
  - Simple Network Management Protocol (SNMP) Console
- Step 2** Enter the IP addresses of the subnets that you want to grant access to via the specified service.
- Step 3** Click **Add**.

The information appears in the table, and then it is sent to the device.

The established connections are outbound connections. The Path Analyzer Server is then allowed to initiate outbound connections to any listed networks.

---

## Configure Access

To restrict access to a specific service, click the button next to the service you wish to restrict.

To prohibit the system from connecting to non-listed networks, check the **Prohibit the system from connecting to non-listed networks** checkbox.

To permit access to a specific service not listed on the screen:

- 
- Step 1** Complete one of these options:
- Uncheck the box next to **Prohibit the system from connecting to non-listed networks**, or
  - Enter the IP address of a specific subnet in the field next to **Add**.
- Step 2** Click **Add**.
- The information will appear in the above box. Repeat the process to define a connection with another subnet, or
- Step 3** Click **Next** to complete the Firewall configuration process.
- Step 4** Click **Finish** when the Server configuration is complete.
- 

## To Override Default or Normal Settings

In the event that you encounter a configuration problem with the initial setup which you cannot resolve in the Management Console, you can use the Configuration Tool. You have a choice of the following commands:

- `firewall ip address`, or
- `firewall off`

The first command allows you to enter a network address (if you are connecting remotely). It will permit you to make changes to the Path Analyzer Server.

The second command disables the firewall and allows you to make changes.

See [The Configuration Tool, page 3-1](#).

## Reconfiguring a Listener

To reconfigure a listener:

- 
- Step 1** Click **Start > Administration > System**.
- The System Administration window appears.
- Step 2** Select the Listener you want to change from the configuration tree in the left side of the window.



### Note

To reconfigure, you must select a Listener, not the Server. You select the Server when you wish to add a new Listener.

---

- Step 3** Click **Reconfigure** in the Configuration tab.
- Step 4** The Listener Configuration Wizard starts, showing the Set Basic Parameters Page, used for [Entering Basic Settings, page 6-15](#). You can delete the existing values and enter new values where you wish.
- The rest of the screens in the wizard are the same as those you use for Adding a Listener. See [Adding a Listener, page 6-14](#).

# Configuring a Collector

A Collector is the virtual router, the internal, software-based part of the Listener that directly forms an adjacency with a router interface and collects routing information. For each Listener in your Path Analyzer system, you can configure one or more Collectors. See [Configuring an OSPF Collector, page 6-25](#) and [Configuring a BGP Collector, page 6-35](#).

## Configuring an OSPF Collector

You will need to perform the following tasks to configure a new OSPF Collector or change the configuration of an existing OSPF Collector:

- [Start the Collector Configuration Wizard, page 6-25](#)
- [Select Collector Protocol, page 6-26](#)
- [Derive or Create an OSPF Collector, page 6-26](#)
- [Set Basic OSPF Parameters, page 6-27](#)
- [Configuring Static Neighbors \(NBMA, P2P, or PTMP Networks Only\), page 6-28](#)
- [Set Inter-Area Parameters, page 6-29](#)
- [Configure a GRE Tunnel \(optional\), page 6-30](#)
- [Set Advanced OSPF Parameters, page 6-30](#)
- [Set Intervals and Delays, page 6-32](#)
- [Set Authentication, page 6-33](#)
- [Message Digest \(MD\) 5 Authentication Features \(Optional\), page 6-34](#)

## Adding a New OSPF Collector

To add a new OSPF collector:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Click <b>Start &gt; Administration &gt; System</b> . The System Administration window appears.                        |
| <b>Step 2</b> | From the configuration tree in the left side of the window, select the Listener to which you want to add a Collector. |
- 

## Start the Collector Configuration Wizard

To start the Collector Configuration wizard:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Click <b>Add Collector</b> in the Configuration tab.<br>The Collector Configuration Wizard starts. |
| <b>Step 2</b> | (Optional) Click the <b>Do not show this screen again</b> check box.                               |
| <b>Step 3</b> | Click <b>Next</b> .  |

The Please Select the Collector's Protocol screen appears (see [Figure 6-19](#)).

## Select Collector Protocol

**Figure 6-19** Collector Protocol Screen in Collector Configuration Wizard



To select the Collector protocol in the Collector Configuration wizard:

- Step 1** Select **OSPF** to create a Collector that passively participates in OSPF routing. That is, it receives, but does not forward the Link State Advertisements (LSAs) of OSPF routers.
- Step 2** Click **Next**.

The Derive or Create Collector screen appears (see [Figure 6-20](#)).

## Derive or Create an OSPF Collector

**Figure 6-20** Derive or Create an OSPF Collector Screen in Collector Configuration Wizard



To derive or create an OSPF collector in the Collector Configuration wizard:

- Step 1** Select one of the following options for setting configuration parameters:
  - **Yes**—Use the configuration of an existing OSPF Collector as a template for creating a new one.

If you select this option, fields in each of the subsequent Collector Configuration Wizard screens display the values of the previously configured Collector. You can select and change the values or leave them as they are.

- **No**—Create a new OSPF Collector without an existing configuration as a basis.

**Step 2** Click **Next**.

The Set Basic OSPF Parameters screen appears, in which you Set Basic OSPF Parameters for the OSPF Collector.

The set basic OSPF parameters screen appears (see [Figure 6-21](#)).

## Set Basic OSPF Parameters

**Figure 6-21** Basic OSPF Collector Parameters Screen in Collector Configuration Wizard



To set basic OSPF parameters in the Collector Configuration wizard:

**Step 1** Enter a name to uniquely identify the Collector in the Collector ID field.

**Step 2** Select one of the following options in the Admin State field:

- **Up**—Enables the Collector immediately.
- **Down**—Causes the Collector to remain in an inactive state until you are ready to enable it.

**Step 3** Select one of the following options in the Interface Type field:

- **Broadcast**—Connect the Collector to a router interface on the Designated Router (DR) of a Transit network.
- **NBMA**—Connect the Collector to a router interface that attaches to a Non-Broadcast Multiple Access (NBMA) network.
- **PTP**—Connect the Collector to a router interface that attaches to a Point-to-Point (P2P or PTP) network.
- **PTMP**—Connect the Collector to a router interface that attaches to a Point-to-Multicast-Point (PTMP) network.

**Step 4** Select the routing domain of the OSPF Collector in the Domain field.

**Step 5** Click **Next**.

- If you configure an OSPF Collector for an NBMA, PTP, or PTMP network, the Configure Static Neighbors screen appears (see [Figure 6-22](#)), in which you configure static neighbors for the OSPF Collector.

*or*

- If you configure an OSPF Collector for a Broadcast network, the Set Inter-Area OSPF Parameters screen appears (see [Figure 6-23](#)), in which you set inter-area parameters for the OSPF Collector.
  - In a network with broadcast capabilities, a Designated Router (DR) broadcasts HELLO packets and routing updates to other routers attached to the network.
  - In an NBMA, P2P, or PTMP network, broadcasting capabilities are not available from an assigned DR. Instead, you configure static neighbors for a router. Each static neighbor is assigned a priority value that determines which router in the network can act as the DR on an as-needed basis, and send HELLO packets via unicast (in a P2P network) or multicast (in a PTMP network) to other routers in the area.

## Configuring Static Neighbors (NBMA, P2P, or PTMP Networks Only)

**Figure 6-22** Static Neighbors Screen in Collector Configuration Wizard

To configure static neighbors in the Collector Configuration wizard:

- Step 1** Enter the Router ID of the router configured with the point-to-point interface to which the Listener connects in the Router field.
- Step 2** Enter the IP address of the point-to-point interface in the Address field.
- Step 3** Enter a priority for the neighbor (0-255) in the Priority field.
- Step 4** Click **Add**.  
Your settings are displayed in the table.
- Step 5** Click **Next**.



The Set Inter-Area OSPF Parameters screen appears, in which you set inter-area parameters for the OSPF Collector.

The Inter-Areas Parameters screen appears (see [Figure 6-23](#)).

## Set Inter-Area Parameters

To set Inter-Area parameters in the Collector Configuration wizard:

- Step 1** Set attributes of the connection between the Collector and a router.
- Enter the Router ID of the OSPF router adjacent to the OSPF Collector in the Router ID field.
  - Enter the unique identifier of the area the router resides in into the Area ID field.
  - Enter the IP address of the interface used by the Collector in the Interface Address field. This field applies to all interface types except Unnumbered Point-to-Point (UP2P) interfaces.
  - Enter the subnet mask of the subnet that receives data flow over the router interface in the Interface Mask field.
  - Enter the Management Information Base (MIB) Index of the UP2P interface in the Interface Index field. For an NP2P interface, enter “0”.
  - Select the port that the Listener assigns to the router interface in the Port field.
  - Click the **GRE Tunnel** check box to create a GRE tunnel between the OSPF Collector on the Listener interface and the adjacent router.

For information about the advantages of GRE tunneling for an OSPF Collector, see [Adjacencies for OSPF or BGP Collection](#), page 6-5.

**Figure 6-23** Inter-Area Parameters Screen in Collector Configuration Wizard



- Step 2** Click **Next**.

If you select to [Configure a GRE Tunnel \(optional\)](#), page 6-30 for the OSPF Collector, the Set GRE Tunnel Parameters screen appears (see [Figure 6-24](#)).

or

If you do not select [Configure a GRE Tunnel \(optional\)](#), page 6-30 for the OSPF Collector, the Set Advanced OSPF Parameters screen appears, in which you set advanced parameters for the OSPF Collector.

## Configure a GRE Tunnel (optional)

**Figure 6-24** GRE Tunnel Screen in Collector Configuration Wizard

The screenshot shows a window titled "Collector Configuration" with a sub-header "Collector Configuration Wizard". Below the header is a message: "Please fill in the collector's GRE tunnel parameters...". There are four text input fields: "GRE Tunnel Source Address:", "GRE Tunnel Source Mask:", "GRE Tunnel Destination Address:", and "GRE Tunnel Destination Next Hop:". To the left of the fields is an icon of a stack of colorful blocks and a gear. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

To configure a GRE tunnel in the Collector Configuration wizard:

- Step 1** Enter the IP address of the Listener interface that serves as the source of the GRE tunnel in the GRE Tunnel Source Address field.
- Step 2** Enter the subnet mask of the Listener interface in the GRE Tunnel Source Mask field.
- Step 3** Enter the IP address of the router that forms an adjacency with the OSPF Listener in the GRE Tunnel Destination Address field.
- Step 4** Enter the IP address of the next hop for the destination in the GRE Tunnel Destination Next Hop field.



**Note**

Because of the configured next hop, the Listener does not use the routing information it receives from the network to make its own routing decision. It uses the setting you apply in the **GRE Tunnel Destination Next Hop** field.

- Step 5** Click **Next**.  
The Set Advanced OSPF Parameters screen appears (see [Figure 6-25](#)), in which you set advanced parameters for the OSPF Collector.

## Set Advanced OSPF Parameters

Cisco recommends that you retain the default values provided in the OSPF Advanced Parameters Page. For information about the fields, refer to RFC 2328 of the OSPF Working Group of the Internet Engineering Task Force (IETF), located at [www.ietf.org](http://www.ietf.org).

**Figure 6-25** Advanced Parameters Screen in Collector Configuration Wizard


To set advanced parameters in the Collector Configuration wizard:

- Step 1** Enter the number of milliseconds that must elapse before the Path Analyzer Server polls each configured Collector in the Poll Period (msec) field.  
The default polling period is 10,000 milliseconds (10 seconds).
- Step 2** Enter the multiplier required to determine the number of milliseconds that must elapse before using a failover Collector in the Switch-Over Ticks field.
  - The Path Analyzer Server sends poll packets to each Collector to determine its availability.
  - Setting the Polling Period to 10,000 milliseconds (10 seconds) and the Switch-Over Ticks period to 60,000 milliseconds (60 seconds) causes the Path Analyzer Server to switch to another Collector in the same area if the Collector fails to respond after 60 seconds.
  - The failover time is equivalent to the Switch-Over Ticks setting (6) multiplied by the Polling Period (10,000 milliseconds), totalling 60,000 milliseconds (60 seconds). You can select a different Switch-Over Tick value.
- Step 3** Enter the number of LSAs for the Collector buffer in the Buffer Size (LSA) field.
  - The buffer holds data between the Collector and the Path Analyzer Server. The default buffer size is 5,000 LSAs.
  - Increase the value if the instrumented OSPF area contains a large number of LSAs. For example, you can increase the value up to 100,000 LSAs for a large network topology.
- Step 4** Enter the number of bytes for the Maximum Transmission Unit, the largest packet size that the Collector can receive from and send to the router interface, in the MTU (bytes) field. The default value is 1500 bytes.
- Step 5** Indicate whether the Collector connects to a router interface that forwards to a stub route in the Stub field.  
Select one of the following options:
  - **Yes**—Indicates that the Collector connects to a router interface that forwards to a stub route.
  - **No**—Indicates that the Collector does not connect to a router interface that forwards to a stub route.
- Step 6** Enter the cost associated with the virtual router interface in the Cost field.
- Step 7** Click **Next** to save your settings.

The Set Intervals and Delays screen appears (see [Figure 6-26](#)), in which you set intervals and delays for the OSPF Collector.

## Set Intervals and Delays

**Figure 6-26** Fill in the Collector's Parameters Screen in Collector Configuration Wizard



To set intervals and delays in the Collector Configuration wizard:

- Step 1** Enter the number of seconds that must elapse before the Collector sends a Hello packet to the adjacent router on the network to determine its availability in the Hello Interval (sec) field. The default value is 10 seconds.
- Step 2** Enter the number of seconds that must elapse before the Collector establishes that its adjacent neighbor is unavailable in the Inactivity Interval (sec) field. The default value is 40 seconds.
- Step 3** Enter the number of seconds that must elapse before the Collector polls an adjacent router interface in an NBMA network in the OSPF Poll Interval (sec) field. The default value is 2 minutes.
- Step 4** Enter the number of seconds that must elapse to determine the age of an update packet in the Retransmission Delay (sec) field. The default value is 10 seconds.
- Step 5** Enter the number of seconds that must elapse between each transmission to the Collector and the adjacent router in the Transmission Delay (sec) field. The default value is 1 second.
- Step 6** Click **Next** to save the new settings.

The Set Authentication Type screen appears (see [Figure 6-27](#)), in which you set authentication for the OSPF Collector.

## Set Authentication

**Figure 6-27** Collector Authentication Type Screen in Collector Configuration Wizard



To set authentication type in the Collector Configuration wizard, select one of the following options in the **Authentication** field:

---

**Step 1** Select **None**, which allows a Collector to form an adjacency with the neighboring router without authentication.

**Step 2** Click **Next**, then click **Finish** to complete the wizard.

*or*

---

**Step 1** Select **Password** to enable the neighboring router to authenticate the Collector through a common password before forming an adjacency.

**Step 2** Enter the shared password in the Password field.

**Step 3** Click **Next**, then click **Finish** to complete the wizard.

*or*

---

**Step 1** Select **MD5 Keys** to enable the neighboring router to authenticate the Collector using Message Digest (MD5) Key encryption. See [Message Digest \(MD\) 5 Authentication Features \(Optional\)](#), page 6-34.

**Step 2** Click **Next**.

The new OSPF and Authentication Features are assigned to the Collector.

The Set MD5 Authentication Parameters screen appears (see [Figure 6-28](#)), in which you set Message Digest (MD5) authentication parameters for the OSPF Collector.

---

## Message Digest (MD) 5 Authentication Features (Optional)

**Figure 6-28** MD5 Parameters Screen in Collector Configuration Wizard

**Collector Configuration Wizard**

Please configure this collector's MD5 parameters...

