Cisco Service Path Analyzer Alarm Reference

Release 1.0

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

Text Part Number: OL-12862-01

Cisco Service Path Analyzer User Guide

CONTENTS

Preface

The *Cisco Service Path Analyzer Alarm Reference* provides information about the messages that are displayed in Alarm Monitor after an alarm is triggered in response to events affecting services and network elements. It explains the types of alarms you can set and the syntax used in displaying them in the Alarm Monitor.

The chapter also includes information about the Management Information Base (MIB) and how it can be used in conjunction with a network management system.

For information about viewing and setting alarms in Alarm Monitor, see Chapter 8, Setting and Monitoring Alarms, in the *Cisco Service Path Analyzer User Guide*.

For information about exporting alarms, see Chapter 8: Exporting Alarm Triggers in the *Cisco Service Path Analyzer Administration Guide*.

Overview of Cisco Service Path Analyzer

The Cisco Service Path Analyzer (hereafter referred to as the 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

Network administrators who set alarms can use the *Cisco Service Path Analyzer Alarm Reference* to find detailed information about every alarm provided in the Alarm Monitor.

Organization

This guide is organized into the following chapters:

Chapter Number	Chapter Title	Description
Chapter 1	Cisco Service Path Analyzer Alarm Conventions	Explains the documentation conventions used in this manual to describe the syntax of Path Analyzer alarms.
Chapter 2	BGP Advertisement Alarms	Explains the syntax and meaning of each advertisement alarm within a BGP environment.
Chapter 3	BGP Threshold per Router Alarms	Explains the syntax and meaning of each threshold per router alarm within a BGP environment.
Chapter 4	BGP Route Alarms	Explains the syntax and meaning of each route alarm within a BGP environment.
Chapter 5	BGP Threshold per AS Alarms	Explains the syntax and meaning of each threshold per AS alarm within a BGP environment.
Chapter 6	BGP Next Hop Alarms	Explains the syntax and meaning of each next hop alarm within a BGP environment.
Chapter 7	Interface Alarms	Explains the syntax and meaning of each interface alarm within an OSPF environment.
Chapter 8	Router Alarms	Explains the syntax and meaning of each router alarm within an OSPF environment.
Chapter 9	Transit Network Alarms	Explains the syntax and meaning of each Transit network alarm within an OSPF environment.
Chapter 10	Advertisement Alarms	Explains the syntax and meaning of each advertisement alarm within an OSPF environment.
Chapter 11	Route Alarms	Explains the syntax and meaning of each route alarm within an OSPF environment.
Chapter 12	Threshold Alarms	Explains the syntax and meaning of threshold alarm within an OSPF environment.
Chapter 13	Error Alarms	Explains the syntax and meaning of each error alarm within an OSPF environment.

Chapter Number	Chapter Title	Description
Chapter 14	Service and Service Path Alarms	Explains the syntax and meaning of each service and service path alarm.
Chapter 15	Wildcard Alarms	Explains the syntax and meaning of OSPF, BGP, and Service/Service Path wildcard alarms.
Chapter 16	SNMP Traps	Explains the Alarm MIB, how it is structured and how it can be used in conjunction with your Network Management System.

Related Documentation

The *Cisco Service Path Analyzer Alarm Reference* is accompanied by the following related documentation:

- *Cisco Service Path Analyzer Installation Guide*—Provides information about the following topics:
  - Prerequisites for installation
  - Loading Cisco Service Path Analyzer software.
  - Initial system configuration tasks.
  - Database backup and restore
- *Cisco Service Path Analyzer System Administration Guide*—Provides detailed information about the following topics:
  - Initial configuration of your Path Analyzer system, including the following configuration tasks:
  - Assigning the Path Analyzer Server IP address, subnet mask, gateway, and other related information using the Server Configuration Tool.
  - Installing the Path Analyzer Management Console.
  - Configuring Listeners and Collectors.
  - Assigning an IP address and subnet mask to each Listener.
  - Administering and maintaining your Path Analyzer system:
    - Adding, removing, and changing Listeners and Collectors.
    - Adding, removing, and modifying user accounts.
    - Upgrading, registering, and licensing your Path Analyzer software.
    - Exporting the Path Analyzer database and system logs.
    - Restarting your Path Analyzer Server.
  - Setting up user accounts or multi-user access to the Management Console.
  - Configuring names for autonomous systems and routing domains, adding static routes, and setting up forwarding resolution.
- *Cisco Service Path Analyzer 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 to Service Monitor to create and monitor network end users, departments and services, using visual representations.
  - Using the 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 Web Schedule Manager to view and manage schedules and completed tasks.
- *Release Notes for Cisco Service Path Analyzer 1.0*—Provide information about the following topics:
  - Compatible hardware and software platforms.
  - System requirements.
  - Known and fixed software and documentation issues.
- *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

Additional Technical References

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

OSPF Technical Information

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

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

BGP Technical Information

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

- RFC 4271, *A Border Gateway Protocol 4*—Provides a comprehensive review of the draft standard protocol. Download a text version at: 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

Support for Alarm Trigger Exporting

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

Syslog

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

- syslog (3)
- syslog.conf (5)
- syslogd (8)
- RFC 3164—The BSD Syslog Protocol, which defines the protocol. See http://www.ietf.org/rfc/rfc3164.txt

Simple Network Management Protocol (SNMP)

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

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

Cisco Service Path Analyzer Alarm Conventions

Alarm Conventions

The *Cisco Service Path Analyzer Alarm Reference* defines the syntax and provides an example of every alarm displayed in the Alarm Monitor. The following topics are covered:

BGP Alarms

OSPF Alarms

Service Alarms

SNMP Traps

SNMP Traps on page 16-1

Alarm Syntax Conventions

Alarms use the following syntax conventions:

Convention	Explanation	Example
<*RouterID*>	The host name or IP address of the router.	`rtr1.domain.com` or `23.2.5.2`
<*NetworkID*>	The IP address/mask.	`23.2.5.0/24`
<*InterfaceID*>	The IP address of a router interface, except in the case of the address of an unnumbered interface, in which case this value is substituted with the <MIBIndex>.	`23.2.5.2`
<*AreaID*>	An integer that identifies the area	`0.0.0.0`
<*AS_ID*>	The IP address and subnet mask of the autonomous system in which an ASBR interface resides.	`0.0.0.10/24`
<*Availability*>	Indicates the availability of a map element, such as a router or router interface.	`Up`
<*Number*>	Is the number of any element.	`1`

Multiple options are indicated by any of the previous options separated by a pipe symbol (`|`).

`For example: <Up | Down>.`

Events describe the name of an entity and all attributes of an entity that can be changed. In Alarm Monitor, attributes of an entity are referred to as qualifiers.

Each change alarm describes the old and new values of a particular changeable qualifier.

Alarms related to deleted network elements describe the name of the entity without additional related information.

Note All triggered alarms are displayed in Alarm Monitor with a Low severity, indicated by a green sphere. For information about alarm severities, see Severity Values of Alarms, Chapter 8: Setting and Monitoring Alarms in the *Cisco Service Path Analyzer User Guide*.

Alarms normally have from one to three possible states, indicated by options in the alarm creation wizard used to set the alarm.

Alarms that are set with a specified time interval, trigger continuously after the set number of events occurs within that interval. The Cisco Service Path Analyzer (hereafter referred to as Path Analyzer) refreshes the count between triggers and restarts the clock.

For example, you can set a Service Path Availability Flap alarm to trigger when 5 flaps occur within 90 seconds. The Path Analyzer tracks the first 5 flaps in a 90 second interval, triggers the alarm, resets the count to 0, tracks the next 5 flaps in 90 seconds, and triggers the alarm again.

Setting Wildcard Alarms

You can set each type of alarm against a specific entity or against any type of entity. Alarms set against any type of entity are referred to as *wildcard alarms.*

For example, you can set an alarm against a *specific* NP2P interface in order to receive notifications when the metric of that interface changes. You can also set an alarm against *any* NP2P interface in order to receive notification when the metric of any NP2P interface changes.

CHAPTER 2

BGP Advertisement Alarms

BGP Advertisement alarms are triggered in response to events affecting BGP routes through your network. The Cisco Service Path Analyzer Server generates these events from BGP update messages it receives from BGP Listeners instrumented in your network.

You can set the following BGP Advertisement Alarms.

BGP Advertisement Alarms

The BGP Entity Alarms that you can set through Alarm Monitor are:

BGP Advertisement Availability Change Alarm

- Alarm on on availability change to a BGP Advertisement
- Alarm on availability change to any BGP Advertisement (wildcard alarm)

Change in availability of a selected BGP Advertisement or any BGP Advertisement

The Service Availability Change Alarm is triggered when a BGP Advertisement changes availability, for example, from Advertised to Withdrawn, in the specified time frame or in an unlimited time frame.

Alarm States

BGP Advertisement Availability Change Alarms have the following states, that you can select in Alarm Monitor:

- **Advertised**—Number of times route is advertised within the set time period.
- **Withdrawn**—Number of times the BGP Advertisement is withdrawn within the set time period.
- **Flap**—Specified number of times the BGP advertisement intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[BGP <mask length> Advertisement. Source <ip_address>, Prefix <prefix>. [route
advertisement | route withdrawal | either]. At least <number> changes within <number>
seconds].
```

Example

```
BGP <greater mask length> Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32.
route advertisement. At least 3 times within 30 seconds.

BGP Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32. route withdrawal. At
least 3 times within 30 seconds.

BGP Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32. route advertisement or
route withdrawal. At least 3 times within 30 seconds.
```

BGP Advertisement Availability Flap Alarm

- Alarm on availability flaps of a specified BGP Advertisement
- Alarm on availability flaps of any BGP Advertisement (wildcard alarm)

Number of Flaps on a selected BGP Advertisement or any BGP Advertisement

The BGP Advertisement Availability Flap Alarm is triggered when a BGP Advertisement intermittently changes availability, for example, from Available to Unavailable, within the specified time period or in an unlimited time frame. The intermittent change in availability is referred to as a flap.

Alarm States

BGP Advertisement Availability Flap Alarms have the following states that you can select in Alarm Monitor:

Flap—Specified number of times the BGP Advertisement intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[BGP <mask length> Advertisement. Source <ip_address>, Prefix <prefix>. Route
Advertisement Flap. At least <number> available flap(s) within <number> seconds].
```

Example

```
BGP <exact mask length> Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32.
Route Advertisement Flap. At least 3 available flaps within 30 seconds.
```

BGP Advertisement AS Path Change Alarm

Alarm is triggered when there is a change on the AS path.

Change to AS Path Attribute

The BGP Advertisement AS Path Change Alarm is triggered when there is a change to the AS path attribute within the set time period.

Alarm Syntax

```
[BGP Advertisement. Source <ip_address>, Prefix <prefix>. AS Path Change. At least
<number> times in <number> seconds].
```

Example

```
BGP Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32. AS Path Change. At least
3 times within 30 seconds.
```

BGP Advertisement Next Hop Change Alarm

Alarm is triggered when there is a change on the Next Hop.

Change to Next Hop Attribute

The BGP Advertisement Next Hop Change Alarm is triggered when there is a change to the Next Hop attribute within the set time period.