Id	Key	Start Accept	Start Generate	Stop Accept	Stop Generate

Id:  Key:

Start Accepting:  Stop Accepting:  ☐ Never

Start Generating:  Stop Generating:  ☐ Never

To set MD5 authentication features in the Collector Configuration wizard:

- 
- Step 1** Select **MD5** in the Authentication field.
- Fields and values are displayed for configuring MD5 authentication.
- Step 2** Enter the unique character string that identifies the MD5 key shared by the Collector and the router interface in the **Id** field.
- From the **Start Accepting** field, select a date and time for the Collector to start accepting OSPF packets over the router interface with the MD5 key.
  - From the **Start Generating** field, select a date and time for the router interface to start generating OSPF packets for the Collector with the MD5 key.
- Step 3** Enter the key that the Collector and the router interface use for authentication in the Key field. Empty, square characters are used to indicate the total length of the key. For security purposes, the key is not displayed.
- From the **Stop Accepting** field, select a date and time for the Listener to stop accepting OSPF packets from the router interface with the MD5 key.
- Select **Never** to allow the Listener to continue using the MD5 key to authenticate the router interface and accept OSPF packets without interruption.
- From the **Stop Generating** field, select a date and time for the router interface to stop generating OSPF packets for the Collector.
- Select **Never** to never stop the router interface from generating OSPF packets for the Listener.
- Step 4** Click **Next**.
- Step 5** Click **Finish** to complete the wizard.
- The new settings are applied and are displayed in the MD5 table.
-

## Reconfiguring an OSPF Collector

To reconfigure an OSPF collector:

- 
- Step 1** From the Path Analyzer taskbar, click **Start > Administration > System**.  
The System Administration window appears.
- Step 2** From the configuration tree in the left side of the window, select the OSPF Collector you want to change.
- Step 3** In the **Configuration** tab, click **Reconfigure**.
- Step 4** The Collector Configuration Wizard starts, showing the [Set Basic OSPF Parameters](#), in which you basic settings.  
The rest of the screens in the wizard are the same as those you use for Configuring an OSPF Collector. You can delete the existing values and enter new values where you wish. See [Configuring an OSPF Collector, page 6-25](#).
- 

## Configuring a BGP Collector

In Path Analyzer, you can configure a new BGP Collector, or change the configuration of a selected BGP Collector.

**Note**

If the Router ID changes on a BGP speaker that has an adjacency with a Path Analyzer Listener, reconfigure each Collector to use the new BGP router ID.

## Adding a New BGP Collector

The process of adding a new BGP Collector involves the following procedures:

- [Start System Administration, page 6-35](#)
- [Start the Collector Configuration Wizard, page 6-36](#)
- [Select BGP Collector Protocol, page 6-36](#)
- [Derive or Create a BGP Collector, page 6-37](#)
- [Set Collector ID and Administrative State, page 6-37](#)
- [Set BGP Peer Speaker Parameters, page 6-38](#)
- [Set the BGP Collector Interface, Mask, and Routes, page 6-39](#)
- [Set Multiple Hops and Delays, page 6-40](#)
- [Set Advanced BGP Parameters, page 6-41](#)

## Start System Administration

To start system administration:

- 
- Step 1** Click **Start > Administration > System**.

The System Administration window appears.

- Step 2** Select the Listener you want to add a BGP Collector to from the configuration tree in the left side of the window.
- 

## Start the Collector Configuration Wizard

To start the Collector Configuration wizard:

---

- Step 1** Click **Add Collector** in the Configuration tab.  
The Collector Configuration Wizard starts.
- Step 2** (Optional) Click the **Do not show this screen again** check box, and click **Next**.  
The Select the Collector's Protocol screen appears (see [Figure 6-29](#)).
- 

## Select BGP Collector Protocol

**Figure 6-29** Collector Protocol Screen in Collector Configuration Wizard



To select the BGP Collector protocol in the Collector Configuration wizard:

---

- Step 1** Select **BGP** to create a Collector that passively participates in BGP routing across autonomous systems.
- Step 2** Click **Next**.  
The Derive or Create a BGP Collector screen appears (see [Figure 6-30](#)).
-



## Derive or Create a BGP Collector

**Figure 6-30** *Derive or Create a BGP Collector in Collector Configuration Wizard*



To derive or create a BGP Collector in the Collector Configuration wizard:

- 
- Step 1** Select one of the following options for setting configuration parameters:
- **Yes**—Use the configuration of an existing BGP Collector as a template for creating a new one.  
If you select this option, fields in each of the subsequent Collector Configuration Wizard screens display the values of the previously-configured Collector. You can select and change the values.
  - **No**—Create a new BGP Collector without an existing configuration as a template.
- Step 2** Click **Next**.  
The Set Collector ID and Administrative State screen appears (see [Figure 6-31](#)).
- 

## Set Collector ID and Administrative State

**Figure 6-31** *Collector ID and Administrative State in Collector Configuration Wizard*



To set the Collector ID and administrative state in the Collector Configuration wizard:

- 
- Step 1** Enter a name to uniquely identify the Collector in the Collector ID field.
- Step 2** Select one of the following options in the Admin State field:
- **Up**—Enables the Collector immediately.

- **Down**—Causes the Collector to remain in an inactive state until you are ready to enable it.

**Step 3** Click **Next**.

The Please Fill in this Collector's BGP Peer Speaker Parameters screen appears (see [Figure 6-32](#)).

## Set BGP Peer Speaker Parameters

**Figure 6-32** BGP Peer Speakers Parameters Screen in Collector Configuration Wizard

To set BGP peer speaker parameters in the Collector Configuration wizard:

- Step 1** Enter the identifier of the autonomous system the BGP Collector resides in into the **AS** field.
- Step 2** Enter the IP address of the interface used by the Collector in the IP Address field.
- Step 3** Enter the router ID of the BGP peer adjacent to the BGP Collector in the Router ID field.
- Step 4** Enter the TCP port used by the BGP Collector to obtain routing data from the BGP peer in the BGP Port field. The default port is 179.
- Step 5** Select **Is also OSPF Router** if the BGP peer is configured with an OSPF interface, indicating that it also participates in OSPF routing.
- Step 6** Enter the router ID of the OSPF interface in the OSPF Router ID field.
- Step 7** For BGP Collector instrumentation, all BGP Speakers must be Route Reflector Servers. Only uncheck the **Strip Cluster ID** check box if this peer Speaker was a Route Reflector prior to implementation.
- Step 8** Enter the Strip Cluster ID.
- Step 9** Click **Next**.

The Set the BGP Collector Interface, Mask, and Routes screen appears (see [Figure 6-33](#)).

## Set the BGP Collector Interface, Mask, and Routes

Figure 6-33 BGP Collector Interface, Mask, and Routes Screen in Collector Configuration Wizard



The screenshot shows the 'Collector Configuration Wizard' window. On the left is an icon of stacked blocks and a gear. The main area contains the following fields and options:

- Interface Address:** 192.14.25.2
- Interface Mask:** 255.255.255.0
- Port:** eth0 (dropdown menu)
- Routes:**
  - ☐ BGP IPv4 Unicast Routes
  - ☒ MP-BGP IPv4 Routes
    - ☐ Unicast Routes
    - ☐ Multicast Routes
    - ☐ VPN Routes

At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

To set the BGP Collector interface, mask, and routes in the Collector Configuration wizard:

- 
- Step 1** Enter the IP address of the BGP Collector in the Interface Address field.
- Step 2** Enter the network mask of the BGP Collector in the Interface Mask field.
- Step 3** Select the Listener port on which the BGP Collector resides from the Port field.
- Step 4** Under **Routes**:
- Check **BGP IPv4 Unicast Routes** if this is a regular BGP Speaker
  - Check **MP-BGP IPv4 Routes** if this is a Multi-Protocol BGP Speaker, then select *one or more* route type(s):
    - **Unicast Routes**
    - **Multicast Routes**
    - **VPN Routes**
- Step 5** Click **Next**.

The Set Multiple Hops and Delays screen appears (see [Figure 6-34](#)).

---

## Set Multiple Hops and Delays

**Figure 6-34** Multi-Hop Option and Delays Screen in Collector Configuration Wizard

To set multiple hops and delays in the Collector Configuration wizard:

- 
- Step 1** In the **Multi-Hop** field:
- a. Select **Yes** to indicate that the BGP peer is more than one hop away from the Listener.
  - b. Enter the IP address of the next hop in the Next Hop field.
- or*
- a. Select **No** to indicate that the BGP peer and Listener are connected to the same network.
- Step 2** Enter the maximum number of seconds that must elapse before the BGP Collector tries to connect to its BGP peer in the Start Delay field.
- If the BGP peer does not respond, the BGP Collector sends another message within the number of seconds specified by the Start Delay interval. The default value is 60 seconds.
- Step 3** Enter the maximum number of seconds that must elapse after a BGP Collector's second attempt at forming an adjacency with a BGP peer fails to receive a response in the Retry Delay field.
- If the BGP peer does not respond, the BGP Collector sends another message within the allotted number of seconds that you specified in the Retry Delay interval. The default value is 60 seconds.
- Step 4** Enter the maximum number of seconds that must elapse before the BGP Collector establishes the availability of its BGP peer in the Hold Delay field. The default value is 90 seconds.
- Step 5** Enter the number of seconds that must elapse before the BGP Collector sends a Keep Alive packet to the BGP peer to establish and maintain its connection to the peer in the Keepalive Timer field.
- Step 6** Enter the number of seconds that must elapse before the BGP Collector establishes the integrity of the connection to the BGP peer in the Adjacency Delay field. This setting informs the BGP peer of the availability of the Collector, which informs the peer that it can send packets to the Collector.
- Step 7** Click **Next**.

The Set Advanced BGP Parameters screen appears (see [Figure 6-35](#)).

---

## Set Advanced BGP Parameters

Figure 6-35 Advanced Parameters Screen in Collector Configuration Wizard



To set advanced BGP parameters in the Collector Configuration wizard:

- 
- Step 1** Enter the number of milliseconds that must elapse before the Path Analyzer Server polls each configured BGP Collector in the Poll Period (msecs) field.
- The default polling period is 10,000 milliseconds (10 seconds).
- Step 2** Enter the multiplier required to determine the number of milliseconds that must elapse before using a failover Collector in the Switch-Over Ticks field.
- The Path Analyzer Server sends poll packets to each Collector to determine its availability.
- Setting the Polling Period to 10,000 milliseconds (10 seconds) and the Switch-Over Ticks period to 60,000 milliseconds (60 seconds) causes the Path Analyzer Server to switch to another Collector in the same area if the Collector fails to respond after 60 seconds.
  - The failover time is equivalent to the Switch-Over Ticks multiplier (6) times the Polling Period (10,000 milliseconds), which equals 60,000 milliseconds (60 seconds). You can select another Switch-Over Tick value.
- Step 3** Under **Authentication**, select either:
- **None**, or
  - **MD5**
- If you selected MD5 in Step 3, enter the **MD5 Key**.
- Step 4** Click **Next**.
- Step 5** Click **Finish** to complete the wizard.
- 

## Reconfiguring a BGP Collector

To reconfigure a BGP Collector:

- 
- Step 1** Click **Start > Administration > System**. The System Administration window appears.
- Step 2** Select the BGP Collector you want to change from the configuration tree in the left side of the window.

- Step 3** Click **Reconfigure** in the Configuration tab.
- Step 4** The Collector Configuration Wizard starts, showing the [Set Collector ID and Administrative State, page 6-37](#) screen.
- The rest of the screens in the wizard are the same as those you use for [Configuring a BGP Collector, page 6-35](#).
- You can delete the existing values and enter new values where you wish.
- See [Configuring a BGP Collector, page 6-35](#).
- 

## Viewing Appliance and Collector Configurations

The Configuration tab shows configured settings for a Path Analyzer Server, Listener, OSPF Collector, or BGP Collector, depending on your selection from the system hierarchy in the System Administration window.

To view appliance and Collector configurations:

- 
- Step 1** Click **Start > Administration > System**. The System Administration window appears.
- Step 2** Select one of the following from the system hierarchy at the left of the window:
- Path Analyzer Server
  - Listener—Expand the Path Analyzer Server to display it.
  - OSPF Collector—Expand a Listener to display it.
  - BGP Collector—Expand a Listener to display it.
- Step 3** Click the **Configuration** tab.
- 

## Viewing Status and Statistics

You can view the status of your Path Analyzer system for information about the system components and active connections in your Path Analyzer system.

### View the Configuration Status of your System

To view the configuration status of your system, click **Start > Administration > System**. The System Administration window appears.

The configuration tree in the left side of the window shows connected and available appliances.

- A blue IP address indicates that the appliance is available on the network.
- A red IP address indicates that the appliance is unavailable, unreachable, or disconnected.

## View Path Analyzer Server Statistics

To view Path Analyzer server statistics:

- 
- Step 1** Click **Start > Administration > System**. The System Administration window appears.
- Step 2** Select one of the following from the configuration tree in the left side of the window:
- Path Analyzer Server
  - Listener—Expand the Path Analyzer Server to display it.
  - OSPF Collector—Expand a Listener to display it.
  - BGP Collector—Expand a Listener to display it.
- Step 3** Click the **Statistics** tab.
- Step 4** Click **Refresh**.
- For a Path Analyzer Server or Listener, the Platform Status portion of the tab shows the administrative state of the selected appliance.
  - The Platform Statistics section of the tab shows information about processes running on the appliance.
  - For an OSPF or a BGP Collector, the Collector Status portion of the tab shows the status of the connection for the selected Collector.
- 

## Statistics Tab

From the Statistics tab of the System Administration window, you can view the administrative status and statistics of a selected Path Analyzer Server, Listener, OSPF Collector, or BGP Collector.

This tab provides a comprehensive set of statistics including the type of output you would generally receive by manually entering the following commands in the Unix environments:

- top
- df

The Statistics tab lets you view the status of a Path Analyzer appliance or the status of an adjacency between an OSPF or BGP Collector and its peer router.

See [Viewing Status and Statistics](#), page 6-42.

Fields of the Statistics tab vary, depending on your selection from the hierarchy on the left side of the System Administration window.

For information about each variation of the Statistics tab, see the following tables:

- [Statistics Tab of a Path Analyzer Server](#), page 6-43
- [Statistics Tab of a Listener](#), page 6-45
- [Statistics Tab of an OSPF Collector](#), page 6-47
- [Statistics Tab of a BGP Collector](#), page 6-48

## Statistics Tab of a Path Analyzer Server

[Table 6-5](#) describes the fields and buttons of the Statistics tab of the Path Analyzer Server.

**Table 6-5 Statistics Tab (Path Analyzer Server)**

Field or Button	Description
Path Analyzer Server Status	Shows the active status of the Path Analyzer Server on the network. <ul style="list-style-type: none"> <li>• <b>Up</b>—Path Analyzer Server is enabled, processes data received from Listeners and provides a view of network activity to the Path Analyzer Management Console.</li> <li>• <b>Down</b>—Path Analyzer Server is disabled.</li> </ul>
Path Analyzer Server Statistics	Shows information about processes, disk space, and CPU usage on the Path Analyzer Server.
Refresh	Updates statistics displayed in the Platform Statistics field.
The following statistics are displayed in the Platform Statistics field after clicking <b>Refresh</b> .	
Date	Shows the current date and time in the following format: MM/DD/YYYY HH:MM:SS Example: 03/16/2004 13:58:49
Uptime	Shows the duration of time that the Path Analyzer Server has been enabled and available on the network.
Load average	Shows the average system load.
Tasks	Shows the total number of tasks running on the Path Analyzer Server followed by a breakdown of the types of processes: <ul style="list-style-type: none"> <li>• running</li> <li>• sleeping</li> <li>• stopped</li> <li>• zombie</li> </ul>
CPU(s)	Shows the percentage of CPU actively used and by which processes: <ul style="list-style-type: none"> <li>• % user</li> <li>• % system</li> <li>• % nice</li> <li>• % idle</li> <li>• % waits</li> <li>• % hardware irq</li> <li>• % software interrupts</li> </ul>



**Table 6-5**      **Statistics Tab (Path Analyzer Server) (continued)**

Field or Button	Description
Memory	Shows the amount, in kilobytes, of allocated memory: <ul style="list-style-type: none"> <li>total</li> <li>used</li> <li>free</li> <li>buffers</li> </ul>
Swap	Shows the amount, in kilobytes, of allocated swap space: <ul style="list-style-type: none"> <li>total</li> <li>used</li> <li>free</li> <li>cached</li> </ul>
Process details	Shows the following details about running processes: <ul style="list-style-type: none"> <li>Process identifier (PID)</li> <li>User</li> <li>PRI</li> <li>NI</li> <li>VIRT</li> <li>RES</li> <li>Share</li> <li>Stat</li> <li>%CPU (used)</li> <li>% Memory (used)</li> <li>Time (running)</li> <li>Command (that started the process)</li> </ul>
Disk space	Shows the total and free disk space for each partitioned drive on the appliance.