Alarm Syntax

```
[BGP Advertisement. Source <ip_address>, Prefix <prefix>. Next Hop Change. At least
<number> times in <number> seconds].
```

Example

```
BGP Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32. Next Hop Change. At
least 3 times within 30 seconds.
```

BGP Advertisement Local Preference Change Alarm

Alarm is triggered when there is a change to the Local Preference attribute.

Change to Local Preference Attribute

The BGP Advertisement Local Preference Change Alarm is triggered when there is a change to the Local Preference attribute within the set time period.

Alarm Syntax

```
[BGP Advertisement. Source <ip_address>, Prefix <prefix>. Local Preference Change. At
least <number> times in <number> seconds].
```

Example

```
BGP Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32. Local Preference Change.
At least 5 times within 45 seconds.
```

BGP Advertisement Multi-Exit Discriminator (MED) Attribute Change Alarm

Alarm is triggered when there is a change to the Multi-Exit Discriminator (MED) attribute.

Change to MED Attribute

The BGP Advertisement MED Attribute Change Alarm is triggered when there is a change to the MED attribute within the set time period.

Alarm Syntax

```
[BGP Advertisement. Source <ip_address>, Prefix <prefix>. MED Change. At least
<number> times in <number> seconds].
```

Example

```
BGP Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32. MED
Change. At least 2 times within 15 seconds.
```

BGP Advertisement Community Attribute Change Alarm

Alarm is triggered when there is a change to the Community attribute.

Change to Community Attribute

The BGP Advertisement Community Attribute Change Alarm is triggered when there is a change to the Community attribute within the set time period.

Alarm Syntax

```
[BGP Advertisement. Source <ip_address>, Prefix <prefix>. Community Change. At least
<number> times in <number> seconds].
```

Example

```
BGP Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32. Community Change. At
least 1 time within 1 second.
```

BGP Advertisement Other Path Change Alarm

Alarm is triggered when there are other path changes.

Other Path Changes Attribute

The BGP Advertisement Other Path Change Alarm is triggered when there are other path changes within the set time period.

Alarm Syntax

```
[BGP Advertisement. Source <ip_address>, Prefix <prefix>. Other Path Changes. At least
<number> times in <number> seconds].
```

Example

```
BGP Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32. Other Path Changes. At
least 2 times within 10 seconds.
```

BGP Advertisement Any Change Alarm

Alarm is triggered when there are any changes.

Any Changes Attribute

The BGP Advertisement Any Change Alarm is triggered when there are any changes within the set time period.

Alarm Syntax

```
[BGP Advertisement. Source <ip_address>, Prefix <prefix>. Any Changes. At least
<number> times in <number> seconds].
```

Example

```
BGP Advertisement. Source 200.223.100.10, Prefix 30.8.8.3/32. Any Changes. At least 5
times within 30 seconds.
```

CHAPTER 3

BGP Threshold per Router Alarms

BGP Threshold per Router Alarms

Threshold per Router alarms notify you when the system perceived (or baseline) behavior of a particular BGP router on your network deviates from by a certain percentage defined by you.

There are two main types of threshold per router alarms:

- Route Changes Threshold per Router Alarm on page 3-1
- Event Rate Threshold per Router Alarm on page 3-2

Route Changes Threshold per Router Alarm

This alarm is triggered when the instantaneous number of route entities become more or less than the defined percentage of the threshold value.

Alarm States

Route Changes Threshold per Router Alarms have the following state:

Crosses Threshold Count—Detection of threshold percentage rate of change in number of routes for a router.

Alarm Syntax

```
[BGP Threshold: Rate of Change in Number of Routes for Router: <ip_address>].
```

Example

```
BGP Threshold: Rate of Change in Number of Routes for Router: 200.210.12.0.
```

Event Rate Threshold per Router Alarm

This alarm is triggered when the rate of BGP events at a particular BGP router exceeds the threshold by more than the defined percentage.

Alarm States

Event Rate Threshold per Router Alarms have the following state:

Changes Threshold Rate—Detection of threshold percentage rate of change in number of route updates for a router.

Alarm Syntax

```
[BGP Threshold: Rate of Change in Number of Route Updates for Router: <ip_address>].
```

Example

```
BGP Threshold: Rate of Change in Number of Route Updates Router: 200.210.12.0.
```

CHAPTER 4

BGP Route Alarms

BGP Route Alarms

You can set the following BGP Route alarms:

BGP Route Availability Alarm

Alarm on the addition of a BGP route. (See BGP Specific Route Withdraw Alarm on page 4-3 for more information.)

BGP Route Addition

This alarm is triggered when a new BGP route is discovered on the network. The Cisco Service Path Analyzer Server generates events from update messages of a BGP speaker, indicating that a new BGP route was added.

Alarm States

BGP Route Availability Alarms have the following states, which for this type of alarm you should select **Advertised**:

- **Advertised**—Specified number of times route is advertised within the set time period.
- **Withdrawn**—Specified number of times the BGP Advertisement is withdrawn within the set time period. You must also specify:
  - **Normal Withdraw**, or
  - **Withdrawn and Non-Reachable**
- **Flap**—Specified number of times the BGP advertisement intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[BGP <mask length> Route:, Prefix <prefix>. Route Advertisement. At least <number>
changes within <number> seconds].
```

Example

```
BGP <greater mask length> Route:, Prefix 30.8.8.3/32. Route Advertisement. At least 3
times within 30 seconds.
```

BGP Specific Route Withdraw Alarm

Alarm on the withdrawal of a specific BGP route. This is the same alarm as the BGP Route Availability Alarm but set to **Withdrawn** for a specific route. You must specify whether the route is **Normal Withdraw** or **Withdrawn and Non-Reachable**.

Withdrawal of a BGP route

This alarm is triggered when a known BGP route is withdrawn from the network. The Cisco Service Path Analyzer Server generates events from update messages of a BGP speaker indicating that a BGP route was withdrawn.

Alarm States

BGP Specific Route Availability Alarms have the following states, which for this type of alarm, should be set to **Withdrawn** for a specific route:

- **Advertised**—Specified number of times route is advertised within the set time period.
- **Withdrawn**—Specified number of times the BGP Advertisement is withdrawn within the set time period. You must also specify:
  - **Normal Withdraw**, or
  - **Withdrawn and Non-Reachable**
- **Flap**—Specified number of times the BGP advertisement intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[BGP <mask length> Route:, Prefix <prefix>. Route Withdrawal. At least <number>
changes within <number> seconds].
```

Example

```
BGP <greater mask length> Route:, Prefix 30.8.8.3/32. Route Withdrawal. At least 3
times within 30 seconds.
```

BGP Specific Route Flap Alarm

Alarm on BGP route flap. This is the same alarm as the BGP Route Availability Alarm but set to **Flap** for a specific route.

Flap on a BGP route

This alarm is triggered when a known BGP route intermittently changes its availability on the network.

Alarm States

BGP Specific Route Availability Alarms have the following states, which for this type of alarm you should select **Flap** for a specific route:

- **Advertised**—Specified number of times route is advertised within the set time period.
- **Withdrawn**—Specified number of times the BGP Advertisement is withdrawn within the set time period. You must also specify:
  - **Normal Withdraw**, or
  - **Withdrawn and Non-Reachable**
- **Flap**—Specified number of times the BGP advertisement intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[BGP <mask length> Route:, Prefix <prefix>. Route Advertisement Flap. At least
<number> flaps within <number> seconds].
```

Example

```
BGP <lesser mask length> Route:, Prefix 30.8.8.3/32. Route Advertisement Flap. At
least 3 flaps within 30 seconds.
```

BGP Route Redundancy Alarm

Alarm on BGP route redundancy.

Redundancy on a BGP route

This alarm is triggered when a known BGP route becomes redundant or non-redundant. A route is redundant when there is more than one way to reach the destination of the route.

Alarm States

BGP Route Redundancy Alarms have the following states. For this type of alarm, you should select **Becomes Redundant** or **Becomes Non-Redundant.**

- **Becomes Redundant**—Specified number of times the route becomes redundant within the set time period.
- **Becomes Non-Redundant**—Specified number of times the route becomes non-redundant within the set time period.
- **Flap**—Specified number of times the route intermittently changes redundancy status within the set time period.

Alarm Syntax

```
[BGP Route:, Prefix <prefix>. Becomes [redundant | non-redundant | either]. At least
<number> times within <number> seconds].
```

Example

```
BGP Route:, Prefix 30.8.8.3/32. Becomes redundant. At least 3 times within 30 seconds.

BGP Route:, Prefix 30.8.8.3/32. Becomes non-redundant. At least 3 times within 30
seconds.

BGP Route:, Prefix 30.8.8.3/32. Becomes non-redundant or redundant. At least 3 times
within 30 seconds.
```

BGP Route Redundancy Flap Alarm

Alarm on availability flaps of a specified BGP route redundancy.

Flap Redundancy on a BGP route

This alarm is triggered when a BGP Route intermittently changes availability, for example, from Redundant to Non-redundant, in the specified time period. The intermittent change in availability is referred to as a flap.

Alarm States

BGP Route Redundancy Flap Alarms have the following state:.

Flap—Specified number of times the route intermittently changes redundancy status within the set time period.

Alarm Syntax

```
[BGP Route:, Prefix <prefix>. Redundancy Flap. At least <number> flaps within <number>
seconds].
```

Example

```
BGP Route:, Prefix 30.8.8.3/32. Redundancy Flap. At least 3 flaps within 30 seconds.
```

CHAPTER 5

BGP Threshold per AS Alarms

BGP Threshold per AS Alarms

BGP Threshold per AS alarms notify you when the system baseline behavior of your network deviates from the norm by a certain percentage, defined by you.

There are two main types of threshold per router alarms:

- Route Count Threshold per AS Alarm on page 5-1
- Event Rate Threshold per AS Alarm on page 5-2

Route Count Threshold per AS Alarm

The Route Count Threshold per AS Alarm is triggered when the number of prefixes become more or less than the defined percentage of the threshold value.

Alarm States

Route Count Threshold per AS alarms have the following state:

Crosses Threshold Count—Detection of percentage rate of change in number of routes in an autonomous system.

Alarm Syntax

```
[BGP Threshold: <%Rate of Change> in <number> Routes in AS].
```

Example

```
BGP Threshold: 1 Percent Change in 10 Routes in AS.
```

Event Rate Threshold per AS Alarm

This Event Rate Threshold per AS Alarm is triggered when the rate of events within a particular AS exceeds the threshold by more than the defined percentage.

Alarm States

Event Rate Threshold per AS alarms have the following state:

Crosses Threshold Count—Detection of percentage rate of change in rate of events within an autonomous system.

Alarm Syntax

```
[BGP Threshold: <%Rate of Change> in <number> Route Updates in AS].
```

Example

```
BGP Threshold: 1 Percent Rate of Change in 10 Route Updates in AS.
```

CHAPTER 6

BGP Next Hop Alarms

BGP Next Hop Alarms

Each router included in a BGP route stores the IP address of the next-hop router interface required to reach a given destination. Next Hop alarms notify you when the next hop is no longer reachable using an OSPF route.

You can set the following BGP Next Hop alarm:

BGP Next Hop Alarm on page 6-2

BGP Next Hop Alarm

Alarm on loss of next hop.

Alarm States

BGP Next Hop alarms have the following states:

- **No OSPF route available for this BGP Hop**—This alarm will always trigger when there is no OSPF route available within the set period of time.
- **Only the default route is matching this BGP Hop**—(Optional setting that can be added to the one above.) Alerts when only the default OSPF route is matching the BGP hop within the set period of time.

Note This alarm will always clear if a non-default route matches the BGP next hop.

Alarm Syntax

```
[BGP Next Hop Alarm. <number> time(s) in <number> second(s). Triggers if <no ospf
route matches NextHop> <only the default ospf route matches or no ospf route matches
NextHop>].
```

Example

```
BGP Next Hop Alarm. 1 time(s) in 1 second(s). Triggers if no ospf route matches
NextHop.