## Statistics Tab of a Listener

[Table 6-6](#) describes the fields and buttons of the Statistics tab of the Listener.

**Table 6-6 Statistics Tab (Listener)**

Field or Button	Description
Platform Status	Shows the active status of the Listener on the network. Options include: <ul style="list-style-type: none"> <li>• <b>Up</b>—Listener is enabled, processes data received from Listeners, and provides a view of network activity to the Path Analyzer Management Console.</li> <li>• <b>Down</b>—Listener is not connected to the Path Analyzer Server.</li> </ul>
Platform Statistics	Shows information about processes, disk space, and CPU usage on the Listener.
Refresh	Updates statistics displayed in the Platform Statistics field.
The following statistics are displayed in the Platform Statistics field after clicking <b>Refresh</b> .	
Date	Shows the current date and time in the following format: MM/DD/YYYY HH:MM:SS Example: 03/16/2004 13:58:49
Uptime	Shows the duration of time that the Listener has been enabled and available on the network.
Load average	Shows the average system load.
Tasks	Shows the total number of processes running on the Listener followed by a breakdown of the types of processes: <ul style="list-style-type: none"> <li>• running</li> <li>• sleeping</li> <li>• stopped</li> <li>• zombie</li> </ul>
CPU	Shows the percentage of CPU actively used and by which processes: <ul style="list-style-type: none"> <li>• % user</li> <li>• % system</li> <li>• % nice</li> <li>• % idle</li> <li>• % waits</li> <li>• % hardware irq</li> <li>• % software interrupts</li> </ul>

**Table 6-6**      **Statistics Tab (Listener) (continued)**

Field or Button	Description
Memory	Shows the amount, in kilobytes, of allocated memory: <ul style="list-style-type: none"> <li>• total</li> <li>• used</li> <li>• free</li> <li>• buffers</li> </ul>
Swap	Shows the amount, in kilobytes, of allocated swap space: <ul style="list-style-type: none"> <li>• total</li> <li>• used</li> <li>• free</li> <li>• cached</li> </ul>
Process details	Shows the following details about running processes: <ul style="list-style-type: none"> <li>• Process identifier (PID)</li> <li>• User</li> <li>• PRI</li> <li>• NI</li> <li>• VIRT</li> <li>• RES</li> <li>• Share</li> <li>• Stat</li> <li>• %CPU (used)</li> <li>• % Memory (used)</li> <li>• Time (running)</li> <li>• Command (that started the process)</li> </ul>
Disk space	Shows the total and free disk space for each partitioned drive on the appliance.

## Statistics Tab of an OSPF Collector

[Table 6-7](#) describes the fields and buttons of the Statistics tab of the OSPF Collector.

**Table 6-7 Statistics Tab (OSPF Collector)**

Field or Button	Description
Collector Status	<p>Shows the connectivity and status of the adjacency between the OSPF Collector and its peer router.</p> <ul style="list-style-type: none"> <li>• <b>Active (Fully Adjacent)</b>—Adjacency between OSPF Collector and its peer router is active. OSPF Listener is actively collecting routing data from its peer and sending the data to the Path Analyzer Server.</li> <li>• <b>Backup (Fully Adjacent)</b>—Adjacency between the backup OSPF Collector and the configured peer router is active. This state indicates that the backup OSPF Collector has taken over collection responsibilities of the primary OSPF Collector, which has become unavailable or unreachable.</li> <li>• <b>Inactive</b>—Adjacency between OSPF Collector and its peer router is inactive.</li> <li>• <b>Disconnected</b>—The peer router has become disconnected from the OSPF Collector.</li> <li>• <b>Not Adjacent</b>—Adjacency between the OSPF Collector and the peer router has been lost.</li> <li>• <b>Unknown</b>—State of the adjacency between the OSPF Collector and the peer router is unknown, indicating that a hardware issue or software misconfiguration has caused interrupted the connection.</li> </ul>
Collector Statistics	Shows information about the database size, Link State Advertisements (LSAs) received, and priorities.
Refresh	Updates statistics displayed in the Collector Statistics field.
The following statistics are displayed in the Collector Statistics field after clicking <b>Refresh</b> .	
Database Size	Shows the number of LSAs collected at the time of refresh.
LSA types	Shows the number of LSAs received of each LSA type.
Priority	Shows the number of bytes of normal priority and high priority data moving into, out of, or pending within a mailbox, which acts as a holding place used to pass information from one process to another.
Max Flow Control	Shows the maximum amount of time (in msec) spent queuing LSAs.

## Statistics Tab of a BGP Collector

Table 6-8 describes the fields and buttons of the Statistics tab of the BGP Collector.

**Table 6-8 Statistics Tab (BGP Collector)**

Field or Button	Description
Collector Status	Shows the connectivity and status of the adjacency between the BGP Collector and its peer router. Options include: <ul style="list-style-type: none"> <li><b>Active (Fully Adjacent)</b>—Adjacency between BGP Collector and its peer router is active. BGP Listener actively collects routing data from its peer and sends the data to the Path Analyzer Server.</li> <li><b>Inactive</b>—Adjacency between BGP Collector and its peer router is inactive.</li> </ul>
Collector Statistics	Shows information derived from the BGP Router Information Base (RIB) of the BGP peer.
Refresh	Updates statistics displayed in the Collector Statistics field.
The following statistics are displayed in the Collector Statistics field after clicking <b>Refresh</b> .	
Prefix Tree	Shows the number of routes and path attributes received on the Collector at the time of refresh.
Priority	Shows the number of bytes of normal priority and high priority data moving into, out of, or pending within a mailbox, which acts as a holding place used to pass information from one process to another.
Max Flow Control	Shows the maximum amount of time (in msec) spent queuing BGP routes.

## Removing Path Analyzer Components

You can remove components from your Path Analyzer system, including Collectors, Listeners, and the Management Console.

### Removing or Uninstalling Physical Components of Your System

Path Analyzer System Administration enables you to prepare the Management Console clients and configuration files for removing hardware components before physically removing them from your system. Changes are made automatically and transparently without requiring manual configuration.

#### Component Removal Tasks

- [Removing a Collector, page 6-50](#)
- [Removing a Listener, page 6-50](#)
- [Uninstalling the Management Console \(Windows Users\), page 6-50](#)
- [Uninstalling the Management Console \(Unix-Bases System Users\), page 6-51](#)


**Note**

Remove all Collectors from the Listener before removing the Listener from your system.

## Removing a Collector

To remove a Collector:

- 
- Step 1** Click **Start > Administration > System**.  
The System Administration window appears.
  - Step 2** Select the Collector you want to remove from the configuration tree at the left side of the window.
  - Step 3** Select the **Configuration** tab in the right side of the window.
  - Step 4** Click **Remove**.
  - Step 5** Click **Yes** in the confirmation box.  
The Collector is removed from your system.
- 

## Removing a Listener

To remove a listener:

- 
- Step 1** Click **Start > Administration > System**.  
The System Administration window appears.
  - Step 2** Select the Listener you want to remove from the configuration tree at the left side of the window.
  - Step 3** Select the **Configuration** tab in the right side of the window.
  - Step 4** Click **Remove**.
  - Step 5** Click **Yes** in the confirmation box.  
The Listener is removed from your system.
- 

## Uninstalling the Management Console (Windows Users)

When you want to upgrade your Path Analyzer installation, you should first uninstall your current Path Analyzer software.

- 
- Step 1** Locate the location you selected during installation for the Path Analyzer icons, then double-click the **Uninstall Path Analyzer** icon.  
*or*  
In Microsoft Windows:  
    - a. From the Windows Control Panel, double-click **Add or Remove Programs**.

- b. In the Add or Remove Programs dialog box, select Path Analyzer.
- c. Click **Change/Remove**.

The Path Analyzer uninstallation wizard Uninstall screen appears.



**Note** If you decide to keep your installed version of Path Analyzer during this part of the uninstallation process, click **Cancel**, then click **Quit** to stop the uninstallation.

- Step 2** In the Uninstall page of the uninstall wizard, click **Uninstall**.



**Note** Once you click **Uninstall**, you cannot stop the uninstallation process.



**Warning**

The uninstallation wizard displays an “Uninstalling” message as it removes **Files, Shortcuts, LaunchAnywhere, and Folders**. On Windows, the “Uninstalling” message also notifies you when it removes Registry components. When all Path Analyzer software components have been successfully uninstalled, the message “Uninstall Complete” is displayed.

- Step 3** Click **Done**.

The Path Analyzer uninstallation wizard closes.

## Uninstalling the Management Console (Unix-Bases System Users)

There is no automatic procedure for uninstalling the supported Unix-based Operating System version of the Management Console. You must manually delete the folders from the file structure.







## CHAPTER 7

# Setting Up and Maintaining User Accounts

---

## Managing Accounts of Path Analyzer Users

As a Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) Administrator, your management responsibilities enable you to control the number and types of Path Analyzer users you create.

To obtain information about the types of Path Analyzer user accounts you can create, see [Path Analyzer Users, page 7-1](#).

## User Account Set Up and Maintenance Tasks

- [Viewing User Details, page 7-2](#)
- [Adding a New User Account, page 7-3](#)
- [Changing Details of a User Account, page 7-5](#)
- [Removing a User Account, page 7-6](#)
- [TACACS+ Authentication, page 7-6](#)

## Path Analyzer Users

Path Analyzer recognizes the following types of users:

- Administrator User
- Power User
- Limited User



### Note

At least one Administrator User is required for each Path Analyzer system. Additional Administrator User accounts can be created and removed as long as one is always active and available.

---

## Administrator User Privileges

The Administrator User has the most privileges within Path Analyzer. As an Administrator User, you can complete the following tasks in addition to all [Power User Privileges, page 7-2](#):

- Add, remove, view, or reset other user accounts and passwords.
- Add, remove, or update Path Analyzer hardware and software components, including Listeners and Collectors.
- Perform all configuration, maintenance, and troubleshooting tasks, including:
  - Exporting the Path Analyzer database
  - Exporting logs
  - Upgrading software versions
  - Maintaining customer support accounts
  - Adding and removing Path Analyzer appliances
- Use all Path Analyzer modules to complete network administration and management tasks.

## Power User Privileges

Power Users can monitor and administer the network using:

- topological views
- Event Logs
- querying capabilities
- alarms
- historical sessions
- reporting

Power Users have read and write privileges for all Path Analyzer modules.

## Limited User Privileges

Limited Users generally complete research and reporting tasks, gathering information about network changes to assist Power Users.

Limited Users have read permissions for real-time viewing of all Path Analyzer modules but cannot access Chart Manager, Report Manager, or Historical Sessions.

## Viewing User Details

From the User Administration window, you can view the total number of users, the number of users logged into the Path Analyzer Server, and details about a specific user account.

### View the Total Number of Users

To view the total number of Path Analyzer users:

---

**Step 1** Click **Start > Administration > User**.

The User Administration window appears.

- Step 2** See the **Total Users** field for the total number of configured user accounts.
- 

## View the Number of Authenticated Users

To view the number of authenticated Path Analyzer users:

- Step 1** Click **Start > Administration > User**.  
The User Administration window appears.
- Step 2** See the **Logged In** field for the total number of configured user accounts.
- 

## View Details of a User Account

To view the details of a Path Analyzer user account:

- Step 1** Click **Start > Administration > User**.  
The User Administration window appears.
- Step 2** Select a user account name from the Path Analyzer Server field.  
Details of the user account including user name, type state, authentication, and user contact information are displayed to the right of the Path Analyzer Server field.
- 

## Adding a New User Account

From the User Administration window, you can run the User Configuration Wizard and create new user accounts. For information about the types of users that Path Analyzer supports, see [Path Analyzer Users, page 7-1](#).

To add a new user account:

- Step 1** Click **Start > Administration > User**.  
The User Administration window appears.
- Step 2** Click **Add User**.  
The User Configuration Wizard appears (see [Figure 7-1](#)).
- Step 3** (Optional) Click the **Do not show this screen again** check box, and click **Next**.  
The User Information screen appears.
- Step 4** Enter a user name for the new account in the Username field.

**Figure 7-1** *User Configuration Wizard*

**Step 5** Select the type of user to create from the Type drop-down box:

- **admin**
- **power**
- **limited**

For a description of each type of user, see [Path Analyzer Users, page 7-1](#).

**Step 6** Select the state of the user account from the State drop-down box:

- **Up**—Grants the user the privilege to log into the system. For the Administrator User, an Admin State of **Up** grants the user full administrative privileges.
- **Down**—Delays user log-in privileges until you decide to grant them. You can also revoke privileges for a configured user by selecting **Down** from the State field.

For information about giving privileges to an Administrator User at a later date, see [Changing Details of a User Account, page 7-5](#).

**Step 7** The Authentication Type field drop-down box defaults to Cisco Path Analyzer Server.

**Step 8** Set a password for the user account.

- a. In the Password field, enter the password for the new account.
- b. In the Confirm field, re-enter the password.

**Step 9** Enter the user's contact information:

- a. In the Email field, enter the email address of the user.
- b. In the Phone field, enter the cell phone or pager number of the user.

**Step 10** Click **Next**.

User account information is submitted to the Path Analyzer Server. A message is displayed to indicate that the user account has been created successfully.

**Step 11** Click **Finish**.

The User Configuration wizard closes. The User Administration window shows the number of configured users and the number of users who have logged into the Path Analyzer Management Console.

# Changing Details of a User Account

From the Administration module, you can change details of a user account, including the password, type of account, and contact information. For information about the types of users that Path Analyzer supports, see [Path Analyzer Users, page 7-1](#).

To change a user's details:

- 
- Step 1** Click **Start > Administration > User**.
- The User Administration window appears.
- Step 2** Select a user account from the **Path Analyzer Server** field.
- Details of the user account, including user name, type status, and user contact information are displayed to the right of the Path Analyzer Server field.
- Step 3** Click **Reconfigure**.
- The User Configuration Wizard appears, in which you can change user information.
- Step 4** To change the type of user:
- From the Type drop-down box, select the new type to assign to the user account:
- **admin**
  - **power**
  - **limited**
- For a description of each type of user, see [Path Analyzer Users, page 7-1](#).
- Step 5** To change the status of the user account:
- From the State drop-down box, select one of the following options:
- **Up**—Grants the ability to log in to a user.
  - **Down**—Revokes the ability to log in.
- Step 6** To change the password of the user account:
- a. In the Password field, enter the new password.
  - b. In the Confirm Password field, re-enter the password.
- Step 7** To change user contact information:
- a. In the Email field, enter a new email address.
  - b. In the Phone field, enter a new phone number.
- Step 8** Click **Next**.
- User account information is submitted to the Path Analyzer Server. A message is displayed to indicate that the user account has been successfully created.
- Step 9** Click **Finish**.
- The User Configuration wizard closes. The User Administration window shows the number of configured users and the number of users who have logged into the Path Analyzer Management Console.
-

## Removing a User Account

You can also remove inactive user accounts for the Administration module. For example, if employees leave your organization and their user accounts are no longer required.