BGP Next Hop Alarm. 2 time(s) in 1 second(s). Triggers if only the default ospf route
matches or no ospf route matches NextHop.
```

CHAPTER 7

Interface Alarms

Within an OSPF environment, you can set the following alarms on a Numbered Point-to-Point (NP2P) interface, an Unnumbered Point-to-Point (UP2P) interface, or a Transit interface.

Point-to-Point Interface Alarms

P2P Interface Availability Change Alarm

- Alarm on availability change of a specified P2P interface, numbered or unnumbered
- Alarm on availability change of any P2P interface, numbered or unnumbered (wildcard alarm)

Changes in Availability of a P2P Interface

This alarm is triggered when a P2P interface changes availability from up to down or down to up on the network.

Alarm States

Router Availability Change Alarms have the following states:

- **Becomes Available**—Specified number of times the P2P interface became available within the set time period.
- **Becomes Unavailable**—Specified number of times the P2P interface became unavailable within the set time period.
- **Flap**—Specified number of times the P2P interface intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Numbered Point-to-Point Interface <interface_id> on router <router_id> in area
<area_id>: at least <number> Availability change(s) in <number> seconds]
[Unnumbered Point-to-Point Interface <interface_id> on router <router_id>: at least
<number> Availability change(s) in <number> seconds].
```

Example

```
[Numbered Point-to-Point Interface 192.168.33.44 on router 192.168.43.22 in area
0.0.0.2: at least 4 Availability change(s) in 30 seconds]
[Unnumbered Point-to-Point Interface 72 on router 192.168.70.35 in area 0.0.0.2: at
least 5 Availability change(s) in 25 seconds].
```

P2P Interface Availability Flap Alarm

- Alarm on availability flaps of a specified P2P interface, numbered or unnumbered
- Alarm on availability flaps of any P2P interface, numbered or unnumbered (wildcard alarm)

Number of Flaps on a Selected Router or on any Router

The P2P Interface Availability Flap Alarm is triggered when an NP2P or UP2P interface availability changes intermittently from down to up and up to down within the specified time period.

P2P Interface Flap Alarms are a subset of P2P Interface Availability Change Alarms. For information about the related P2P Interface Availability Change Alarm, see P2P Interface Availability Change Alarm on page 7-2.

Alarm States

P2P Interface Availability Flap Alarms have the following state:

Flap—Specified number of times the P2P interface intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Numbered Point-to-Point Interface <interface_id> on router <router_id> in area
<area_id>: at least <number> availability flap(s) within <number> seconds]
[Unnumbered Point-to-Point Interface <interface_id> on router <router_id> in area
<area_id>: at least <number> availability flap(s) within <number> seconds].
```

Example

```
Numbered Point-to-Point Interface 10.29.88.1 on router 192.168.43.22 in area 0.0.0.1:
at least 4 availability flap(s) within 30 seconds.

Unnumbered Point-to-Point Interface 72 on router 192.168.70.35 in area 0.0.0.1: at
least 5 availability flap(s) within 25 seconds.
```

P2P Interface Metric Change Alarm

- Alarm on metric change of a specified P2P interface, numbered or unnumbered
- Alarm on metric change of any P2P interface, numbered or unnumbered (wildcard alarm)

Changes in Metric of a P2P interface.

This alarm is triggered when a P2P interface metric changes value. The interface metric provides the cost in traversing the link associated with the interface.

Alarm States

P2P Interface Metric Change Alarms have the following state:

Any Change—Specified umber of times the P2P interface metric changed within the set time period.

Alarm Syntax

```
[Numbered Point-to-Point Interface <interface_id> on router <router_id> in area
<area_id>: at least <number> metric change(s) in <number> seconds].

[Unnumbered Point-to-Point Interface <interface_id> on router <router_id> in area
<area_id>: at least <number> metric change(s) in <number> seconds].
```

Example

```
[Numbered Point-to-Point Interface 192.168.33.44 on router 192.168.43.22 in area
0.0.0.2: at least 4 metric change(s) in 30 seconds].

[Unnumbered Point-to-Point Interface 72 on router 192.168.70.35 in area 0.0.0.2: at
least 5 metric change(s) in 25 seconds].
```

Transit Interface Alarms

Transit interface alarms notify you about changes to a router interface that connects to a Transit network.

In Alarm Monitor, you can set the following types of alarms against a Transit interface:

Transit Interface Availability Change Alarm

- Alarm on availability change of a specified Transit interface
- Alarm on availability change of any Transit interface (wildcard alarm)

Changes in Availability of a Transit Interface.

This alarm is triggered when a Transit interface changes availability from up to down or down to up on the network.

Alarm States

Transit Interface Availability Change Alarms have the following states:

- **Becomes Available**—Specified number of times the Transit interface became available within the set time period.
- **Becomes Unavailable**—Specified number of times the Transit interface became unavailable within the set time period.
- **Flap**—Specified number of times the Transit interface intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Transit Interface <interface_id> on router <router_id> in area <area_id>: at least
<number> change(s) within <number> seconds].
```

Example

```
Transit Interface 192.168.39.24 on router 192.168.43.22 in area 0.0.0.2: at least 4
change(s) within 15 seconds.
```

Transit Interface Availability Flap Alarm

- Alarm on availability flap of a specified Transit interface
- Alarm on availability flap of any Transit interface

Number of Flaps on a Selected Transit Interface or on any Transit Interface

The Transit Interface Availability Flap Alarm is triggered when the availability of a Transit interface changes intermittently from down to up and up to down within the specified time period.

Transit Interface Availability Flap Alarms are a subset of Transit Interface Availability Change Alarms. For information about the related Transit Interface Availability Change Alarm, see Transit Interface Availability Change Alarm on page 7-5.

Alarm States

Transit Interface Availability Flap Alarms have the following states that you can select in Alarm Monitor:

Flap—Specified number of times the Transit interface intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Transit Interface <interface_id> on router <router_id> in area <area_id>: at least
<number> Availability flap(s) within <number> seconds].
```

Example

```
Transit Interface 192.168.20.10 on router 192.168.43.22 in area 0.0.0.1: at least 4
Availability flap(s) within 30 seconds.
```

Transit Interface Metric Change Alarm

- Alarm on metric change of a specified Transit interface
- Alarm on metric change of any Transit interface

Changes in Metric of a Transit interface.

This alarm is triggered when a Transit interface metric changes value. The Transit interface metric provides the cost in traversing the link associated with the Transit interface.

Alarm States

Transit Interface Metric Change Alarms have the following state:

Any Change—Specified umber of times the Transit interface metric changed within the set time period.

Alarm Syntax

```
[Transit Interface <interface_id> on router <router_id> in area <area_id>: at least
<number> metric change in <number> seconds].
```

Example

```
Transit Interface 192.168.20.10 on router 192.168.43.22 in area 0.0.0.1: at least 4
metric changes in 30 seconds.
```

CHAPTER 8

Router Alarms

Router Alarms

A router is a network device or software program that routes packets toward their destinations. Specialized types of routers include:

- Area Border Routers (ABR's)—Connects to multiple areas.
- Autonomous System Boundary Routers (ASBR's)—Connects to more than one autonomous system. Sends summarized *external route* information to designated routers in a neighboring autonomous system.

For detailed information about the types of routers supported in Cisco Service Path Analyzer, see Chapter 6 of the *Cisco Service Path Analyzer System Administration Guide*.

Alarm Monitor informs about the following types of router alarms:

Router Availability Change Alarm

- Alarm on on availability change of a specified router
- Alarm on availability change to any router (wildcard alarm)

Changes in Availability of a Router.

This alarm is triggered when a router changes its availability on the network. This alarm can be triggered under the following conditions:

- The router changes availability from up to down or down to up due to configuration changes.
- The router is removed from the network.

For information about the related Router Availability Flap Alarm, which is a type of Router Availability Change Alarm, see Router Availability Flap Alarm on page 8-3.

Alarm States

Router Availability Change Alarms have the following states:

- **Becomes Available**—Specified number of times the router became available within the set time period.
- **Becomes Unavailable**—Specified number of times the router became unavailable within the set time period.
- **Flap**—Specified number of times the router intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Router <router_id>: at least <number> change(s) in <number> seconds].
```

Example

```
Router 192.168.43.22: at least 4 change(s) in 30 seconds.
```

Router Availability Flap Alarm

- Alarm on availability flaps of a specified router
- Alarm on availability flaps of any router (wildcard alarm)

Number of Flaps on a Selected Router

The Router Availability Flap Alarm is triggered when a router intermittently changes its availability on the network. For example, if you issue a Router Availability Flap Alarm against a router, the alarm is triggered when the router changes from up to down and back a specified number of times within the set time interval.

Router Availability Flap Alarms are a subset of Router Availability Change Alarms. For information about the related Router Availability Change Alarm, see Router Availability Change Alarm on page 8-2.

Alarm States

Router Availability Flap Alarms have the following state in Alarm Monitor:

Flap—Specified number of times the router intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Router <router_id>: at least <number> Availability flap(s) within <number> seconds].
```

Example

```
Router 192.168.43.22: at least 4 Availability flap(s) within 30 seconds.
```

ABR Status Change Alarm

- Alarm on availability change of a specified ABR router
- Alarm on availability change to any ABR router (wildcard alarm)

Changes in Status of an ABR.

This alarm is triggered when an ABR establishes or loses connectivity in areas. This alarm can be triggered under the following conditions:

- The ABR advertises a decreased number of areas in which it is configured.
- An ABR configured in two areas, advertises configuration in only one area.
- An ABR interface is removed from an area.

For information about the related ABR Status Flap Alarm, which is a type of ABR Availability Change Alarm, see ABR Status Flap Alarm on page 8-5.

Alarm States

ABR Status Change Alarms have the following states:

- **Becomes Available**—Specified number of times the ABR router became available within the set time period.
- **Becomes Unavailable**—Specified number of times the ABR router became unavailable within the set time period.
- **Flap**—Specified number of times the ABR router intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Router <abr_id>: Becomes [ABR or Non-ABR] at least <number> time(s) in <number>
second(s)].
```

Example

```
Router 192.168.43.22: Becomes ABR at least 4 times in 30 seconds.

Router 192.168.43.22: Becomes Non-ABR at least 4 times in 30 seconds.
```

ABR Status Flap Alarm

- Alarm on availability flaps of a specified ABR router
- Alarm on availability flaps of any ABR router (wildcard alarm)

Number of Flaps on a Selected Router

The ABR Status Flap Router Availability Flap Alarm is triggered when an ABR router intermittently changes its availability on the network. For example, if you issue an ABR Status Flap Alarm against a router, the alarm is triggered when the ABR router changes from up to down and back a specified number of times within the set time interval.

ABR Status Flap Alarms are a subset of ABR Status Change Alarms. For information about the related ABR Status Change Alarm, see ABR Status Change Alarm on page 8-4.

Alarm States

ABR Status Flap Alarms have the following state in Alarm Monitor:

Flap—Specified number of times the ABR router intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Router <abr_id>: Becomes ABR/Non-ABR Flap. <number> time(s) in <number> second(s)].
```

Example

```
Router 192.168.43.22: Becomes ABR/Non-ABR Flap. 7 times in 30 seconds.
```

ASBR Status Change Alarm

- Alarm on availability change of a specified ASBR router
- Alarm on availability change to any ASBR router (wildcard alarm)

Changes in Status of an ASBR.

This alarm is triggered when an ASBR establishes or loses connectivity with, or discovers new routes in external Autonomous Systems. For example, the ASBR can temporarily lose its connection to an external network and be displayed as an internal router.

For information about the related ASBR Status Flap Alarm, which is a type of ASBR Status Change Alarm, see ASBR Status Flap Alarm on page 8-7.

Alarm States

ASBR Status Change Alarms have the following states:

- **Becomes Available**—Specified number of times the ASBR router became available within the set time period.
- **Becomes Unavailable**—Specified number of times the ASBR router became unavailable within the set time period.
- **Flap**—Specified number of times the ASBR router intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Router <asbr_id>: Becomes [ASBR or Non-ASBR] at least <number> time(s) in <number>
second(s)].
```

Example

```
Router 192.168.43.22: Becomes ASBR at least 4 times in 30 seconds.

Router 192.168.43.22: Becomes Non-ASBR at least 4 times in 30 seconds.
```

ASBR Status Flap Alarm

- Alarm on availability flaps of a specified ASBR router
- Alarm on availability flaps of any ASBR router (wildcard alarm)

Number of Flaps on a Selected Router

The ASBR Status Flap Router Availability Flap Alarm is triggered when an ASBR router intermittently changes its availability on the network. For example, if you issue an ASBR Status Flap Alarm against a router, the alarm is triggered when the ASBR router changes from up to down and back a specified number of times within the set time interval.

ASBR Status Flap Alarms are a subset of ASBR Status Change Alarms. For information about the related ASBR Status Change Alarm, see ASBR Status Change Alarm on page 8-6.

Alarm States

Router Status Flap Alarms have the following state in Alarm Monitor:

Flap—Specified number of times the ASBR router intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Router <asbr_id>: Becomes ASBR/Non-ASBR Flap. <number> time(s) in <number>
second(s)].
```

Example

```
Router 192.168.43.22: Becomes ASBR/Non-ASBR Flap. 7 times in 30 seconds.
```

Router Area Count Change Alarm

Alarm on area count change of a specified router.

- Alarm on area count change of a specified router
- Alarm on area count change of any router (wildcard alarm)

Number of Areas in which a Router is Connected.

Area Count refers to the number of areas in which a specified router has advertised connectivity. This connectivity can be learned only by instrumenting Cisco Service Path Analyzer Listeners in those areas.

The Router Area Count Change Alarm is triggered when a router advertises connectivity in a different number of areas than it advertised previously.

Alarm States

Router Area Count Change Alarms have the following state in Alarm Monitor:

Count Change—Number of times the router changed its advertised area count in the set period of time.

Alarm Syntax

```
[Router <router_id>: at least <number> Area Count change(s) within <number> seconds].
```

Example

```
Router 192.168.43.22: at least 4 Area Count change(s) within 30 seconds.
```

CHAPTER 9

Transit Network Alarms

Transit Network Alarms

Transit Network Alarms notify you of changes in state or configuration of a specified Transit network.

In Alarm Monitor, you can set the following alarms for Transit networks:

Transit Network Availability Change Alarm

Alarm on network availability change of a specified Transit network

- Alarm on availability change of a specified Transit network
- Alarm on availability change to any Transit network (wildcard alarm)

Changes in Availability of a Transit Network.

This alarm is triggered when a Transit network changes in availability affecting routing patterns.

Alarm States

Transit Network Availability Change Alarms have the following states:

- **Becomes Available**—Specified number of times the Transit network became available within the set time period.
- **Becomes Unavailable**—Specified number of times the Transit network became unavailable within the set time period.
- **Flap**—Specified number of times the Transit network intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Transit Network <network_id> in area <area_id> with Route/Prefix <route_id>: at least
<number> change(s) within <number> seconds].
```

Example

```
Transit Network 192.168.40.28/24 in area 0.0.0.2 with Route/Prefix 19.2.51.0/24: at
least 4 change(s) within 60 seconds.
```

Transit Network Availability Flap Alarm

- Alarm on availability flap of a specified Transit network
- Alarm on availability flap to any Transit network (wildcard alarm)

Number of Flaps on a Selected Transit Network

The Transit Network Availability Flap Alarm is triggered when a Transit network intermittently changes its availability on the network. For example, if you issue a Transit Network Availability Flap Alarm against a Transit network, the alarm is triggered when the network changes from up to down and back a specified number of times within the set time interval.

Transit Network Availability Flap Alarms are a subset of Transit Network Availability Change Alarms. For information about the related Transit Network Availability Change Alarm, see Transit Network Availability Change Alarm, page 9-2.

Alarm States

Transit Network Availability Flap Alarms have the following state in Alarm Monitor:

Flap—Specified number of times the Transit network intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Transit Network <network_id> in area <area_id> with Route/Prefix <route_id>: at least
<number> availability flap(s) within <number> seconds].
```

Example

```
Transit Network 192.168.10.20/32 in area 0.0.0.0 with Route/Prefix 19.2.50.0/24: at
least 4 availability flap(s) within 30 seconds.
```

Transit Network Designated Router (DR) Change Alarm

- Alarm on Designated Router (DR) change for a specified Transit network
- Alarm on Designated Router (DR) change for any Transit network

DR Changes for a Transit Network

The Transit Network Designated Router (DR) Change Alarm is triggered when the interface that connects the DR to the network changes. For example, if the DR becomes unavailable and the backup DR takes over the former DR's responsibilities on the network, the Transit Network Designated Router (DR) Change Alarm issues a notification of the change.

Alarm States

Transit Network DR Change Alarms have the following state in Alarm Monitor:

Number of Changes—Specified number of times a change occurred to the DR assigned to the Transit network with the set time period.

Alarm Syntax

```
[Transit Network <network_id> in area <area_id> with Route/Prefix <route_id>: DR
change(s) at least <Number> within <Number> seconds].
```

Example

```
Transit Network 192.168.10.20/32 in area 0.0.0.1 with Route/Prefix 19.2.2.0/24: DR
change(s) at least 3 times within 30 seconds.
```

Transit Network Connected Router Count Change Alarm

- Alarm on connected router count change for a specified Transit network
- Alarm on connected router count change for any Transit network (wildcard alarm)

Number of Connected Routers Changed on a Transit Network

The Transit Network Connected Router Count Change Alarm is triggered when the number of routers connected to a Transit network changes. For example, the Transit Network Connected Router Count Change Alarm notifies you if the number of routers connected to a Transit network changes from five to four, indicating that a router became unavailable on the network.

Alarm States

Transit Network Connected Router Count Change Alarms have the following state in Alarm Monitor:

Number of Changes—Specified number of times the number of connected routers changed within the set time period.

Alarm Syntax

```
[Transit Network <network_id> in area <area_id> with Route/Prefix <route_id>: Router
count changes at least <number> times within <number> seconds].
```

Example

```
Transit Network 192.168.10.20/32 in area 0.0.0.1 with Route/Prefix 19.2.2.0/24: Router
count changes at least 2 times within 30 seconds.
```

Transit Network Designated Router (DR) Interface Change Alarm

- Alarm on Designated Router (DR) Interface change for a specified Transit network
- Alarm on Designated Router (DR) Interface change for any Transit network (wildcard alarm)

DR Changes for Selected Transit Network

The Transit Network Designated Router (DR) Interface Change Alarm is triggered when changes occur to the DR assigned to a Transit network. For example, if the DR becomes unavailable and the backup DR takes over the former DR's responsibilities on the network, the Transit Network Designated Router (DR) Change Alarm issues a notification of the change.

Alarm States

Transit Network DR Interface Change Alarms have the following state in Alarm Monitor:

Number of Changes—Specified number of times the number of connected DR router interfaces changed within the set time period.

Alarm Syntax

```
[Transit Network <network_id> in area <area_id> with Route/Prefix <route_id>: DR
Interfaces changes at least <Number> within <Number> seconds].
```

Example

```
Transit Network 192.168.10.20/32 in area 0.0.0.2 with Route/Prefix 19.2.2.0/24: DR
Interface changes at least 3 times within 30 seconds.
```

CHAPTER 10

Advertisement Alarms

Advertisement Alarms for Stub Routes and External Routes

Advertisement Alarms consist of the following:

Stub Route Advertisement Alarms

The Stub route indicates the destination of a packet in a Stub network. In Alarm Monitor, you can set the following alarms on a Stub route:

Stub Route Availability Change Alarm

- Alarm on availability change to specified Stub route
- Alarm on availability change to any Stub route (wildcard alarm)

Changes in Availability of a Stub Route.

This alarm is triggered when a Stub route is advertised or withdrawn on the network.

Alarm States

Stub Route Availability Change Alarms have the following states:

- **Advertised**—Specified number of times Stub route is advertised within the set time period.
- **Withdrawn**—Specified number of times the Stub route is withdrawn within the set time period.
- **Flap**—Specified number of times the Stub route intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Stub <mask length> Route Advertisement: Source <ip_address> in Area <area_id>, Prefix
<prefix>. [route advertisement | route withdrawal | either] At least <number> changes
within <number> seconds].
```

Example

```
Stub <exact> Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix 20.8.8.3/32.
route advertisement. At least 4 change(s) within 15 seconds.

Stub <exact> Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix 20.8.8.3/32.
route withdrawal. At least 4 change(s) within 15 seconds.

Stub <exact> Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix 20.8.8.3/32.
route advertisement or route withdrawal. At least 4 change(s) within 15 seconds.
```

Stub Route Availability Flap Alarm

- Alarm on availability flaps of a specified Stub route
- Alarm on availability flaps of any Stub route (wildcard alarm)

Number of Flaps on a Selected Router

The Stub Route Availability Flap Alarm is triggered when a Stub route is intermittently withdrawn and re-advertised within the specified time interval.