To remove a user's account:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Click <b>Start &gt; Administration &gt; User</b> .<br>The User Administration window appears.  |
| <b>Step 2</b> | Select a user account from the <b>Path Analyzer Server</b> field.<br>Details of the user account, including user name, type status, and user contact information are displayed to the right of the Path Analyzer Server field. |
| <b>Step 3</b> | Click <b>Remove</b> .  |
| <b>Step 4</b> | Click <b>Yes</b> in the confirmation box to remove the account.  |
- 

## TACACS+ Authentication

Users can be authenticated for Path Analyzer using TACACS+ servers. A maximum of two TACACS+ servers are allowed, primary and secondary. The primary TACACS+ server must be configured before the secondary server can be configured.

The authentication hierarchy is as follows:

1. The Path Analyzer server checks to see if RADIUS authentication is enabled. If RADIUS authentication is enabled, it tries to authenticate the user with the RADIUS Server. If the primary RADIUS server connection times out, the Path Analyzer Server tries to authenticate through the secondary RADIUS server, if a second one exists. If this second authentication attempt fails, an authentication failure notification is displayed.
2. If the RADIUS authentication is disabled, or both primary and secondary RADIUS servers are unreachable, the Path Analyzer Server checks to see if there are any TACACS+ servers configured. If a primary TACACS+ server is configured, the Path Analyzer server tries to authenticate through the primary TACACS+ server. If the primary TACACS+ connection fails, the user is authenticated through a secondary TACACS+ server, if a second one is configured, and returns an authentication failure notification if the authentication fails.

To ensure that users are authenticated only through a TACACS+ server, the administrator should disable RADIUS server authentication.

3. In cases where both the RADIUS servers and TACACS+ servers are unreachable, the user will be authenticated through the Path Analyzer server.

Path Analyzer user accounts are added to the TACACS+ server by its administrator. You must then add the server to Path Analyzer.

The following tasks are discussed in this section:

- [Add a Primary TACACS+ Server, page 7-7](#)
- [Change a Primary TACACS+ Server, page 7-8](#)
- [Disable a Primary TACACS+ Server, page 7-8](#)

- [Enable a Primary TACACS+ Server, page 7-8](#)
- [Secondary TACACS+ Server Tasks, page 7-9](#)

## Add a Primary TACACS+ Server

TACACS+ servers are configured in the User Administration module of Path Analyzer.

To add a primary TACACS+ server:

- 
- Step 1** Navigate to **Start > Administration > User**.
- Step 2** Make sure that the top level of the server tree on the left side of the screen is selected.
- Step 3** Click the **Primary TACACS+** tab.
- Step 4** Click the **Reconfigure** button.
- The TACACS+ Configuration wizard appears.
- Step 5** Click **Next**.
- The TACACS+ Server fields screen appears.
- Step 6** Check the **Enabled** check box if you want the TACACS+ server to be enabled upon completion of the wizard.
- Step 7** Enter the TACACS+ server's address in the Host field.
- Step 8** Enter the TACACS+ server's port number in the Port field.
- Step 9** Enter the number of seconds before authentication times out in the Timeout field.
- Step 10** Enter the server's key in the Key field. This will be provided by your System Administrator.
- Step 11** Click **Next**.
- A confirmation message is displayed.
- Step 12** Click **Finish**.

**Figure 7-2** TACACS+ Server Configuration Wizard



## Change a Primary TACACS+ Server

To change a primary TACACS+ server's configuration:

- 
- Step 1** Navigate to **Start > Administration > User**.
  - Step 2** Make sure that the top level of the server tree on the left side of the screen is selected.
  - Step 3** Click the **Primary TACACS+** tab.
  - Step 4** Click the **Reconfigure** button.  
The TACACS+ Configuration wizard appears.
  - Step 5** Follow the steps detailed in [Add a Primary TACACS+ Server, page 7-7](#), and make any necessary changes to the server configuration.
- 

## Disable a Primary TACACS+ Server

To disable a primary TACACS+ Server:

- 
- Step 1** Navigate to **Start > Administration > User**.
  - Step 2** Make sure that the top level of the server tree on the left side of the screen is selected.
  - Step 3** Click the **Primary TACACS+** tab.
  - Step 4** Click the **Reconfigure** button.  
The TACACS+ Configuration wizard appears.
  - Step 5** Uncheck the **Enable** check box.
  - Step 6** Click **Next**.
  - Step 7** Click **Finish**.
- 

## Enable a Primary TACACS+ Server

To enable a disabled primary TACACS+ Server:

- 
- Step 1** Navigate to **Start > Administration > User**.
  - Step 2** Make sure that the top level of the server tree on the left side of the screen is selected.
  - Step 3** Click the **Primary TACACS+** tab.
  - Step 4** Click the **Reconfigure** button.  
The TACACS+ Configuration wizard appears.
  - Step 5** Select the **Enable** check box.
  - Step 6** Click **Next**.



**Step 7** Click **Finish**.

---

## Secondary TACACS+ Server Tasks

Secondary TACACS+ servers are configured using the same procedures as primary TACACS+ servers. The only difference is that the procedures are initiated from the Secondary TACACS+ tab instead of the Primary TACACS+ tab.



**Note**

A primary TACACS+ server must be configured and enabled before a secondary TACACS+ server can be configured.

---

For details on each procedure, see the following sections:

- [Add a Primary TACACS+ Server, page 7-7](#)
- [Change a Primary TACACS+ Server, page 7-8](#)
- [Disable a Primary TACACS+ Server, page 7-8](#)
- [Enable a Primary TACACS+ Server, page 7-8](#)





## CHAPTER 8

# Exporting Alarm Triggers

---

## Viewing Path Analyzer Events that Trigger Alarms in your Network Management System (NMS)

You can use the OSPF, BGP, or Service Alarm Monitor to set alarms on entities, such as routers, interfaces, routes, router advertisements, and services, so you receive notifications when these entities change in your network. When changes occur on your network and trigger an alarm, you receive a notification and a set of generated triggers describing the changes that occurred. All triggers are displayed in the Alarm Trigger Log.

For information about setting alarms in Alarm Monitor and viewing triggers in the Alarm Trigger Log, see Chapter 8, Setting and Monitoring Alarms, in the *Cisco Service Path Analyzer User Guide*.

After setting alarms and analyzing their triggers, you can export the triggers to a syslog host or a Simple Network Management Protocol (SNMP) agent so that you can view them in your network management system.

The Alarm Export Administration module provides the Alarm Export Wizard to guide you through the process of configuring the export of alarm triggers.

The following sections explain how to run the wizard and configure your Cisco Service Path Analyzer (herein referred to as the Path Analyzer) system to export alarm triggers to a selected host.

## Path Analyzer Alarm Integration Tasks

- [Integrating Path Analyzer Alarm Triggers into Your NMS, page 8-2](#)
- [Configuring the Export of Alarm Triggers to a Syslog Host, page 8-2](#)
- [Configuring the Export of Alarm Triggers to an SNMP Agent, page 8-5](#)

## Path Analyzer Alarm Maintenance Tasks

- [Reconfiguring a Syslog or SNMP Alarm Destination, page 8-7](#)
- [Removing an Existing Syslog or SNMP Alarm Destination, page 8-7](#)
- [Configuring the Export of Alarm Triggers to a Syslog Host, page 8-2](#)

## Integrating Path Analyzer Alarm Triggers into Your NMS

You can view the events that trigger Path Analyzer alarms in your local NMS by:

- Applying a severity to each alarm you create in the OSPF, BGP, or Service Alarm Monitor. See Severity Values of Alarms in Chapter 8 of the *Cisco Service Path Analyzer User Guide* for information.
- Specifying a severity threshold for alarm triggers to be exported.
- Setting parameters for a syslog host or SNMP agent to receive the alarm triggers.

**Note**

The severity level you assign to an alarm is subjective and depends on your estimation of the significance of the events that trigger the alarm.

## Configuring the Export of Alarm Triggers to a Syslog Host

The syslog logging system centralizes the management of log files from distributed network locations to a central log server. Syslog sorts messages by their level of severity and routes them to various destinations on a host, including log files, centralized servers, or user computers.

## Syslog Priority Levels Compared to Alarm Monitor Severities

Table 8-1 shows how Path Analyzer maps alarm severities to syslog priorities.

**Table 8-1** Path Analyzer Alarm Severities and Syslog Priorities

Alarm Monitor Severity Levels	Syslog Priority Levels	Significance
Critical	critical	Critical condition that severely impacts your network, resulting in downtime, network unavailability; substantial impact to customers and business at significant cost, including time and cost to repair.
High	error	Condition that affects an important path, router, route, or interface, impacting high-volume traffic flow to key areas of the network.
Medium	warning	Condition that acutely degrades network performance, leading to eventual downtime and unavailability.
Low	notice	Unusual events that have the potential to negatively affect network performance and availability and which require further investigation.

## Export to Syslog Destinations

Path Analyzer exports alarm triggers in the form of syslog messages, and tags each message with one of the following syslog facilities:

- LOG\_USER—To a user-related process.
- LOG\_LOCAL0 through LOG\_LOCAL7—To local messages.

### Export Alarm Triggers to Syslog

To export alarm triggers to the syslog:

- 
- Step 1** Click **Start > Administration > Alarm Export**.
- The Alarm Export Administration module appears.
- Step 2** From the configuration tree at the left of the Alarm Export Administration window, select the Path Analyzer Server that generated the alarm triggers you want to export.
- Step 3** Click **Add Destination** in the Export Destinations for Path Analyzer Server field. The Alarm Export Wizard appears.
- Step 4** (Optional) Click the **Do not show this screen again** check box.
- Step 5** Click **Next**. The Select Destination Type wizard page appears.
- Step 6** In the **Select destination type** field, select **Syslog**.
- Step 7** Click **Next**. The Configure Syslog Destination wizard screen appears (see [Figure 8-1](#)).

**Figure 8-1** Configure Syslog Destination Screen in Alarm Export Wizard



- Step 8** Configure the Syslog Destination:
- a. Enter a name for the syslog destination in the Name field.
  - b. Select a severity threshold in the Threshold drop-down box:
    - **Critical**—Exports only Critical alarm triggers.
    - **High**—Exports only High and Critical alarm triggers.
    - **Medium**—Exports alarm triggers that have Medium, High, or Critical severity.
    - **Low**—Exports all alarm triggers.

- c. Enter the IP address or host name of the destination syslog host in the Host field.
- d. Enter the port number of the syslog daemon on the syslog host in the Port field. The default syslog port is **514**.
- e. Select a syslog facility for exported syslog messages in the Facility scrolling list:
  - LOG\_USER—To a user-related process.
  - LOG\_LOCAL0 through LOG\_LOCAL7—To local messages.
- f. Select **Enabled** to export the alarm triggers to the syslog host. A check mark is displayed in the Enabled check box when the option is selected.

**Step 9** Click **Next**. The Select Domains to Export wizard screen appears (see [Figure 8-2](#)).

**Figure 8-2** Select Domains to Export Screen in Alarm Export Wizard



**Step 10** In the My Enterprise field, select one or more autonomous systems that generate alarm triggers to export. You can also select one or more routing domains within each autonomous system.

**Step 11** Click **Next**.

**Step 12** Click **Finish**.

Path Analyzer is enabled to export alarm triggers to the selected syslog host.

## For More Information about Syslog

For detailed information about the syslog daemon and its message format, see the syslog man pages and the syslog Request for Comments (RFC):

### On supported Unix-based systems:

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

### From the IETF:

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

# Configuring the Export of Alarm Triggers to an SNMP Agent

You can export alarm triggers to your network management system (NMS) as SNMP v1 or v2c traps. If your NMS runs SNMP v. 3, export alarms using the SNMP v2c option.

## Export Alarm Triggers to an SNMP Agent

To export alarm triggers to an SNMP agent:

- 
- Step 1** Click **Start > Administration > Alarm Export**.  
The Alarm Export Administration module appears.
- Step 2** Select the Path Analyzer Server that generated the alarm triggers you want to export from the configuration tree at the left of the Alarm Export Administration window.
- Step 3** Click **Add Destination** in the Export Destinations for Path Analyzer Server field.  
The Alarm Export Wizard appears.
- Step 4** (Optional) Click the **Do not show this screen again** check box.
- Step 5** Click **Next**. The Select Destination Type wizard screen appears.
- Step 6** Select **SNMP** in the Select destination type field.
- Step 7** Click **Next**.  
The Configure SNMP Destination wizard screen appears (see [Figure 8-3](#)).

**Figure 8-3** *Configure SNMP Destination Screen in Alarm Export Wizard*



- Step 8** Configure the SNMP Destination:
- Enter a name for the SNMP destination host in the Name field.
  - Select an alarm severity threshold in the Threshold field:
    - Critical**—Exports only Critical alarm triggers.
    - High**—Exports only High and Critical alarm triggers.
    - Medium**—Exports alarm triggers that have Medium, High, or Critical severity.
    - Low**—Exports all alarm triggers to a specified SNMP agent.

- c. Enter the SNMP community in the Community field. The default SNMP community is **public**.
- d. Enter the IP address or hostname of the destination SNMP agent in the Host field.
- e. Enter the port number used by the SNMP agent in the Port field. The default SNMP port is **162**.
- f. Select the version of SNMP you are running on the agent in the Version field:
  - Select **1** if your system runs SNMP version 1.
  - Select **2c** if your system runs SNMP version 2c.
- g. Select **Enabled** to enable the export of alarm triggers to the SNMP agent. A check mark is displayed in the Enabled check box when the option is selected.

**Step 9** Click **Next**. The Select Domains to Export wizard screen appears (see [Figure 8-4](#)).

**Figure 8-4** Select Domains to Export Screen in Alarm Export Wizard



**Step 10** In the My Enterprise field, select one or more autonomous systems that generate alarm triggers to export. You can also select one or more routing domains within each autonomous system.

**Step 11** Click **Next**.

**Step 12** Click **Finish**.

Path Analyzer is enabled to export alarm triggers to the selected SNMP agent.

## For more information about SNMP

For detailed information about the Simple Network Management Protocol (SNMP) see:

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



## Reconfiguring a Syslog or SNMP Alarm Destination

Once you have created a Syslog or SNMP Alarm Destination, you can make changes to it at any time using the **Reconfiguration** button.

To reconfigure a syslog or SNMP alarm destination:

- 
- Step 1** Click **Start > Administration > Alarm Export**.  
The Alarm Export Administration module appears.
- Step 2** From the configuration tree at the left of the Alarm Export Administration window, select the Syslog or SNMP Alarm Destination you wish to reconfigure.
- 

## Reconfigure an Existing Alarm Destination

To reconfigure an existing alarm destination:

- 
- Step 1** Click **Reconfigure** in the Export Destinations for Path Analyzer Server field.  
The Alarm Export Wizard appears.
- Step 2** The rest of the screens in the wizard are the same as those you use for:
- [Configuring the Export of Alarm Triggers to a Syslog Host, page 8-2](#).
  - [Configuring the Export of Alarm Triggers to an SNMP Agent, page 8-5](#).
- Step 3** Make any changes you wish on the subsequent screens, and click **Finish**.
- 

## Removing an Existing Syslog or SNMP Alarm Destination

You can easily remove a Syslog or SNMP Alarm Destination using the **Remove** button.

To remove an existing a syslog or SNMP alarm destination:

- 
- Step 1** Click **Start > Administration > Alarm Export**.  
The Alarm Export Administration module appears.
- Step 2** Select the Syslog or SNMP Alarm Destination you wish to remove from the configuration tree at the left of the Alarm Export Administration window.
- Step 3** Click **Remove** in the Export Destinations for Path Analyzer Server field.  
You are prompted to confirm the removal.
- Step 4** Click **Yes**.
-





## CHAPTER 9

# XML Configuration Files

---

## XML Configuration Files

You can modify your Cisco Service Path Analyzer (herein referred to as the Path Analyzer) configuration using XML instead of using the Management Console. To do so, you must follow a three-step process.

- 
- Step 1** Export the current Path Analyzer configuration data using the configuration wizard within the Management Console.
  - Step 2** Modify the XML configuration file.
  - Step 3** Import the modified XML configuration file back into the Path Analyzer System.  
Path Analyzer will identify the changes so you can immediately recognize where the changes are applied.
- 

## Why Use XML Configuration Files?

You can use XML to back up your Path Analyzer configurations. If your configuration become corrupted, you can reload it easily without having to reconfigure your entire system.

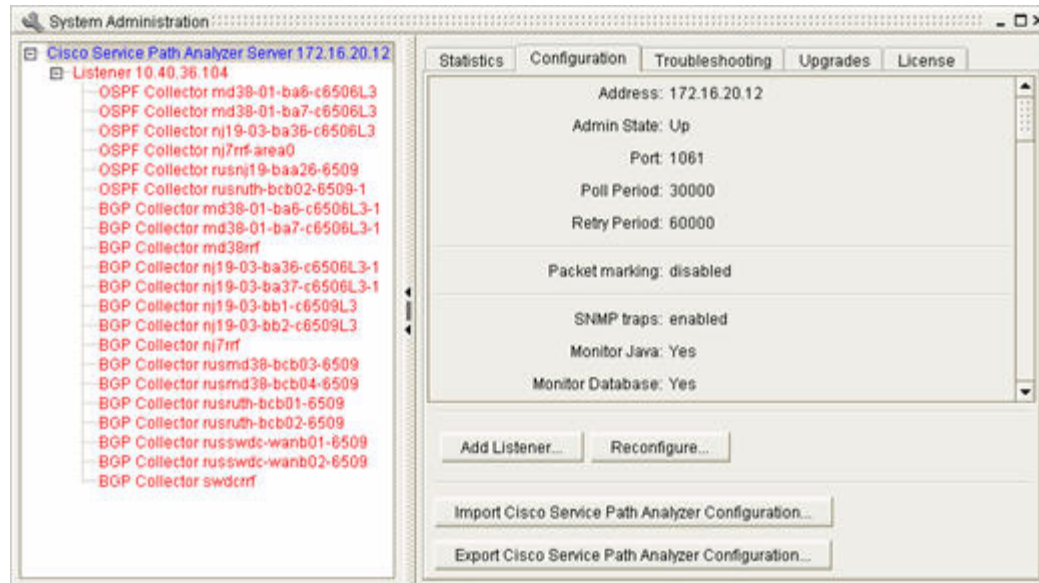
You can also send your configuration data to other network sites that have a setup similar to yours. They can load the XML files and modify them to suit their needs.

You may find it easier to work directly with configuration data in an XML file, rather than making configuration changes using the Management Console.

## Exporting XML Configuration Files

To export the XML Configuration:

- 
- Step 1** Click **Start > Administration > System**. The System Administration window appears.
  - Step 2** Click the **Configuration** tab (see [Figure 9-1](#)).

**Figure 9-1 Configuration Tab: Importing and Exporting a Path Analyzer Configuration via XML**

**Step 3** Click on **Export Path Analyzer Configuration**.

The Path Analyzer Configuration Export Wizard appears.

**Step 4** (Optional) De-select the check box **Do not show this screen again** and click **Next**.

The Please provide a file name for export screen appears.

**Step 5** Select the location on your local computer where you want the XML Export Configuration File to be stored.

**Step 6** Enter a file name in the field.

**Step 7** Click **Next**.

**Step 8** Click **Finish** to complete the Wizard.

The XML Configuration File is stored on your local computer. The process may take a few minutes to finish.



**Note**

XML Export Configuration File is also available via HTTPS. Enter the following URL to access the Path Analyzer Server:

URL: <https://<serverip>/xmlexport.php?user=<username>&pass=<password>> where **server ip** is the IP of the Server, and username and password are the username and password for any admin level user.

## Modifying XML Configuration Files

The process of modifying XML configuration files has two steps:

- [Modify the XML Export File, page 9-3](#)
- [Importing XML Configuration Files, page 9-3](#)

### Modify the XML Export File

Open a text editor such as Notepad. (Notepad is available under the Accessories Menu from the Windows desktop).

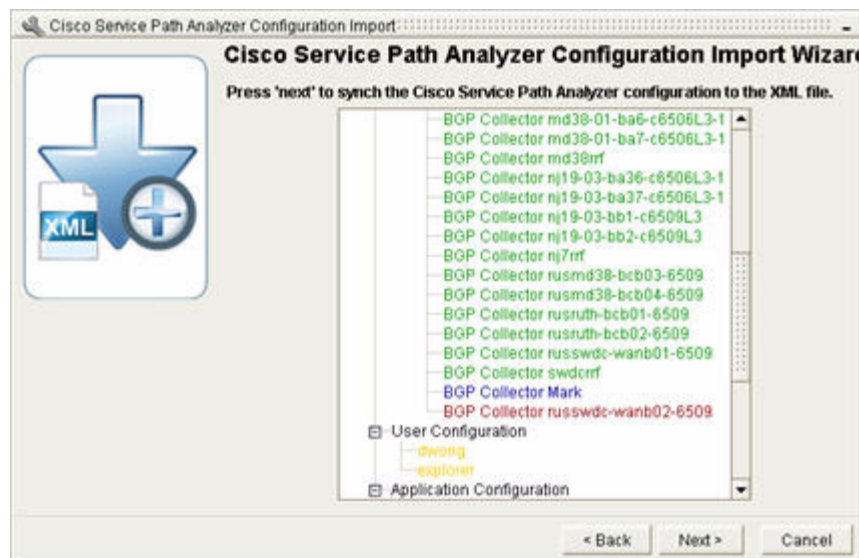
- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Click on the text editor.  |
| <b>Step 2</b> | Select <b>Open</b> and locate the selected folder for the name of your XML Export Configuration. |
| <b>Step 3</b> | Click on the file to open it.  |
| <b>Step 4</b> | Edit the Configuration file as needed.   |
| <b>Step 5</b> | Save the file locally for re-importation.  |
- 

### Importing XML Configuration Files

To import an XML Configuration file:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Click <b>Start &gt; Administration &gt; System</b> . The System Administration window appears.  |
| <b>Step 2</b> | Click on the <b>Configuration</b> tab.  |
| <b>Step 3</b> | Click on <b>Import Path Analyzer Configuration</b> .<br>The Path Analyzer Configuration Import Wizard appears.  |
| <b>Step 4</b> | (Optional) De-select the check box <b>Do not show this screen again</b> and click <b>Next</b> . The Please select the XML file screen appears.  |
| <b>Step 5</b> | Select the location on your local computer where you want to store the XML Configuration file.  |
| <b>Step 6</b> | Enter a file name in the field.   |
| <b>Step 7</b> | Click <b>Next</b> . <ul style="list-style-type: none"><li>• The Path Analyzer System indicates where changes are made to the configuration by highlighting the affected components in yellow.</li><li>• The color blue indicates additions to the configuration.</li><li>• The color green indicates that the configuration of these specific appliances is identical in the XML file and the system.</li><li>• The color red indicates the corresponding appliances are not in the XML file and <i>will be removed</i> upon completion of the wizard (see <a href="#">Figure 9-2</a>).</li></ul> |

**Figure 9-2** Configuration Changes Displayed in the Configuration Import Wizard



**Step 8** Click **Next**.

**Step 9** Click **Finish**.

The configuration changes are processed.

---



## CHAPTER 10

# Maintaining Your Path Analyzer Database

## Purging Your Path Analyzer Database

Periodic maintenance of your Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) database frees space for new data and allows you to store historical data in a safe location where you can restore it when you need it. If you do not configure periodic purges of data, your Path Analyzer system will automatically notify you when you have used 80% of the total disk space available.

You can view statistics regarding disk space in your Path Analyzer database and purge accumulated data from the Data Management Administration module. You can also configure a temporal purge to remove data that occurred on or before a selected date or time. You can set the purge to occur one time or on at periodic intervals.



### Note

Before purging your Path Analyzer database, export the data to a server for storage. For information about completing an export by uploading the database file to a Path Analyzer server, see [Uploading Files, page 11-17](#). Also, see [Configuring a Purge, page 10-3](#).

## Data Management Tasks

- [Starting the Data Management Administration Module, page 10-1](#)
- [Managing Your Data, page 10-2](#)
- [Configuring a Purge, page 10-3](#)
- [Completing a Temporal Purge, page 10-7](#)
- [Canceling a Temporal Purge, page 10-8](#)

## Starting the Data Management Administration Module

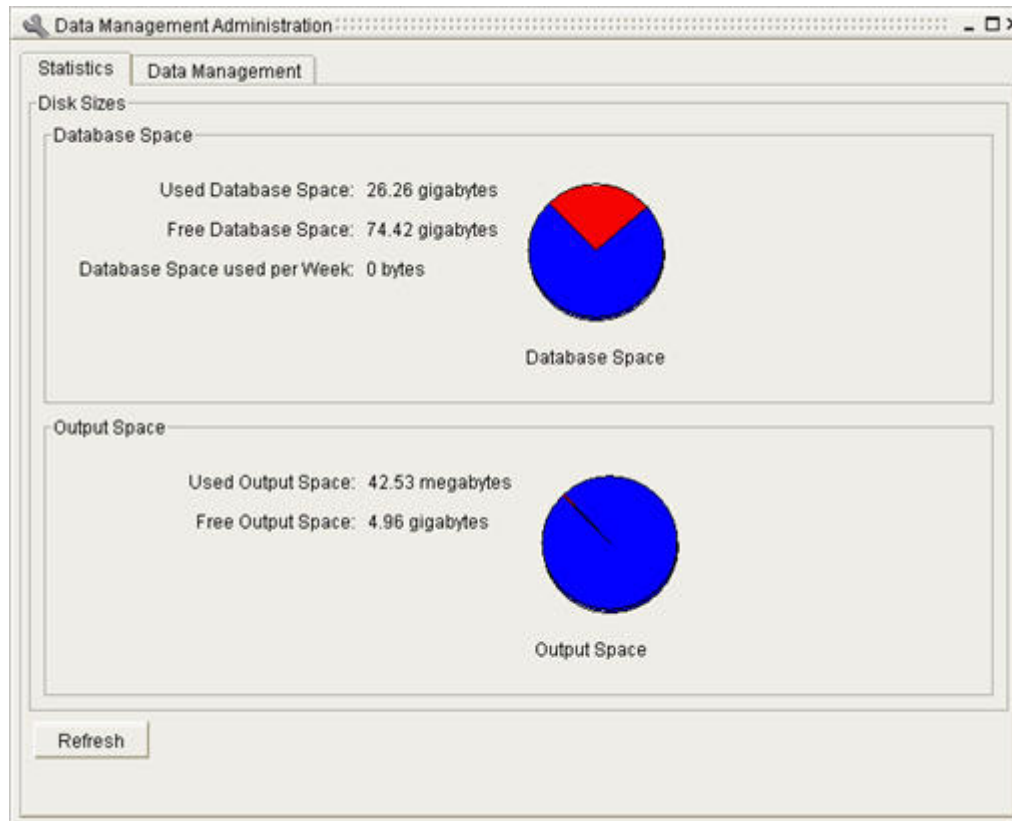
To start the Data Management Administration Module, click **Start > Administration > Data Management**.

The Statistics tab of the Data Management window appears, as shown in [Figure 10-1](#).

See [Viewing Database Statistics, page 10-2](#).

The Data Management window also provides options for purging your database.

See [Scheduling a Periodic Purge, page 10-3](#).

**Figure 10-1 Statistics Tab in Data Management Administration Module**

## Managing Your Data

Good practice suggests that you should periodically export your database to a file on a server or storage device, then purge or remove data from the database. Purging data makes room for new, real-time data.

**Note**

If you select not to clear your database on a regular schedule, Path Analyzer alerts you when your database becomes 80% full. At that time, you can see [Uploading Files, page 11-17](#) and [Completing a Temporal Purge, page 10-7](#) or [Scheduling a Periodic Purge, page 10-3](#).

## Viewing Database Statistics

To view database statistics:

- Step 1** Click **Start > Administration > Data Management**.  
The Data Management Administration window appears.
- Step 2** Select the **Statistics** tab. The following information is displayed:  
Database Space—Information about total database usage.



- Used Database Space—Total number of megabytes of space used for data.
- Free Database Space—Total number of megabytes of space unused space.
- Database Space used per Week—Estimated number of megabytes of space used for data per week.

Output Space—Information about database space allocated for modules that provide output, such as charts and reports.

- Used Output Space—Total number of megabytes of space used for data output.
- Free Output Space—Total number of megabytes of unused space for data output.

Refresh Button—Updates statistics displayed in the Statistics tab.

---

## Configuring a Purge

Path Analyzer enables you to export a slice of data, collected within a selected period of time, to a file, before purging it from your system. This safeguards your data by preserving it in a location from where it can be restored, if necessary.



### Note

If you are certain that you will not require your data in the future, don't export it. However, best practices suggest exporting the data before purging it, and configuring an export is recommended.

---

After configuring an export, you can configure a temporal purge, which removes data that occurred on or before a selected date and time.

Additionally, you can configure periodicity, which allows you to issue the temporal purge on a periodic basis, for example, at midnight on the first of the month.

For information about completing an export by uploading the database file to a Path Analyzer server, see [Uploading Files, page 11-17](#).

## Scheduling a Periodic Purge

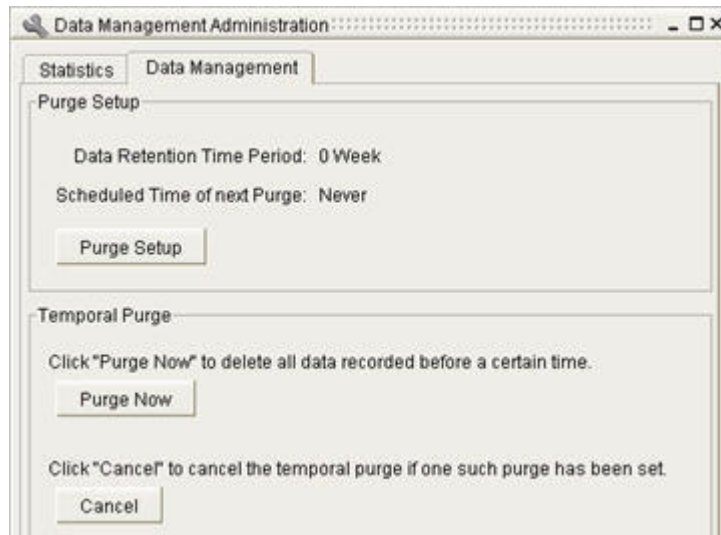
You can schedule periodic purges of the database to save disk space.

To schedule a periodic database purge:

---

- Step 1** Click **Start > Administration > Data Management**.  
The Statistics tab of the Data Management window appears.
- Step 2** Select the **Data Management** tab (see [Figure 10-2](#)).

**Figure 10-2** Data Management Tab in Data Management Administration Module



- Step 3** Click **Purge Setup** in the **Purge Setup** field.  
The Enter the Time Retention Parameters wizard screen appears (see [Figure 10-3](#)).

**Figure 10-3** Enter Time Retention Parameters Screen in Purge Setup Wizard



- Step 4** Select an amount of data to keep:
- Enter a number in the Keep field, (1-4095).
  - Click the arrow and select **Week**, **Month**, or **Year** from the drop-down box to indicate the number of weeks, months, or years of data to keep.

- Step 5** Click **Next**.

The Select the Periodic Purge Type wizard screen appears (see [Figure 10-4](#)).

**Figure 10-4** Periodic Purge Type Screen in Purge Setup Wizard

**Step 6** Configure the interval of the purge period:

a. Select the interval for the purge in the Please select the periodic purge type field:

- **Daily**—Enables a daily purge.

If you select a daily purge, select **Daily** and click **Next**.

The Daily Time Parameters screen appears.

- **Weekly**—Enables a weekly purge.