Alarm States

Stub Route availability Flap Alarms have the following state in Alarm Monitor:

- **Flap**—Specified number of times the Stub route intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Stub <mask length> Route Advertisement: Source <ip_address> in Area <area_id>, Prefix
<prefix>. Route Advertisement Flap. At least <number> flaps within <number> seconds].
```

Example

```
Stub <exact> Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix 20.8.8.3/32.
Route Advertisement Flap. At least 4 flaps within 15 seconds.
```

Stub Route Metric Change Alarm

- Alarm on metric changes of a specified Stub route
- Alarm on metric changes of any Stub route (wildcard alarm)

Changes in Metric of a Stub Route.

This alarm is triggered when a Stub route metric changes value. The Stub route metric provides the cost in traversing the link associated with the Stub route.

Alarm States

Stub Route Metric Change Alarms have the following state in Alarm Monitor:

Metric Change—Specified number of times the Stub route metric changed in the set time period.

Alarm Syntax

```
[Stub Route Advertisement: Source <ip_address> in Area <area_id>, Prefix <prefix>.
Metric Change. At least <number> times within <number> seconds].
```

Example

```
Stub Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix 20.8.8.3/32. Metric
Change. At least 4 times within 15 seconds.
```

External Route Alarms

External routes indicate destinations in networks outside the autonomous system. ASBR's advertise routes to external destinations in Link State Advertisements (LSA's).

In Alarm Monitor, you can set the following types of alarms against External routes:

- External Route Availability Change Alarm on page 10-4
- External Route Availability Flap Alarm on page 10-5
- External Route Metric Change Alarm on page 10-6

External Route Availability Change Alarm

- Alarm on availability change to specified External route
- Alarm on availability change to any External route (wildcard alarm)

Changes in Availability of an External Route.

This alarm is triggered when an External route is withdrawn or advertised on the network.

Alarm States

External Route Availability Change Alarms have the following states:

- **Advertised**—Specified number of times External route is advertised within the set time period.
- **Withdrawn**—Specified number of times the External route is withdrawn within the set time period.
- **Flap**—Specified number of times the External route intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[External <mask length> Route Advertisement: Source <ip_address> in Area <area_id>,
Prefix <prefix>. [route advertisement | route withdrawal | either] At least <number>
changes within <number> seconds].
```

Example

```
External <exact> Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix
20.8.8.3/32. route advertisement. At least 4 change(s) within 15 seconds.

External <exact> Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix
20.8.8.3/32. route withdrawal. At least 4 change(s) within 15 seconds.

External <exact> Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix
20.8.8.3/32. route advertisement or route withdrawal. At least 4 change(s) within 15
seconds.
```

External Route Availability Flap Alarm

- Alarm on availability flaps of a specified External route
- Alarm on availability flaps of any External route (wildcard alarm)

Number of Flaps on a Selected External Route

The External Route Availability Flap Alarm is triggered when an External route is intermittently withdrawn and re-advertised on the network within a specified time interval.

External Route Availability Flap Alarms are a subset of External Route Availability Change Alarms. See External Route Availability Change Alarm on page 10-4.

Alarm States

External Route Availability Flap Alarms have the following state in Alarm Monitor:

Flap—Specified number of times the External route intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[External <mask length> Route Advertisement: Source <ip_address> in Area <area_id>,
Prefix <prefix>. Route Advertisement Flap. At least <number> flaps within <number>
seconds].
```

Example

```
External <exact> Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix
20.8.8.3/32. Route Advertisement Flap. At least 4 flaps within 15 seconds.
```

External Route Metric Change Alarm

- Alarm on metric changes of a specified External route
- Alarm on metric changes of any External route (wildcard alarm)

Changes in Metric of an External Route.

This alarm is triggered when an External route metric changes value. The External route metric provides the cost in traversing the link toward the destination in the External network.

Alarm States

External Route Metric Change Alarms have the following state in Alarm Monitor:

Metric Change—Specified number of times the External route metric changed in the set time period.

Alarm Syntax

```
[External Route Advertisement: Source <ip_address> in Area <area_id>, Prefix <prefix>.
Metric Change. At least <number> times within <number> seconds].
```

Example

```
External Route Advertisement: Source 20.0.0.3 in Area 0.0.0.1, Prefix 20.8.8.3/32.
Metric Change. At least 4 times within 15 seconds.
```

CHAPTER 11

Route Alarms

OSPF Route Alarms consist of the following:

Core Route Alarms

OSPF Core Route Alarms notify you of changes to an OSPF Core route. OSPF Core Route Alarms include:

OSPF Core Route Addition Alarm

Alarm on addition of an OSPF Core route.

Addition of an OSPF Core Route

This alarm is triggered when a new OSPF Core route is discovered on the network.

Alarm States

OSPF Core Route Addition Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Advertised**.

- **Advertised**—Specified number of times the Core route is advertised within the set time period.
- **Withdrawn**—Specified number of times the Core route is withdrawn within the set time period.
- **Flap**—Specified number of times the Core route is intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Core <mask length> Route:, Prefix <prefix>. Route Advertisement. At least <number>
changes within <number> seconds].
```

Example

```
Core <greater mask length> Route:, Prefix 30.8.8.3/32. Route Advertisement. At least 3
times within 30 seconds.
```

OSPF Core Route Withdrawal Alarm

Alarm on withdrawal of an OSPF Core route.

Withdrawal of an OSPF Core Route

This alarm is triggered when a known OSPF Core route is withdrawn from the network.

Alarm States

OSPF Core Route Withdrawal Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Withdrawn**.

- **Advertised**—Specified number of times the Core route is withdrawn within the set time period.
- **Withdrawn**—Specified number of times the Core route is withdrawn within the set time period.
- **Flap**—Specified number of times the Core route is intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Core <mask length> Route:, Prefix <prefix>. Route Withdrawal. At least <number>
changes within <number> seconds].
```

Example

```
Core <greater mask length> Route:, Prefix 30.8.8.3/32. Route Withdrawal. At least 3
times within 30 seconds.
```

OSPF Core Route Flap Alarm

Alarm on an OSPF Core route flap

Flap on an OSPF Core Route

This alarm is triggered when a known OSPF Core route intermittently changes its availability on the network.

Alarm States

OSPF Core Route Flap Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Flap**.

- **Advertised**—Specified number of times the Core route is withdrawn within the set time period.
- **Withdrawn**—Specified number of times the Core route is withdrawn within the set time period.
- **Flap**—Specified number of times the Core route is intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Core <mask length> Route:, Prefix <prefix>. Route Advertisement Flap. At least
<number> flaps within <number> seconds].
```

Example

```
Core <lesser mask length> Route:, Prefix 30.8.8.3/32. Route Advertisement Flap. At
least 3 flaps within 30 seconds.
```

OSPF Core Route Redundancy Alarm

Alarm on OSPF Core route redundancy.

Redundancy on an OSPF Core Route

This alarm is triggered when a known OSPF Core route becomes redundant or non-redundant. A route is redundant when there is more than one way to reach the destination of the route.

Alarm States

OSPF Core Route Redundancy Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Becomes Redundant** or **Becomes Non-Redundant.**

- **Becomes Redundant**—Specified number of times the route becomes redundant within the set time period.
- **Becomes Non-Redundant**—Specified number of times the route becomes non-redundant within the set time period.
- **Flap**—Specified number of times the route intermittently changes redundancy status within the set time period.

Alarm Syntax

```
[Core Route:, Prefix <prefix>. Becomes [redundant | non-redundant | either]. At least
<number> times within <number> seconds].
```

Example

```
Core Route:, Prefix 30.8.8.3/32. Becomes redundant. At least 3 times within 30
seconds.

Core Route:, Prefix 30.8.8.3/32. Becomes non-redundant. At least 3 times within 30
seconds.

Core Route:, Prefix 30.8.8.3/32. Becomes non-redundant or redundant. At least 3 times
within 30 seconds.
```

OSPF Core Route Redundancy Flap Alarm

Alarm on availability flaps of an OSPF Core route redundancy.

Flap Redundancy on an OSPF Core Route

This alarm is triggered when an OSPF Core Route intermittently changes availability, for example, from Redundant to Non-redundant, in the specified time period.

Alarm States

OSPF Core Route Redundancy Flap Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Flap**.

- **Becomes Redundant**—Specified number of times the route becomes redundant within the set time period.
- **Becomes Non-Redundant—**Specified number of times the route becomes non-redundant within the set time period.
- **Flap**—Specified number of times the route intermittently changes redundancy status within the set time period.

Alarm Syntax

```
[Core Route:, Prefix <prefix>. Redundancy Flap. At least <number> flaps within
<number> seconds].
```

Example

```
Core Route:, Prefix 30.8.8.3/32. Redundancy Flap. At least 3 flaps within 30 seconds.
```

External Route Alarms

OSPF External Route Alarms notify you of changes to an OSPF External route. OSPF External Route Alarms include:

OSPF External Route Addition Alarm

Alarm on addition of an OSPF External route.

Addition of an OSPF External Route

This alarm is triggered when a new OSPF External route is discovered on the network.

Alarm States

OSPF External Route Addition Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Advertised**.

- **Advertised**—Specified number of times the External route is advertised within the set time period.
- **Withdrawn**—Specified number of times the External route is withdrawn within the set time period.
- **Flap**—Specified number of times the External route is intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[External <mask length> Route:, Prefix <prefix>. Route Advertisement. At least
<number> changes within <number> seconds].
```

Example

```
External <greater mask length> Route:, Prefix 30.8.8.3/32. Route Advertisement. At
least 3 times within 30 seconds.
```

OSPF External Route Withdrawal Alarm

Alarm on withdrawal of an OSPF External route.

Withdrawal of an OSPF External Route

This alarm is triggered when a known OSPF External route is withdrawn from the network.

Alarm States

OSPF External Route Withdrawal Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Withdrawn**.

- **Advertised**—Specified number of times the External route is withdrawn within the set time period.
- **Withdrawn**—Specified number of times the External route is withdrawn within the set time period.
- **Flap**—Specified number of times the External route is intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[External <mask length> Route:, Prefix <prefix>. Route Withdrawal. At least <number>
changes within <number> seconds].
```

Example

```
External <greater mask length> Route:, Prefix 30.8.8.3/32. Route Withdrawal. At least
3 times within 30 seconds.
```

OSPF External Route Flap Alarm

Alarm on an OSPF External route flap.

Flap on an OSPF External Route

This alarm is triggered when a known OSPF External route intermittently changes its availability on the network.

Alarm States

OSPF External Route Flap Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Flap**.

- **Advertised**—Specified number of times the External route is withdrawn within the set time period.
- **Withdrawn**—Specified number of times the External route is withdrawn within the set time period.
- **Flap**—Specified number of times the External route is intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[External <mask length> Route:, Prefix <prefix>. Route Advertisement Flap. At least
<number> flaps within <number> seconds].
```

Example

```
External <lesser mask length> Route:, Prefix 30.8.8.3/32. Route Advertisement Flap. At
least 3 flaps within 30 seconds.
```

OSPF External Route Redundancy Alarm

Alarm on OSPF External route redundancy

Redundancy on an OSPF External Route

This alarm is triggered when a known OSPF External route becomes redundant or non-redundant. A route is redundant when there is more than one way to reach the destination of the route.

Alarm States

OSPF External Route Redundancy Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Becomes Redundant** or **Becomes Non-Redundant**.

- **Becomes Redundant**—Specified number of times the route becomes redundant within the set time period.
- **Becomes Non-Redundant**—Specified number of times the route becomes non-redundant within the set time period.
- **Flap**—Specified number of times the route intermittently changes redundancy status within the set time period.

Alarm Syntax

```
[External Route:, Prefix <prefix>. Becomes [redundant | non-redundant | either]. At
least <number> times within <number> seconds].
```

Example

```
External Route:, Prefix 30.8.8.3/32. Becomes redundant. At least 3 times within 30
seconds.