If you select a weekly purge, select **Weekly** and click **Next**.

The Weekly Time Parameters screen appears.

- **Monthly**—Enables a monthly purge.

If you select a monthly purge, select **Monthly** and click **Next**.

The Monthly Time Parameters screen appears.

- **End of every Month**—Enables a purge on the last day of each month.

If you select to purge the database at the end of every month, select **End of every Month** and click **Next**.

The End of Month Time Parameters screen appears.

- **Yearly**—Enables a yearly purge.

If you select a yearly purge, select **Yearly** and click **Next**.

The Yearly Time Parameters screen appears.

- **Once at a future time**—Set a future date and time for the purge.

If you select to purge the database once at a future time, select **Once at a future time** and click **Next**.

The Future Time Parameters screen appears.

- **No purge**—Completes a single, one-time purge without setting periodic purging.

If you select not to purge the database, select **No purge** and click **Next**

**Step 7** Click **Finish**.

## Select Daily Purge Parameters

For a daily purge:

- 
- Step 1** Select the hour you want the purge to occur in the Day of Week field.
- **Hour**
  - **AM or PM**
- Step 2** Click **Next**.
- Step 3** Click **Finish**.
- 

## Select Weekly Purge Parameters

For a weekly purge:

- 
- Step 1** Select the day of the week on which you want the purge to occur in the Day of Week field.
- Step 2** Select the time for the purge to occur in the Time fields.
- Step 3** Click **Next**.
- Step 4** Click **Finish**.
- 

## Select Monthly Purge Parameters

For a monthly purge:

- 
- Step 1** Select the day of the month on which you want the purge to occur in the Day of Month field.
- Step 2** Select the time for the purge to occur in the Time fields, including:
- **Hour**
  - **AM or PM**
- Step 3** Click **Next**.
- Step 4** Click **Finish**.
- 

## Select End- of-Month Purge Parameters

For a purge that occurs at the end of every month:

- 
- Step 1** Select the date and time for the purge to occur.
- **Hour**
  - **AM or PM**
- Step 2** Click **Next**.

**Step 3** Click **Finish**.

---

### Select Yearly Purge Parameters

For a yearly purge:

- 
- Step 1** Select the month in which you want the purge to occur in the **Month** field.
- Step 2** In the **Day of Month** field, select the day of the month on which you want the purge to occur.
- Step 3** In the **Time** fields, select the time for the purge to occur including:
- **Hour**
  - **AM or PM**
- Step 4** Click **Next**.
- Step 5** Click **Finish**.
- 

### Select a Future One-Time Purge

For a purge selected to occur once on a future date and time:

- 
- Step 1** In the **Time** field, click the arrow and open the calendar.
- Step 2** Select the year and month from the calendar.
- Step 3** Select the hour, minute, second, and AM or PM options.
- Step 4** Click the date in the calendar to complete the past time. *Select the date after all other settings, as it closes the calendar.*
- 

### Select a Single One-Time Purge

For a single, one-time purge:

- 
- Step 1** Select **No Purge** and click **Next**.
- Step 2** Click **Finish**.

The Purge Setup Wizard is completed. The database is purged regularly on the selected date and time.

---

## Completing a Temporal Purge

You can schedule a temporal purge to remove data recorded on and before a selected date and time.

**Note**

After you complete the Temporal Purge Wizard, Path Analyzer allots 5 minutes before purging your database. During that time, you can cancel the purge if you change your mind or decide to set different parameters.

To complete a temporal purge:

- 
- Step 1** Click **Start > Administration > Data Management**.  
The Data Management window appears.
- Step 2** Select the **Data Management** tab.
- Step 3** Click **Purge Now** in the Temporal Purge field.  
The Enter a Past Time wizard screen of the Temporal Purge Wizard appears.
- Step 4** Click the arrow and open the calendar in the Time field. Set the year, month, time, date:
- Select the year and month from the calendar.
  - Select the hour, minute, second, and AM or PM options.
  - Click the date in the calendar to complete the past time. *Select the date after all other settings, as it closes the calendar.*
- Step 5** Click **Next**.  
The Please Select box appears to confirm the purge and inform you that purged data cannot be retrieved.
- Step 6** Click **Yes** to confirm that you want to purge data that occurred on or before the selected date and time.  
A message is displayed to inform you that the purge will occur in five minutes. In this timeframe, you can cancel the purge entirely or configure a new set of purge parameters
- Step 7** Click **OK**.
- Step 8** Click **Finish** to complete the wizard.
- 

## Canceling a Temporal Purge

To cancel a Temporal Purge, click the **Cancel** button on the Data Management tab.



# CHAPTER 11

## System Diagnostics and Troubleshooting

---

Cisco Service Path Analyzer (hereafter referred to as the Path Analyzer) comes with a variety of tools you can use to monitor system performance and troubleshoot network problems, should they arise. The following topics are covered in this chapter:

- [Monitoring Performance, page 11-1](#)
- [Using System Diagnostics, page 11-3](#)
- [Troubleshooting a Path Analyzer Appliance, page 11-5](#)
- [Troubleshooting a Collector, page 11-9](#)
- [Uploading Files, page 11-17](#)

### Monitoring Performance

Path Analyzer has a number of diagnostic, monitoring, and troubleshooting tools that are used to optimize system performance. Graphs that chart Path Analyzer statistics are available for viewing with a Web browser.

### Statistics Graphs

The Path Analyzer System provides easy-to-read graphs of important system functions for all the appliances in your system (Servers, Listeners, and Collectors). These graphs are useful for monitoring system performance and for troubleshooting. All statistics can be viewed by hour, day (the default setting), week, month, or year.

The following statistics are available:

#### Server and Listener Statistic Screens

- CPU Utilization
- Memory Utilization
- Java Memory Utilization
- Disk Utilization
- Load Average
- Swap Memory Utilization

- Processes
- Disk I/O Statistics Read and Write Bytes per Second
- CPU Time Awaiting I/O to Complete
- CPU Holding Time IRQ's
- File Handles Used
- Uptime and Idle Time
- Established TCP Connections
- Processor Temp
- System Board Ambient Temp
- System Board Planar Temp
- System Board Riser Temp
- Listeners
- Java Threads
- Network Interfaces
  - Traffic Analysis for I/O, Eth0, and Eth1
  - Traffic Error for I/O, Eth0, and Eth1
  - Traffic Drops for I/O, Eth0, and Eth1

## Collector Statistic Screens

- Collector State
- Collector Route

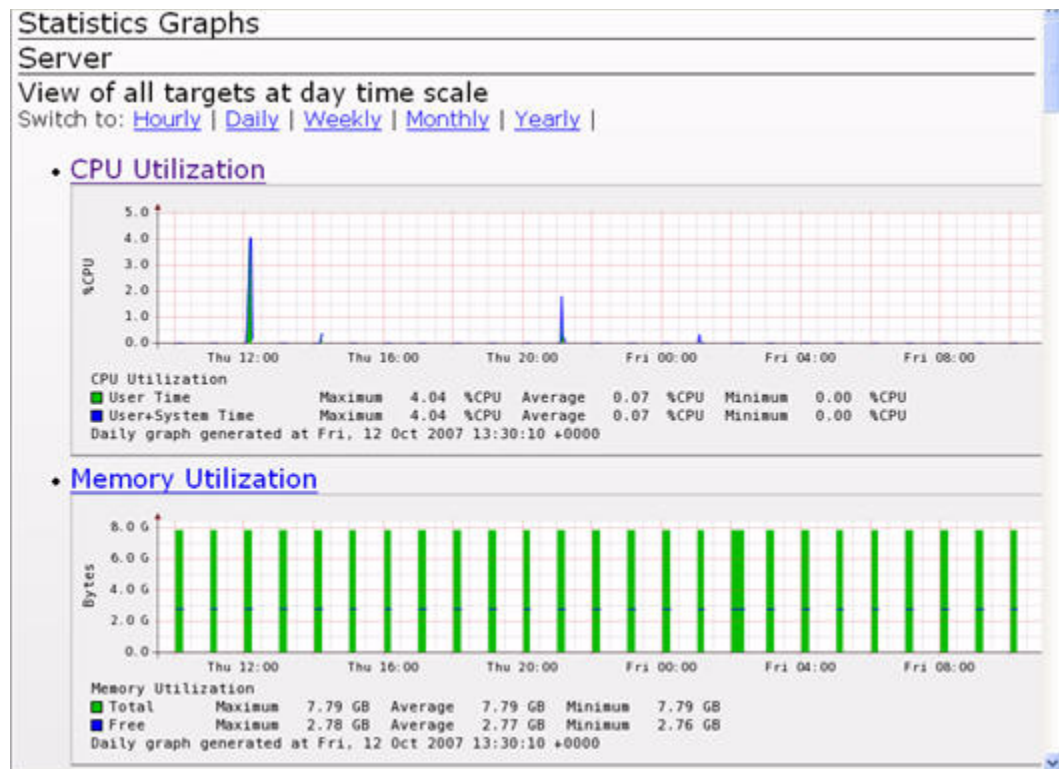
## Accessing Statistics Graphs

To access graphs and view system statistics:

- 
- Step 1** Start your Web browser.
- Step 2** Enter: *http://<IP\_Address>* in the Locator or Address field of your browser, where *<IP\_Address>* is the IP address, or hostname as a URL, of your Path Analyzer Server.
- The Path Analyzer System Management Panel, Management Main Menu page is displayed in your Web browser.
- Step 3** Click **Statistics** on the Main Menu.
- The User Login screen appears.
- Step 4** Log in to authenticate yourself as the system administrator:
- a. In the User Name field, enter the Path Analyzer administrator user name.
  - b. In the Password field, enter the Path Analyzer administrator password.
- Step 5** Click **Login**.
- The Statistics screen appears (see [Figure 11-1](#)).



Figure 11-1 Statistics Graphs Screen (First Two Graphs Shown)



## Using System Diagnostics

Path Analyzer provides diagnostic tools as part of the Configuration Tool, described in [The Configuration Tool, page 3-1](#).

## Viewing System Diagnostics

Diagnostics procedures can be viewed in two ways:

- By accessing the Path Analyzer System Management Panel, Management Main Menu with your browser, or
- Using the Configuration Tool.

## Using Your Browser to View System Diagnostics

To use a Web browser to view system diagnostics:

- Step 1** Enter: `http://<IP_Address>` in the Locator or Address field of your browser, where `<IP_Address>` is the IP address, or hostname as a URL, of your Path Analyzer Server.

The Path Analyzer System Management Panel, Management Main Menu page is displayed in your Web browser.

**Step 2** Click **Diagnostics** on the Main Menu.

The User Login screen appears.

**Step 3** Log in to authenticate yourself as the system administrator:

a. In the User Name field, enter the Path Analyzer administrator user name.

b. In the Password field, enter the Path Analyzer administrator password.

**Step 4** Click **Login**.

The Diagnostics screen appears. The following information is provided:

**Diagnostic hard**

```
system product=PowerEdge 2850
system serial=8QQDLB1
firmware version=A05 (01/09/2006)
disk size=136GB
no link on eth1
ambient temperature=23
system temperature=50
check hard: FAILED
```

**Diagnostic sys**

```
CentOS release 4.4 (Final)
low memory 29244/4151296
SwapCached=52
Inactive=823532
Active=3233572
MemTotal=4151296
SwapTotal=2096472
SwapFree=2096352
MemFree=29244
check sys: PASSED
```

**Diagnostic proc**

```
server (pid 21243) is running... syslogd (pid 1787) is running...
klogd (pid 1791) is running... sshd (pid 21552) is running...
iptivia_watchdog (pid 21249) is running... ntpd (pid 21436) is
running... httpd (pid 21657 21656 21655 21654 21651 21650 21649
21648 21618) is running... mysql (pid 1929) is running...
check proc: PASSED
```

**Diagnostic rpm**

```
check rpm: PASSED
final score: 1
```

---

**Note**

Items shown in red text indicate a failure. Items shown in pink text provide the reason for the failure.

## Using Your Configuration Tool to View System Diagnostics

The Configuration Tool provides the following commands that can be used for viewing diagnostic information.

**Table 11-1 Configuration Tool Commands**

diag	<p><b>Usage:</b> diag [all hard sys proc rpm]</p> <p>The diag command calls the diagtool utility.</p> <p>Perform diagnostics:</p> <p>all</p> <p>Perform all diagnostic checks (default)</p> <p>hard</p> <p>Perform some hardware tests: machine type and CPU, temperature, voltages, power redundancy and RAID checks (if applicable).</p> <p>sys</p> <p>Current system check: Only memory occupation is tested at present.</p> <p>proc</p> <p>Verify that critical processes and services are running.</p> <p>rpm</p> <p>Verify files against RPM (Redhat Packet Maintenance) database</p>
------	---

The command line lets you run any or all of these diagnostic commands. Otherwise, the same information is provided as is available from the browser method.

Instructions for running the Configuration Tool diagnostics utility are provided in [The Configuration Tool, page 3-1](#).

## Troubleshooting a Path Analyzer Appliance

You can troubleshoot a Path Analyzer Server or Listener in the following ways:

- [Verify Connectivity, page 11-6](#) and availability of the IP interfaces that enable Listeners to provide the Path Analyzer Server with data.
- [Verify the Configuration of an Interface, page 11-7](#) on the appliance, including the Eth(*n*) interfaces and loopback interface.
- [Restart an Appliance, page 11-8](#).

## Tools for Completing Troubleshooting Tasks

You can troubleshoot your Path Analyzer system and your network from the Path Analyzer Administration module.

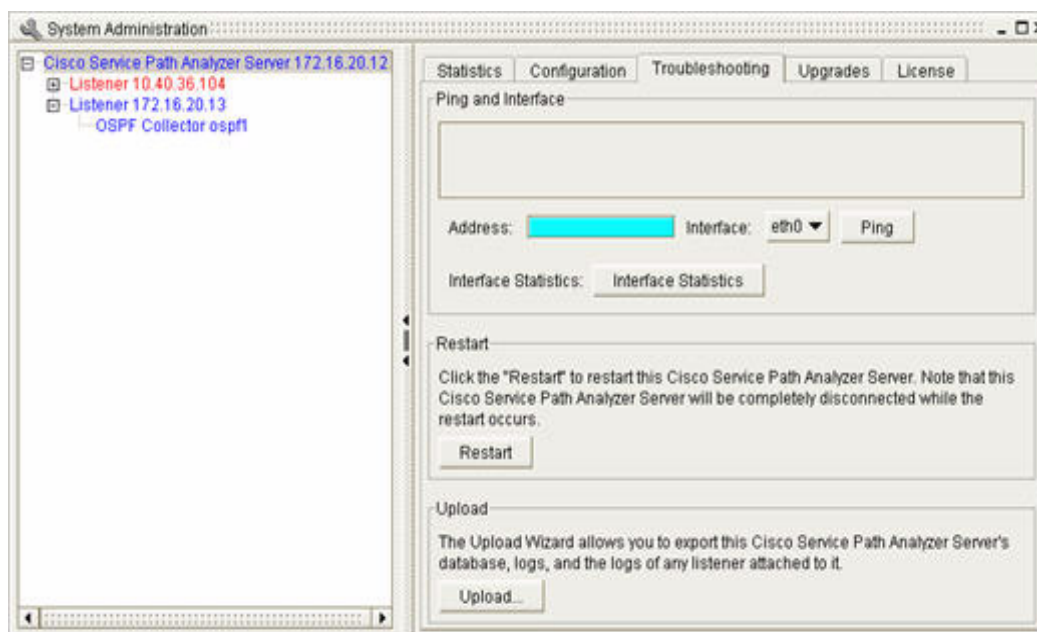


### Note

The **Troubleshooting** tab (see [Figure 11-2](#)) provides data about Listener interfaces and Collector configurations. Analysis of the information requires experience in interpreting results of the ping, ipconfig, top, and df Linux commands as well as familiarity with OSPF RFC 2328 (See <http://www.ietf.org/rfc/rfc2328.txt>) and BGP RFC 1771 (See <http://www.ietf.org/rfc/rfc1771.txt>).

For further assistance in troubleshooting your Path Analyzer system, contact your Cisco Customer Support Representative.

**Figure 11-2** Troubleshooting Tab on Path Analyzer Administration Screen



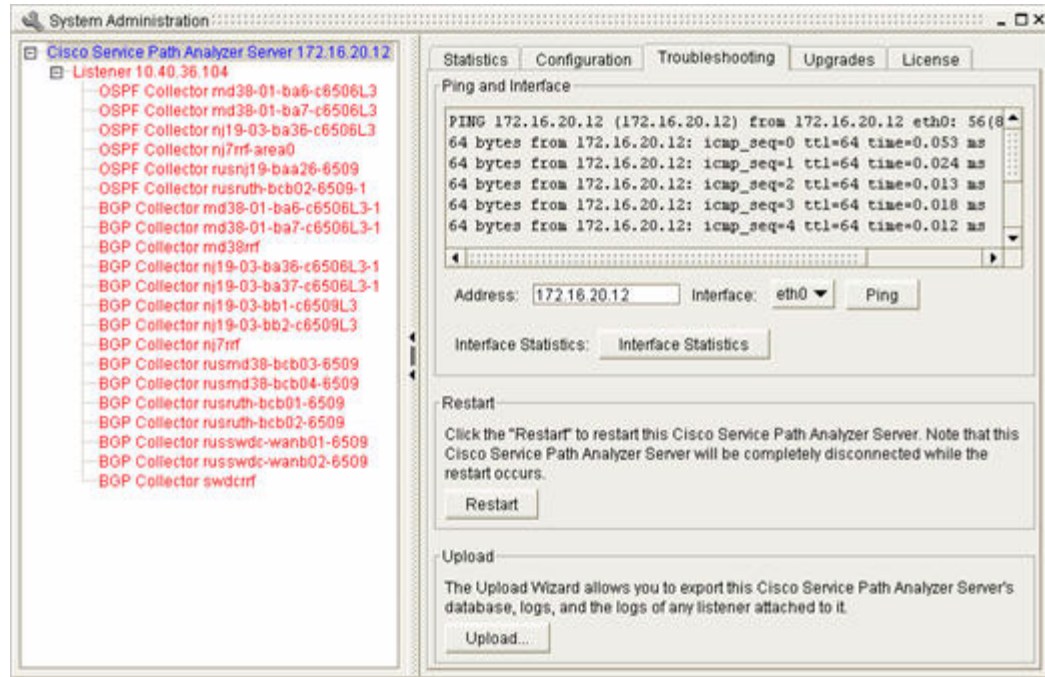
## Verify Connectivity

To verify system connectivity:

- Step 1** Click **Start > Administration > System**. The System Administration window appears.
- Step 2** Select a Path Analyzer Server or a Listener from the configuration tree at the left side of the window.
- Step 3** Select the **Troubleshooting** tab in the right side of the window.
- Step 4** Enter the IP address of the Eth(*n*) interface in the Address field.
- Step 5** Click the drop-down arrow in the Interface field, and select an Eth(*n*) interface on which to issue the ping command.
- Step 6** Click **Ping**.

- The ping command is issued for the selected device. Echo replies returned over Internet Control Message Protocol (ICMP) indicate the availability of the appliance on the network (see [Figure 11-3](#)).
- For information about the data returned, see the man pages that support the ping command in your operating environment.

**Figure 11-3** Ping Results in Troubleshooting Tab

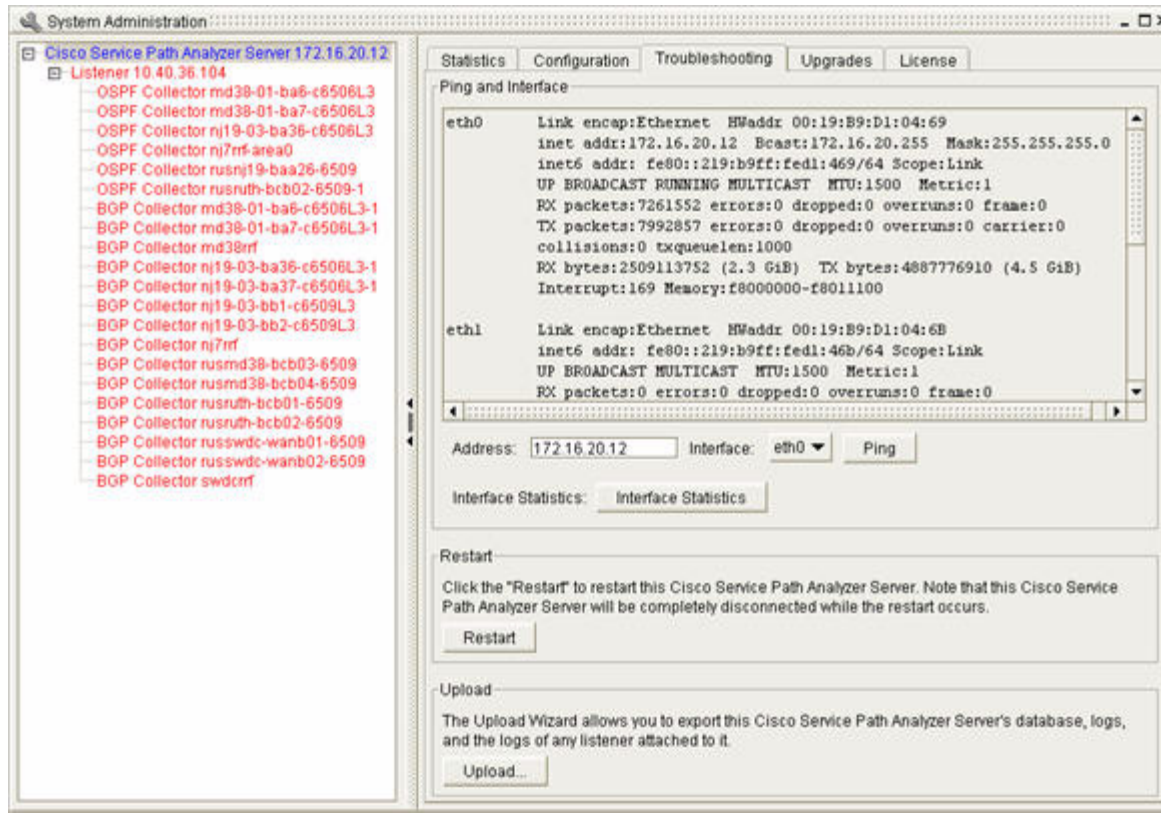


## Verify the Configuration of an Interface

To verify the configuration of an interface:

- Step 1** Click **Start > Administration > System**. The System Administration window appears.
- Step 2** Select a Path Analyzer Server or Listener from the configuration tree at the left side of the window.
- Step 3** Select the **Troubleshooting** tab in the right side of the window.
- Step 4** Click **Interface Statistics**.
  - Details presented after clicking **Interface Statistics** are equivalent to the results provided when you issue an `ifconfig` command using the Configuration Tool (see [Figure 11-4](#)).
  - For information about the significance of each statistic, see the man pages that support the `ifconfig` command in your operating environment.

Figure 11-4 Interface Statistics Results in Troubleshooting Tab



## Restart an Appliance

To restart an appliance:

- Step 1** Click **Start > Administration > System**.  
The System Administration window appears.
- Step 2** Select a Path Analyzer Server or Listener from the configuration tree at the left side of the window.
- Step 3** Select the **Troubleshooting** tab in the right side of the window.
- Step 4** Click **Restart**.  
The appliance is restarted.



### Note

Restarting a Path Analyzer Server interrupts the operation of Path Analyzer clients installed with the Management Console until the Path Analyzer Server finishes the restart and becomes available on your network.

# Troubleshooting a Collector

You can troubleshoot a Collector in the following ways to verify that it is receiving routing updates from its adjacent OSPF or BGP router:

- Verify the adjacency status of a Collector and its OSPF neighbor.
- View the packet stream of an OSPF or BGP collector to ensure that it is receiving and gathering packets.
  - Refresh the packet stream to view current details about a packet.
  - Resume the packet stream.
- View the Link State Advertisement (LSA) database of an OSPF Collector to ensure that it is receiving and gathering packets.
  - Browse the database for LSAs of a specific type.
  - Query for specific LSAs.
- View the Route Database of a BGP Collector.

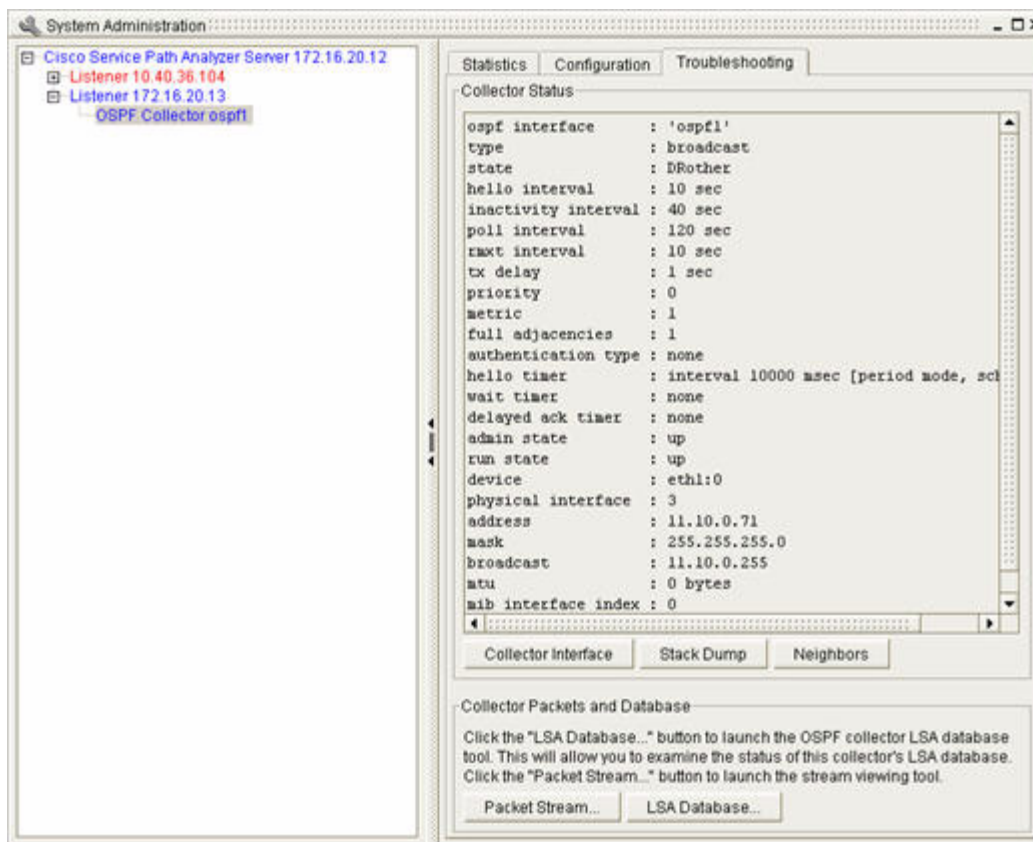
## Verify the Configuration of a Collector Interface

To verify the configuration of a Collector interface:

- 
- Step 1** Click **Start > Administration > System**.  
The System Administration window appears.
- Step 2** Expand an OSPF or BGP Listener in the configuration tree at the left side of the window, and select the Collector from which you want to obtain more information.
- Step 3** Select the **Troubleshooting** tab in the right side of the window. (see [Figure 11-5](#))



Figure 11-5 Collector Interface Screen for OSPF or BGP Collector



**Step 4** Click **Collector Interface** in the Collector Status field at the right side of the window.

Configuration settings of the OSPF or BGP collector interface are displayed.

- Settings for an OSPF Collector include interval and timer values, administrative state, physical and logical connections. These settings can assist in identifying the cause of a possible misconfiguration. To change a misconfigured setting, reconfigure the OSPF Collector in the Collector Configuration Wizard. See [Configuring an OSPF Collector, page 6-25](#).
- Settings for a BGP Collector include the state of the connection, administrative and running states, and attributes of the physical interface. These settings can assist in identifying a possible misconfiguration. To change a misconfigured setting, reconfigure the BGP Collector in the Collector Configuration Wizard. See [Configuring a BGP Collector, page 6-35](#).

## View the OSPF or BGP Stack of a Collector

To view the OSPF or BGP stack of a Collector:

**Step 1** Click **Start > Administration > System**.

The System Administration window appears.

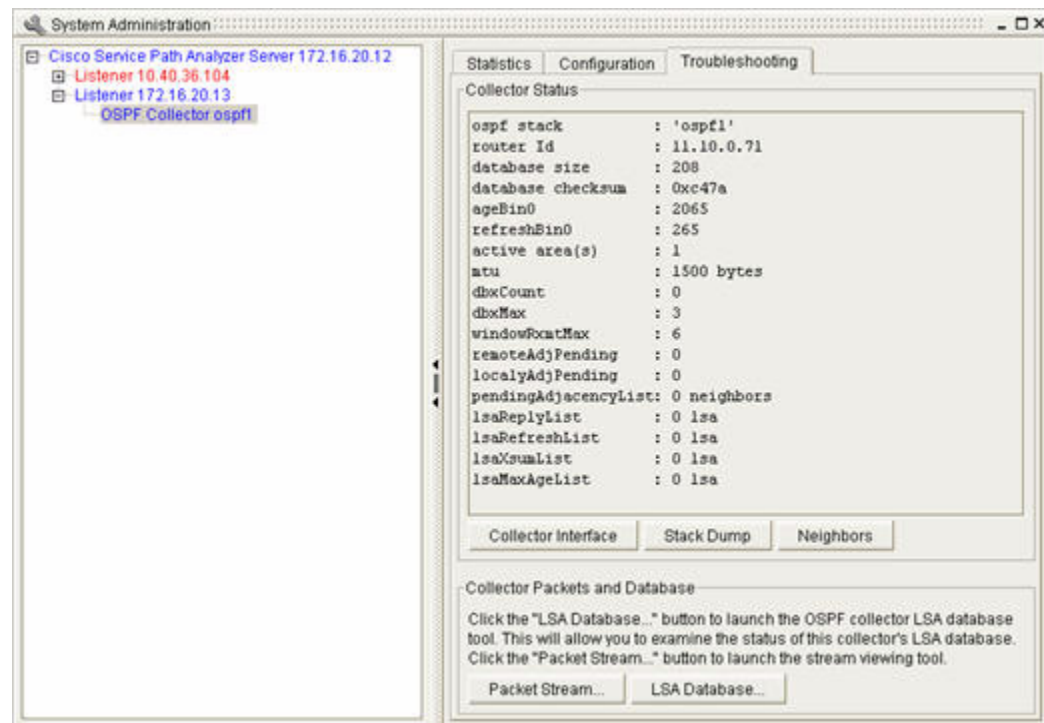


- Step 2** Expand an OSPF or BGP Listener in the configuration tree at the left side of the window, and select the Collector from which you want to obtain more information.
- Step 3** Select the **Troubleshooting** tab in the right side of the window.
- Step 4** Click **Stack Dump** in the Collector Status field at the right side of the window.

Parameters of the OSPF or BGP collector's stack are displayed in the Collector Status field (see Figure 11-5).

- OSPF stack parameters include the name of the collector configured with the stack, the Router ID of the adjacent router, bin and count values, and the number of LSAs recorded in the Reply, Refresh, Checksum, and Maximum Age lists.
- BGP stack parameters include the name of the collector configured with the stack, the Router ID of the adjacent router, number of routes in the route tree, and hold, keepalive, and connection retry intervals and timers.