External Route:, Prefix 30.8.8.3/32. Becomes non-redundant. At least 3 times within 30
seconds.

External Route:, Prefix 30.8.8.3/32. Becomes non-redundant or redundant. At least 3
times within 30 seconds.
```

OSPF External Route Redundancy Flap Alarm

Alarm on availability flaps of an OSPF External route redundancy.

Flap Redundancy on an OSPF External Route

This alarm is triggered when an OSPF External Route intermittently changes availability, for example, from Redundant to Non-redundant, in the specified time period.

Alarm States

OSPF External Route Redundancy Flap Alarms have the following states in the Alarm Monitor. For this type of alarm, you must select **Flap**.

- **Becomes Redundant**—Specified number of times the route becomes redundant within the set time period.
- **Becomes Non-Redundant**—Specified number of times the route becomes non-redundant within the set time period.
- **Flap**—Specified number of times the route intermittently changes redundancy status within the set time period.

Alarm Syntax

```
[External Route:, Prefix <prefix>. Redundancy Flap. At least <number> flaps within
<number> seconds].
```

Example

```
External Route:, Prefix 30.8.8.3/32. Redundancy Flap. At least 3 flaps within 30
seconds.
```

CHAPTER 12

Threshold Alarms

Threshold alarms notify you of when the system perceived (or baseline) behavior of your network deviates from the norm by a certain percentage defined by the user. For OSPF alarms, there are two main types of threshold alarms:

Entity Rate

This alarm is triggered when the number of entities becomes more or less than the defined percentage of the threshold value.

Event Rate

This alarm is triggered when the rate of events exceeds the threshold by more than the defined percentage.

You can set both Entity and Event Rate Threshold alarms for:

- Routers
- External Routes
- Stub Routes
- Transit Networks
- Numbered Point-to-Point Interfaces
- Unnumbered Point-to-Point Interfaces
- Transit Interfaces

For additional information regarding OSPF threshold alarms, see Chapter 8, Setting and Monitoring Alarms in the *Cisco Service Path Analyzer User Guide*.

Entity Count Threshold Alarm

Alarm States

Entity Count Threshold Alarms have the following state:

Percentage Change—Detection of threshold percentage rate of change in number of entities.

Alarm Syntax

```
[Detection of Threshold Rate of Change in <number> {router | external route | stub
route | transit network | numbered P2P interface | unnumbered P2P interface | transit
interface} Entities].
```

Example

```
Detection of Threshold Rate of Change in 50 Router Entities.

Detection of Threshold Rate of Change in 70 External Route Entities.

Detection of Threshold Rate of Change in 9 Stub Route Entities.

Detection of Threshold Rate of Change in 20 Transit Network Entities.

Detection of Threshold Rate of Change in 800 Numbered P2P Interface Entities.

Detection of Threshold Rate of Change in 200 Unnumbered P2P Interface Entities.

Detection of Threshold Rate of Change in 47 Transit Interface Entities.
```

Event Rate Threshold Alarm

Alarm States

Event Rate Threshold Alarms have the following state:

Percentage Change—Detection of threshold percentage rate of change in number of events.

Alarm Syntax

```
[Detection of Threshold Rate of Change in Number of {router | external route | stub
route | transit network | numbered P2P interface | unnumbered P2P interface | transit
interface} Events].
```

Example

```
Detection of Threshold Rate of Change in 50 Router Events.

Detection of Threshold Rate of Change in 70 External Route Events.

Detection of Threshold Rate of Change in 9 Stub Route Events.

Detection of Threshold Rate of Change in 77 Transit Network Events.

Detection of Threshold Rate of Change in 200 Numbered P2P Interface Events.

Detection of Threshold Rate of Change in 89 Unnumbered P2P Interface Events.

Detection of Threshold Rate of Change in 58 Transit Interface Events.
```

CHAPTER 13

Error Alarms

Error Alarms for Interface Conflict Errors

Interface conflicts occur when the same IP address is assigned to more than one network interface. Error alarms are triggered when an interface conflict error is detected or resolved.

Alarm Manager informs about the following types of Error alarms:

Interface Conflict Error Detection Alarm

Alarm on the detection of a conflict.

Alarm States

No settings are required except for severity.

Alarm Syntax

```
[Detection of Interface Address Conflict].
```

Example

```
Detection of Interface Address Conflict.
```

Interface Conflict Error Resolution Alarm

Alarm on the resolution of a conflict.

Alarm States

No settings are required except for severity.

Alarm Syntax

```
[Resolution of Interface Address Conflict].
```

Example

```
Resolution of Interface Address Conflict.
```

CHAPTER 14

Service and Service Path Alarms

The term, service, refers to the collections of service paths over which data is transported from applications you provide on your network. Your business relies on the availability and reliability of services. For detailed information about setting service alarms, see Chapter 8, Setting and Monitoring Alarms in the *Cisco Service Path Analyzer User Guide*.

You can set the following alarms:

Unicast Service Alarms

From Alarm Monitor, you can set an alarm on a specific unicast service to notify you when changes occur.

When a unicast service alarm is triggered, it provides information about the events that triggered the alarm, enabling you to quickly identify the cause of changes to a service.

Alarm Monitor informs about the following types of service alarms:

Unicast Service Availability Change Alarm

The Unicast Service Availability Change Alarm monitors the availability of a unicast service or services on your network and notifies you if the availability changes.

For information about the Unicast Service Availability Flap Alarm, which is a type of Service Availability Change Alarm, see Unicast Service Availability Flap Alarm on page 14-3.

Instances

Alarm on availability change to a specified service or services.

Alarm States

Unicast Service Availability Change Alarms have the following states, which for this type of alarm should be set to **Becomes Available** or **Becomes Unavailable**.

- **Becomes Available—**Specified number of times the service became available within the set time period.
- **Becomes Unavailable—**Specified number of times the service became unavailable within the set time period.
- **Flap**—Specified number of times the service intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Service <name>: becomes [available | unavailable | either] at least <number> changes
within <number> seconds].
```

Example

```
Service ERP: becomes available at least 3 times in 15 seconds.

Service ERP: becomes unavailable at least 3 times in 15 seconds.

Service ERP: becomes available or unavailable at least 3 times in 15 seconds.
```

Unicast Service Availability Flap Alarm

Alarm on availability flaps of a specified unicast service or services.

Number of Flaps on a Selected Service

The Unicast Service Availability Flap Alarm is triggered when a service path of a unicast service intermittently changes availability within the specified time period.

Unicast Service Availability Flap Alarms are a subset of Unicast Service Availability Change Alarms. See Unicast Service Availability Change Alarm on page 14-2.

Alarm States

Service Availability Flap Alarms have the following state:

Flap—Specified number of times the service intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Service <name>: at least <number> available flap(s) within <number> seconds].
```

Example

```
Service ERP: at least 4 available flap(s) within 30 seconds.
```

Unicast Service Conformity Change Alarm

Alarm on conformity change to a unicast service or services.

Change in Conformity of a Service

The Unicast Service Conformity Change Alarm is triggered when a unicast service deviates from the set baseline within the set time period. A service is considered to be non-conforming when any of its associated service paths deviate from the set baseline.

Conformance is a binary state that is calculated as the Boolean AND of the conformance of all service paths associated with a service.

Alarm States

Unicast Service Conformity Change Alarms have the following states, which for this type of alarm you should select **Becomes Conformant** or **Becomes Deviant**.

- **Becomes Conformant—**Specified number of times the service becomes conformant within the set time period.
- **Becomes Deviant—**Specified number of times the service becomes deviant within the set time period.
- **Flap**—Specified number of times the service changed intermittently, indicating a flap, within the set time period.

For information about the Unicast Service Conformity Flap Alarm, which is a type of Service Conformity Change Alarm, see Unicast Service Conformity Flap Alarm on page 14-5.

Alarm Syntax

```
[Service <Name>: becomes [conformant | deviant | either] at least <number> changes
within <number> seconds].
```

Example

```
Service ERP: becomes conformant at least 3 times in 15 seconds.

Service ERP: becomes deviant at least 3 times in 15 seconds.

Service ERP: becomes conformant or non-conformant at least 3 times in 15 seconds.
```

Unicast Service Conformity Flap Alarm

Alarm on conformity flaps of a unicast service or services.

Number of Flaps on a Selected Service or any Service

The Unicast Service Conformity Flap Alarm is triggered when any service path of a service intermittently deviates from the set baseline a specified number of times within a set interval of time. The intermittent change is referred to as a conformity flap.

Unicast Service Conformity Flap Alarms are a subset of Unicast Service Conformity Change Alarms. For information see Unicast Service Conformity Change Alarm on page 14-4.

Alarm States

Unicast Service Conformity Flap Alarms have the following state:

Flap—Specified number of times the service changed intermittently, indicating a flap, within the set time period.

Alarm Syntax

```
[Service <name>: at least <number> conforming flap(s) within <number> seconds].
```

Example

```
Service ERP: at least 4 conforming flap(s) within 30 seconds.
```

Unicast Service Path Alarms

The term, *service path*, refers to the direction that data flows through your network from a source to a destination router or host. For detailed information about setting alarms on unicast service paths, see Chapter 8, Setting and Monitoring Alarms in the *Cisco Service Path Analyzer User Guide*.

You can set an alarm on a specific unicast service path to notify you when changes occur to that service path.

When a unicast service path alarm is triggered, it provides information about the events that triggered the alarm, enabling you to quickly identify changes to a service path.

Alarm Monitor informs about the following types of unicast service path alarms:

- Unicast Service Path Availability Change Alarm on page 14-7
- Unicast Service Path Availability Flap Alarm on page 14-8
- Unicast Service Path Conformity Change Alarm on page 14-9
- Unicast Service Path Conformity Flap Alarm on page 14-10
- Unicast Service Path Loop Alarm on page 14-11

Unicast Service Path Availability Change Alarm

Alarm on availability change to a specified unicast service path or paths.

Change in Availability of a Selected Service or any Service

The Unicast Service Availability Change Alarm is triggered when a service path of a unicast service changes availability in the specified time period.

Alarm States

Unicast Service Path Availability Change Alarms have the following states which for this type of alarm you should select **Becomes Available** or **Becomes Unavailable**.

- **Becomes Available—**Specified number of times the service path became available within the set time period.
- **Becomes Unavailable—**Specified number of times the service path became unavailable within the set time period.
- **Flap**—Specified number of times the service path intermittently changed availability, indicating a flap, within the set time period.

For information about the Unicast Service Path Availability Flap Alarm, which is a type of Service Path Availability Change Alarm, see Unicast Service Path Availability Flap Alarm on page 14-8.

Alarm Syntax

```
[Service Path <name>, Service <name>. becomes [available | unavailable | either] at
least <number> changes within <number> seconds].
```

Example

```
Service Path PaloAlto_To_NYC, Service ERP. becomes available at least 3 times in 15
seconds.

Service Path PaloAlto_To_NYC, Service ERP. becomes unavailable at least 3 times in 15
seconds.

Service Path PaloAlto_To_NYC, Service ERP. becomes available or unavailable at least 3
times in 15 seconds.
```

Unicast Service Path Availability Flap Alarm

Alarm on availability flaps of a specified service path or paths.

Number of Flaps on a Selected Service Path or any Service Paths

The Unicast Service Availability Flap Alarm is triggered when a service path of a unicast service intermittently changes availability in the specified time period.

Unicast Service Path Availability Flap Alarms are a subset of Unicast Service Path Availability Change Alarms. For information about the related Service Path Availability Change Alarm, see Unicast Service Path Availability Change Alarm on page 14-7.

Alarm States

Unicast Service Path Availability Flap Alarms have the following state:

Flap—Specified number of times the service path changed intermittently, indicating a flap, within the set time period.

Alarm Syntax

```
[Any Service Path: <name>, Service <name>. at least <number> available flap(s) within
<number> seconds].
```

Example

```
Any Service Path: PaloAlto_To_NYC, Service ERP. at least 4 available flap(s) within 30
seconds.
```

Unicast Service Path Conformity Change Alarm

Alarm on conformity change to a unicast service path or paths.

Change in Conformity of a Service

The Service Path Conformity Change Alarm is triggered when a targeted service path deviates from the set baseline at least once within the specified time period. A service path is considered to be non-conforming when it deviates from the set baseline.

Conformance is a binary state that is calculated as the Boolean AND of the conformance of all service paths associated with a service.

Alarm States

Unicast Service Path Conformity Change Alarms have the following states, which for this type of alarm you should select **Becomes Conformant** or **Becomes Deviant**.

- **Becomes Conformant—**Specified number of times the service path becomes conformant within the set time period.
- **Becomes Deviant—**Specified number of times the service path becomes deviant within the set time period.
- **Flap**—Specified number of times the service path changed intermittently, indicating a flap, within the set time period.

For information about the Unicast Service Path Conformity Flap Alarm, which is a type of Unicast Service Path Conformity Change Alarm, see Unicast Service Path Conformity Flap Alarm on page 14-10.

Alarm Syntax

```
[Any Service Path: <name>, Service <name>. Becomes [conformant | deviant| either] at
least <number> changes within <number> seconds].
```

Example

```
Service Path PaloAlto_To_NYC, Service ERP. Becomes conformant at least 3 times in 15
seconds.

Service Path PaloAlto_To_NYC, Service ERP. Becomes deviant at least 3 times in 15
seconds.

Service Path PaloAlto_To_NYC, Service ERP. Becomes conformant or deviant at least 3
times in 15 seconds.
```

Unicast Service Path Conformity Flap Alarm

Alarm on conformity flaps of a unicast service path or paths.

Number of Conformity Flaps on a Selected Service Path or any Service Path

The Unicast Service Path Conformity Flap Alarm is triggered when a service path intermittently deviates from the set baseline a specified number of times within the specified time period.

Alarm States

Service Path Conformity Flap Alarms have the following state:

Flap—Specified number of times the service path intermittently changed conformance, indicating a flap, in the set time period.

Unicast Service Path Conformity Flap Alarms are a subset of Unicast Service Path Conformity Change Alarms. For information about the related Service Conformity Change Alarm, see Unicast Service Path Conformity Change Alarm on page 14-9.

Alarm Syntax

```
[Any Service Path: <name>, Service <name>. Conformity Flap. At least <Number>
conforming flap(s) within <Number> seconds].
```

Example

```
Service Path PaloAlto_To_NYC, Service ERP. Conformity Flap. At least 4 conforming
flap(s) within 30 seconds.
```

Unicast Service Path Loop Alarm

Alarm on detection of a loop in a unicast service path or paths.

Number of loops on a selected service path or any service path

The Service Path Loop Alarm is triggered when a loop in service path is detected within the specified time period.

Alarm States

Alarm is either off or on. Only the Alarm Severity, Count, and Time Window settings are required.

Alarm Syntax

```
[Any Service Path: <name>, Service <name>. Detection of Loop in Service Path. At least
<Number> conforming flap(s) within <Number> seconds].
```

Example

```
Service Path PaloAlto_To_NYC, Service ERP. Detection of Loop in Service Path. At least
4 times within 30 seconds.
```

Multicast Service Alarms

From Alarm Monitor, you can set an alarm on a specific multicast service to notify you when changes occur.

When a multicast service alarm is triggered, it provides information about the events that triggered the alarm, enabling you to quickly identify the cause of changes to a service.

Alarm Monitor informs about the following types of service alarms:

Multicast Service Availability Change Alarm

The Multicast Service Availability Change Alarm monitors the availability of a multicast service on your network and notifies you if the availability changes.

A subset of the Multicast Service Availability Change Alarm is the Multicast Service Availability Flap Alarm, which notifies you when a flap has occurred on a selected service.

Instances

Alarm on availability change to a specified multicast service or services.

Alarm States

Multicast Service Availability Change Alarms have the following states, which for this type of alarm you should select **Becomes Available** or **Becomes Unavailable**.

- **Becomes Available—**Specified number of times the service became available within the set time period.
- **Becomes Unavailable—**Specified number of times the service became unavailable within the set time period.
- **Flap**—Specified number of times the service intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[Multicast Service <name>: becomes [available | unavailable | either] at least
<number> changes within <number> seconds].
```

Example

```
Multicast Service ERP: becomes available at least 3 times in 15 seconds.

Multicast Service ERP: becomes unavailable at least 3 times in 15 seconds.

Multicast Service ERP: becomes available or unavailable at least 3 times in 15
seconds.
```

Multicast Service Availability Flap Alarm

Alarm on availability flaps of a multicast service or services.

Number of Flaps on a Selected Service or any Service

The Multicast Service Availability Flap Alarm is triggered when a service path of a multicast service intermittently changes availability.

Alarm States

Multicast Service Availability Flap Alarms have the following state:

Flap—Specified number of times the service intermittently changed availability, indicating a flap, in the set time period.

Multicast Service Availability Flap Alarms are a subset of Multicast Service Availability Change Alarms. For information about the related Multicast Service Availability Change Alarm, see Multicast Service Availability Change Alarm on page 14-13.

Alarm Syntax

```
[Service <name>: at least <number> available flap(s) within <number> seconds].
```

Example

```
Service ERP: at least 4 available flap(s) within 30 seconds.
```

Multicast Service Conformity Change Alarm

Alarm on conformity change to a multicast service or services.

Change in Conformity of a Selected Service

The Multicast Service Conformity Change Alarm is triggered when a service deviates from the set baseline at least once in the specified time period. A multicast service is considered to be non-conforming when any of its associated service paths deviates from the set baseline.

Alarm States

Multicast Service Conformity Change Alarms have the following states, which for this type of alarm you should select **Becomes Conformant** or **Becomes Deviant**.

- **Becomes Conformant—**Specified number of times the service becomes conformant within the set time period.
- **Becomes Deviant—**Specified number of times the service becomes deviant within the set time period.
- **Flap**—Specified number of times the service changed intermittently, indicating a flap, within the set time period.

For information about the Unicast Service Conformity Flap Alarm, which is a type of Service Conformity Change Alarm, see Multicast Service Conformity Flap Alarm on page 14-16.

Alarm Syntax

```
[Multicast Service <Name>: becomes [conformant | deviant | either] at least <number>
changes within <number> seconds].
```

Example

```
Multicast Service ERP: becomes conformant at least 3 times in 15 seconds.

Multicast Service ERP: becomes deviant at least 3 times in 15 seconds.

Multicast Service ERP: becomes conformant or deviant at least 3 times in 15 seconds.
```

Multicast Service Conformity Flap Alarm

Alarm on conformity flaps of a multicast service or services.

Number of Flaps on a Selected Service or any Service

The Multicast Service Conformity Flap Alarm is triggered when any service path of a multicast service intermittently deviates from the set baseline a specified number of times within a set interval of time.

Multicast Service Conformity Flap Alarms are a subset of Multicast Service Conformity Change Alarms. For information about the related Multicast Service Conformity Change Alarm, see Multicast Service Conformity Change Alarm on page 14-15.

Alarm States

Service Conformity Flap Alarms have the following state:

Flap—Specified number of times the service intermittently changed conformance, indicating a flap, within the set time period.

Alarm Syntax

```
[Multicast Service <name>: at least <number> conforming flap(s) within <number>
seconds].
```

Example

```
Multicast Service ERP: at least 4 conforming flap(s) within 30 seconds.
```

Multicast Service Redundancy Change Alarm

The Multicast Service Redundancy Change Alarm alarms on a multicast service redundancy.

Redundancy on a Multicast Service

This alarm is triggered when a known multicast service becomes redundant or non-redundant. A multicast service is considered redundant when there is more than one path to a given leaf.

Alarm States

Multicast Service Redundancy Alarms have the following states, which for this type of alarm you should select **Becomes Redundant** or **Becomes Non-Redundant**.

- **Becomes Redundant—**Specified number of times the service becomes redundant within the set time period.
- **Becomes Non-Redundant**—Specified number of times the service becomes non-redundant within the set time period.
- **Flap**—Specified number of times the service intermittently changes redundancy status within the set time period.

Alarm Syntax

```
[Multicast Service <name>: Becomes [redundant | non-redundant | either]. At least
<number> times within <number> seconds].
```

Example

```
[Multicast Service <name>. Becomes redundant. At least 3 times within 30 seconds].
[Multicast Service <name>. Becomes non-redundant. At least 3 times within 30 seconds].
```

Multicast Service Redundancy Flap Alarm

Alarm on availability flaps of a multicast service redundancy.

Flap Redundancy on a Multicast Service

This alarm is triggered when a multicast service intermittently changes from Redundant to Non-redundant, in the specified time period.

Alarm States

Multicast Service Redundancy Flap Alarms have the following state:

Flap—Specified number of times the service intermittently changes redundancy status within the set time period.

Alarm Syntax

```
[Multicast Service <name>. Redundancy Flap. At least <number> flaps within <number>
seconds].
```

Example

```
Multicast Service Movie1. Redundancy Flap. At least 3 flaps within 30 seconds.
```

SSM Multicast Group Alarms

Cisco Service Path Analyzer lets you define SSM Service groups using the Multicast Group Creation Wizard. An SSM Service Group is created by defining:

- Multicast Group Name
- Multicast Group Address
- Source IP Address
- Recipient's AS or domain
- Individual recipients (leaf routers)

For more information on creating SSM Multicast Groups, see Creating Multicast Services and Related SSM Multicast Groups, in Chapter 3 of the *Cisco Service Path Analyzer User Guide*.

You can set an alarm on an SSM Multicast Service group or groups to notify you when changes occur to any of the leaf routers within the group.

Note Source Specific Multicast (SSM) is one method of implementing multicasting. In SSM, packets are forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created.