**Figure 11-6** Stack Dump Screen for OSPF or BGP Collector



## Verify Configured OSPF Neighbors

OSPF neighbors share a point-to-point (P2P) or point-to-multicast-point (PTMP) link with the router that forms an adjacency with the OSPF Collector.



### Note

This option is not available for BGP Collectors because in BGP the type of connection that two speakers share is irrelevant.

To verify configured OSPF neighbors:

**Step 1** Click **Start > Administration > System**.

The System Administration window appears.

**Step 2** Expand an OSPF or BGP Listener in the configuration tree at the left side of the window, and select the Collector from which you want to obtain more information.

**Step 3** Select the **Troubleshooting** tab in the right side of the window.

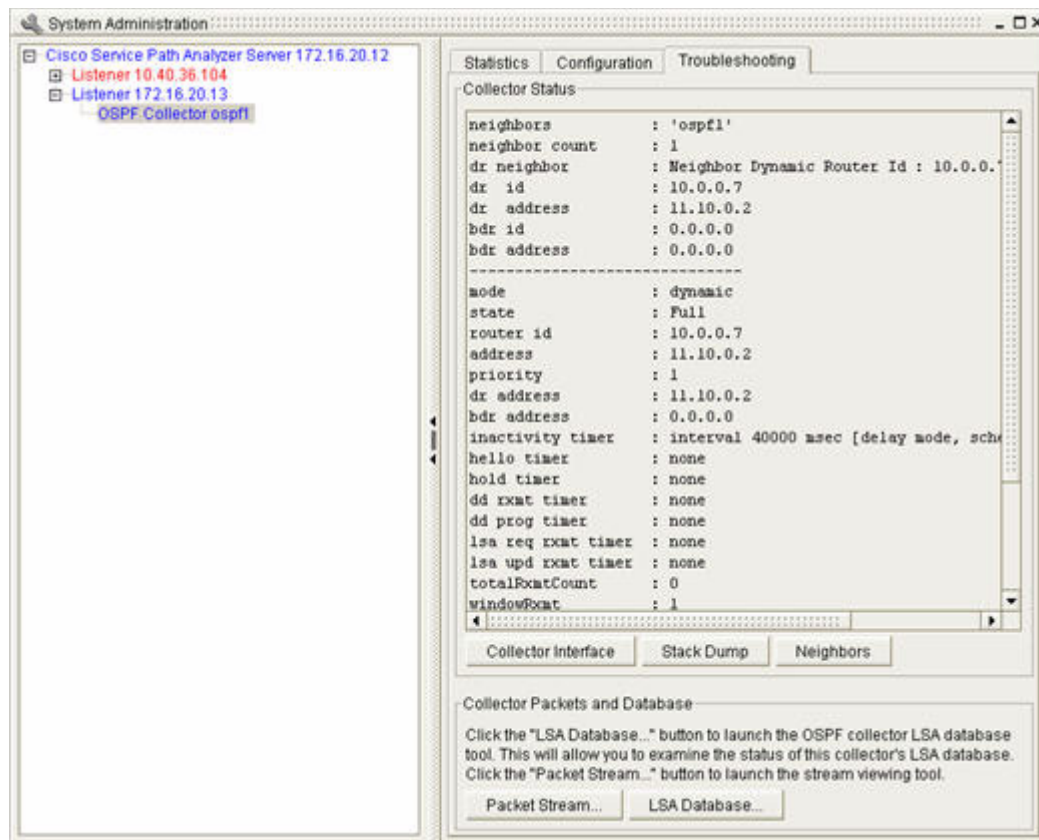
**Step 4** Click **Neighbors** in the Collector Status field at the right side of the window.

Information about OSPF neighbors are displayed. This information includes:

- Name of the OSPF collector configured for the OSPF neighbor
- Router ID and interface address of the Designated Router (DR) and Backup Designated Router (BDR)
- Mode and state of connection
- Values set for timers and counts

This information is valuable in identifying potential disconnects or changes in the availability of an OSPF neighbor (see [Figure 11-7](#)).

**Figure 11-7** Neighbors Screen for OSPF Collector



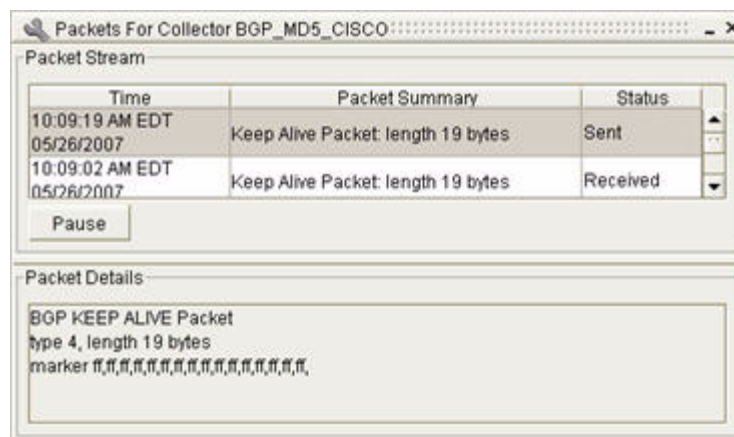
## Analyze the Packet Stream of a Collector

To analyze the packet stream of a collector:

- Step 1** Click **Start > Administration > System**.  
The System Administration window appears.
- Step 2** Expand a Listener from the configuration tree at the left side of the window, and select the OSPF or BGP Collector from which you want to obtain more information.
- Step 3** Select the **Troubleshooting** tab in the right side of the window.
- Step 4** Click **Packet Stream** in the Collector Packets and Database field at the right side of the window.
  - For an OSPF Collector, the Packets for (OSPF) Collector dialog box appears, listing Hello Packets received by the OSPF Collector.
  - For a BGP Collector, the Packets for (BGP) Collector dialog box appears, listing Packets received by the BGP Collector.
- Step 5** Click **Pause** from the Packet Stream table, and select a packet to view its details (see [Figure 11-8](#)).
- Step 6** Click **Resume** to continue processing the packet stream.

The packet stream indicates the Collector's ability to receive packets from the adjacent router and distribute packets to the Path Analyzer Server. Viewing the packet stream assists in identifying configuration changes required on the adjacent router or on another router in the network.

**Figure 11-8** Pack Stream Dialog Box for OSPF or BGP Collector



## Browse the LSA Database of an OSPF Collector

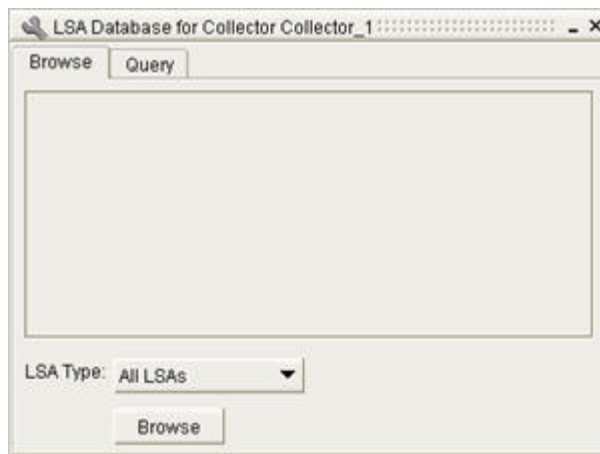
LSAs provide information about network topology and how to route packets across an area, autonomous system, or multiple systems. You can browse the LSA database to monitor your OSPF Collectors.

### Browse the LSA Database

To browse the LSA database:

- 
- Step 1** Click **Start > Administration > System**.  
The System Administration window appears.
- Step 2** Expand an OSPF Listener from the configuration tree at the left side of the window, and select the Collector from which you want to obtain more information.
- Step 3** Select the **Troubleshooting** tab in the right side of the window.
- Step 4** Click **LSA Database** in the Collector Packets and Database field at the right side of the window.  
The Browse tab appears, listing LSAs the collector has received and processed.
- Step 5** Select an LSA Type from the LSA Type field of the LSA Database for Collector dialog box:
- **All LSAs**
  - **Router LSAs**
  - **Network LSAs**
  - **T3 Summary LSAs**
  - **T4 Summary LSAs**
  - **External LSAs**
- Step 6** Click **Browse**.  
The Browse tab displays the list of LSAs of the selected type that the collector has received (see [Figure 11-9](#)). From the list of LSAs, you can select a specific LSA to query for more information.

**Figure 11-9** Browse Tab of LSA Database for OSPF Collector



This information can assist you in verifying that:

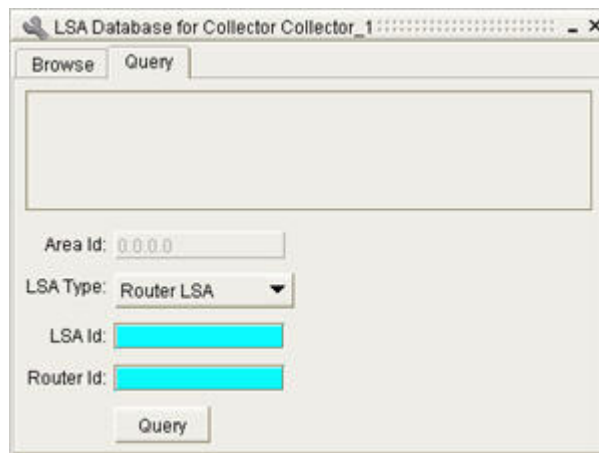
- OSPF Collector receives LSAs from the configured router over the correct interface.
  - Checksum indicates that all data arrived that was included in an LSA.
  - Age of the data is correct.
- 

## Query the OSPF Route Database

To query the OSPF route database:

- 
- Step 1** Click the **Query** tab in the LSA Database for Collector dialog box.
- Step 2** Enter the area where the OSPF Collector is located in the Area Id field.
- Step 3** Select an LSA type to query from the LSA Type field.
- Step 4** Enter the LSA Id of a specific LSA to query in the LSA Id field.
- Step 5** Click **Query** (see [Figure 11-10](#)).  
Details about the selected LSA are displayed.

**Figure 11-10** Query Tab of LSA Database for OSPF Collector



## Browse the Route Database of a BGP Collector

When viewing the route database of a BGP Collector, you can perform the following tasks:

- [Browse the BGP Route Database, page 11-15](#)
- [Query the BGP Route Database, page 11-16](#)

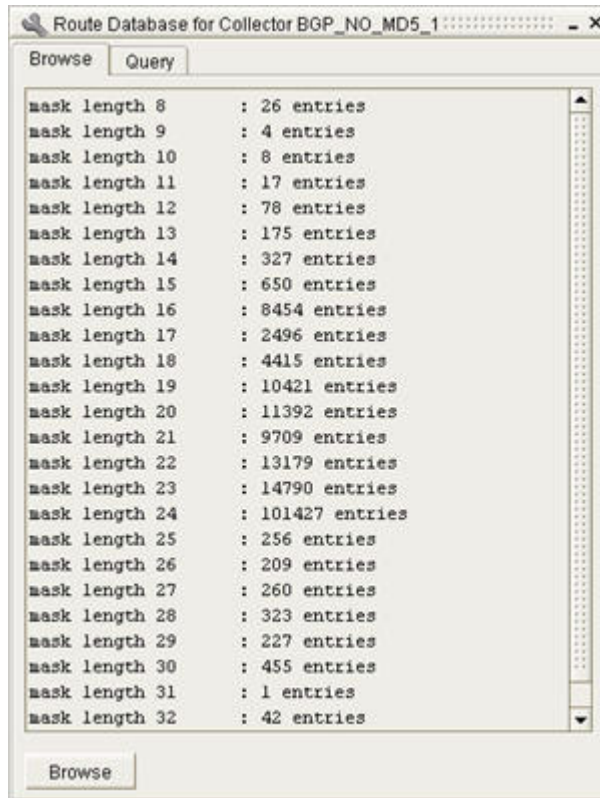
### Browse the BGP Route Database

To browse the BGP route database:

- 
- Step 1** Click **Start > Administration > System**.  
The System Administration window appears.
- Step 2** Expand a BGP Listener from the configuration tree at the left side of the window, and select the BGP Collector from which you want to obtain more information.
- Step 3** Select the **Troubleshooting** tab in the right side of the window.
- Step 4** Click **Route Database** in the Collector Packets and Database field at the right side of the window.  
The Browse tab of the Route Database dialog box appears.
- Step 5** Click **Browse**.

You will see a list of BGP routes the Collector has received (see [Figure 11-11](#)). This information can help you determine that the BGP Collector receives correct and complete information about routes from the configured BGP peer.

**Figure 11-11** Browse Tab of Route Database Screen for BGP Collectors

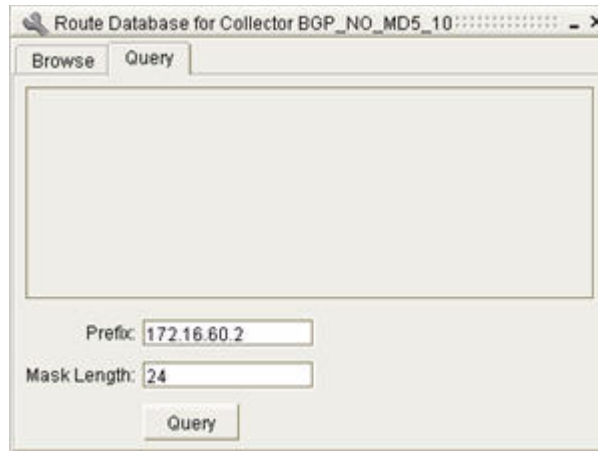


## Query the BGP Route Database

To query the BGP route database:

- Step 1** Click the **Query** tab in the Route Database for Collector dialog box.
- Step 2** Enter the prefix of a BGP route in the Prefix field.
- Step 3** Enter the mask length of the route in the Mask Length field.
- Step 4** Click **Query** (see [Figure 11-12](#)).

Details about the selected route are displayed.

**Figure 11-12 Query Tab of Route Database Screen for BGP Collectors**

## Uploading Files

If you require assistance with troubleshooting or if you choose to store your data off site before purging your database, you can upload your database to a local server or to a Path Analyzer server. Contact Cisco Technical Support for assistance.

A Technical Support representative will provide you with a case number, document your issue, and assist you in completing the Log and Database Upload Wizard. You can use this wizard to:

- Upload your Path Analyzer database and the log files of the Path Analyzer Server and Listeners to an Path Analyzer server.

*or*

- Download these files to your local computer and e-mail them to your Technical Support representative for analysis.

## Upload Path Analyzer Files

To upload Path Analyzer files into the system:

- 
- Step 1** Click **Start > Administration > System**.  
The System Administration window appears.
  - Step 2** Select the Path Analyzer Server from the configuration tree at the left of the window.
  - Step 3** Click the **Troubleshooting** tab in the right side of the window.
  - Step 4** Click **Upload** in the Upload section of the tab.  
The Log and Database Upload Wizard appears.
  - Step 5** (Optional) Click the **Do not show this screen again** check box.
  - Step 6** Click **Next**.  
The Upload Parameters screen appears (see [Figure 11-13](#)).

**Figure 11-13 Upload Parameters Screen of Upload Wizard**

- a. Enter the case number that your Cisco Technical Support representative gave you in the Case Number field.
- b. Select the type of file to upload in the Uploads field:
  - **Path Analyzer Server Database**
  - **Path Analyzer Server and Listener Logs**
- c. Select the location where you want to temporarily store the files in the Location field:
  - **Directly to Cisco Technical Support**
  - **Locally to Your Computer**
- d. Click **Next**.

If you selected to upload files to Cisco Technical Support, a message is displayed informing you that the files are being uploaded to a server.

If you selected to download files to your local system, a message is displayed indicating that your files are being downloaded and that your further instructions will appear in your Web browser. When your Web browser opens, you can select to open the downloaded files or save them to a local directory.

**Note**

Sometimes Web browsers are configured to save files to a default location such as your desktop.

To save exported Path Analyzer database and log files to a directory on your local computer, you may have to change your default browser settings.

After you change the default settings, you can browse to any location on your computer and save the files to that location.