When a SSM Multicast Group Alarm is triggered, it provides information about the events that triggered the alarm, enabling you to identify how many leaf routers have been affected. This information is displayed in the Alarm Trigger Log. You can identify the addresses of the specific routers involved using the Service Monitor. For more information, see Chapter 3: Monitoring Unicast and Multicast Service in the *Cisco Service Path Analyzer User Guide.*

For detailed information about setting alarms on SSM Multicast groups, see Chapter 8, Setting and Monitoring Alarms in the *Cisco Service Path Analyzer User Guide*.

Alarm Monitor informs about the following types of SSM Multicast Group alarms:

- SSM Multicast Group Availability Alarm on page 14-20
- SSM Multicast Group Availability Flap Alarm on page 14-21
- SSM Multicast Group Conformity Alarm on page 14-22
- SSM Multicast Group Conformity Flap Alarm on page 14-23

SSM Multicast Group Availability Alarm

The SSM Multicast Group Availability Alarm monitors the availability of an SSM Multicast Group on your network and notifies you if the availability changes.

A subset of the SSM Multicast Group Availability Alarm is the SSM Multicast Group Availability Flap Alarm, which notifies you when a flap has occurred on a selected service.

Instances

Alarm on availability change to a specified SSM multicast group or groups.

Alarm States

SSM Multicast Group Availability Alarms have the following states, which for this type of alarm you should select **Becomes Available** or **Becomes Unavailable**.

- **Becomes Available—**Specified number of times the group became available within the set time period.
- **Becomes Unavailable—**Specified number of times the group became unavailable within the set time period.
- **Flap**—Specified number of times the group intermittently changed availability, indicating a flap, within the set time period.

Alarm Syntax

```
[SSM Multicast Group <name>: becomes [available | unavailable | either] at least
<number> changes within <number> seconds].
```

Example

```
SSM Multicast Group ERP: becomes available at least 3 times in 15 seconds.

SSM Multicast Group ERP: becomes unavailable at least 3 times in 15 seconds.
```

SSM Multicast Group Availability Flap Alarm

Alarm on availability flaps of a SSM Multicast group or groups.

Number of Flaps on a Selected Group or any Group

The SSM Multicast Group Availability Flap Alarm is triggered when an SSM Multicast group intermittently changes availability.

Alarm States

SSM Multicast Group Availability Flap Alarms have the following state:

Flap—Specified number of times the group intermittently changed availability, indicating a flap, in the set time period.

SSM Multicast Group Availability Flap Alarms are a subset of SSM Multicast Group Availability Change Alarms. For more information, see SSM Multicast Group Availability Alarm on page 14-20.

Alarm Syntax

```
[SSM Service Group <name>: at least <number> available flap(s) within <number>
seconds].
```

Example

```
SSM Service Group ERP: at least 4 available flap(s) within 30 seconds.
```

SSM Multicast Group Conformity Alarm

Alarm on conformity change to a SSM Multicast group or groups.

Change in Conformity of a Selected Group or Groups

The SSM Multicast Group Conformity Alarm is triggered when a group deviates from the set baseline at least once in the specified time period. An SSM Multicast Group is considered to be non-conforming when it deviates from the baseline you set for it.

Alarm States

SSM Multicast Group Conformity Alarms have the following states, which for this type of alarm you should select **Becomes Conformant** or **Becomes Deviant**.

- **Becomes Conformant—**Specified number of times the group becomes conformant within the set time period.
- **Becomes Deviant—**Specified number of times the group becomes deviant within the set time period.
- **Flap**—Specified number of times the group changed intermittently, indicating a flap, within the set time period.

For information about the Unicast Service Conformity Flap Alarm, which is a type of Service Conformity Change Alarm, see Multicast Service Conformity Flap Alarm on page 14-16.

Alarm Syntax

```
[MSSM Multicast Group <Name>: becomes [conformant | deviant | either] at least
<number> changes within <number> seconds].
```

Example

```
SSM Multicast Group ERP: becomes conformant at least 3 times in 15 seconds.

SSM Multicast Group ERP: becomes deviant at least 3 times in 15 seconds.

SSM Multicast Group ERP: becomes conformant or deviant at least 3 times in 15 seconds.
```

SSM Multicast Group Conformity Flap Alarm

Alarm on conformity flaps of an SSM Multicast group or groups.

Number of flaps on a selected group or any group

The SSM Multicast Group Conformity Flap Alarm is triggered when any SSM Multicast group intermittently deviates from the set baseline a specified number of times within a set interval of time.

SSM Multicast Group Conformity Flap Alarms are a subset of SSM Multicast Group Conformity Alarms. For more information, see SSM Multicast Group Conformity Alarm on page 14-22.

Alarm States

SSM Multicast Group Conformity Flap Alarms have the following state:

Flap—Specified number of times the group intermittently changed conformance, indicating a flap, within the set time period.

Alarm Syntax

```
[SSM Multicast Group <name>: at least <number> conforming flap(s) within <number>
seconds].
```

Example

```
SSM Multicast Group ERP: at least 4 conforming flap(s) within 30 seconds.
```

CHAPTER 15

Wildcard Alarms

Wildcard alarms allow you to set alarms that are triggered in response to any change in advertisements, routes and thresholds.

The following sections describe wildcard alarms that pertain to any change to any *collective* type of network element.

Wildcard alarms that alert to any type of change to any *specific* network element are described in Chapter 6, Setting and Monitoring Alarms, of the *Cisco Service Path Analyzer User Guide* and in the chapters of this reference manual.

Cisco Service Path Analyzer provides the following types of wildcard alarms:

BGP Advertisement Wildcard Alarms

The BGP Advertisement Wildcard Alarms consist of the following:

BGP Advertisement Availability Change Wildcard Alarm

[Any BGP Advertisement Availability Change: any single Availability change].

BGP Advertisement Availability Flap Wildcard Alarm

[Excessive Availability Flapping on Any BGP Advertisement: at least <number> Availability flap(s) within <number> seconds].

BGP Advertisement AS Path Change Wildcard Alarm

[Any BGP Advertisement AS Path Change: any single AS Path change].

BGP Advertisement Next Hop Change Wildcard Alarm

[Any BGP Advertisement Next Hop Change: any single Next Hop change].

BGP Advertisement Local Preference Change Wildcard Alarm

[Any BGP Advertisement Local Preference Change: any single Local Preference change].

BGP Advertisement Multi-Exit Discriminator (MED) Attribute Change Wildcard Alarm

[Any BGP Advertisement MED Change: any single MED change].

BGP Advertisement Community Attribute Change Wildcard Alarm

[Any BGP Advertisement Community Attribute Change: any single Community Attribute change].

BGP Advertisement Other Path Change Wildcard Alarm

[Any BGP Advertisement Other Path Change: any single Other Path change].

BGP Advertisement Any Change Wildcard Alarm

[Any BGP Advertisement Any Change: any single change].

BGP Threshold per Router Wildcard Alarms

The Threshold per Router Wildcard Alarms consist of the following:

Percent Threshold Change per Route Change Wildcard Alarm

[BGP Threshold: Rate of Change in Number of Routes for Router: Any].

Percent Threshold Change per Event Wildcard Alarms

[BGP Threshold: Rate of Change in Number of Route Updates for Router: Any].

BGP Route Wildcard Alarms

The BGP Route Wildcard Alarms consist of the following:

Any Availability Change on Any BGP Route Wildcard Alarm

```
[Any BGP Route Availability Change: any single Availability change].
```

Excessive Availability Flapping on Any BGP Route Wildcard Alarm

```
[Excessive Availability Flapping on Any BGP Route: at least <number> Availability
flap(s) within <number> seconds].
```

Any Redundancy Change on Any BGP Route Wildcard Alarm

```
[Any BGP Route Redundancy Change: at least <number> change(s) within <number>
seconds].
```

Excessive Redundancy Flapping on Any BGP Route Wildcard Alarm

```
[Excessive Redundancy Flapping on Any BGP Route: at least <number> Availability
flap(s) within <number> seconds].
```

Any Change on Any BGP Route Wildcard Alarm

```
[Any BGP Route Any Change: at least <number> changes within <number> seconds].
```

BGP Threshold per AS Wildcard Alarms

The Threshold per Router Wildcard Alarms consist of the following

Percent Threshold Change per Prefix Wildcard Alarms

```
[BGP Threshold: Rate of Change in Number of Routes in AS].
```

Percent Threshold Change per Event Wildcard Alarms

```
[BGP Threshold: Rate of Change in Number of Route Updates in AS].
```

BGP Next Hop Wildcard Alarms

The Next Hop Alarm consist of the following:

BGP Next Hop Alarm

```
[Any BGP Next Hop change: any single Next Hop change].
```

Interface Wildcard Alarms

The Interface Wildcard Alarms consist of the following:

Point-to-Point (P2P) Interface Wildcard Alarms

You can set an alarm on any P2P interface to receive notifications about changes to the interface.

Numbered NP2P (NNP2P) Interface Wildcard Alarms

The following NP2P interface wildcard alarms are provided in Alarm Monitor:

Any Availability Change on Any NP2P Interface

```
[Any NP2P Interface Availability Change: any single Availability change].
```

Excessive Availability Flapping on Any NP2P Interface

```
[Excessive Availability Flapping on Any NP2P Interface: at least <number> Availability
flap(s) within <number> secs].
```

Metric Change on Any NP2P Interface

```
[Any NP2P Interface Metric Change: at least <number> metric change(s) within <number>
secs].
```

Any Change on Any NP2P Interface

```
[Any NP2P Interface Any Change: at least <number> change(s) within <number> seconds.
```

Unnumbered (UP2P) Interface Wildcard Alarms

The following UP2P interface wildcard alarms are provided in Alarm Monitor

Any Availability Change on Any UP2P Interface

```
[Any UP2P Interface Availability Change: any single Availability change].
```

Excessive Availability Flapping on Any UP2P Interface

```
[Excessive Availability Flapping on Any UP2P Interface: at least <number> Availability
flap(s) within <number> secs].
```

Metric Change on Any UP2P Interface

```
[Any UP2P Interface Metric Change: at least <number> metric change(s) within <number>
secs].
```

Any Change on Any UP2P Interface

```
[Any UP2P Interface Any Change: at least <number> change(s) within <number> seconds].
```

Transit Interface Wildcard Alarms

You can set an alarm on any transit interface to receive notifications about changes to the interface.

The following transit interface wildcard alarms are provided in Alarm Monitor:

Any Availability Change to Any Transit Interface

```
[Any Transit Interface Availability Change: any Single Availability change].
```

Excessive Availability Flapping on Any Transit Interface

```
[Excessive Availability Flapping on Any Transit Interface: at least <number>
availability flap(s) within <number> seconds].
```

Metric Change on Any Transit Interface

```
[Any Transit Interface Metric Change: at least <number> Metric change(s) within
<number> seconds].
```

Any Change on Any Transit Interface

```
[Any Transit Network Interface Any Change: at least <number> change(s) within <number>
seconds].
```

Router Wildcard Alarms

You can set an alarm on any router to receive notifications about changes.

The following router wildcard alarms are provided in Alarm Monitor:

Availability Change on Any Router

```
[Any Router Availability Change: any single Availability change].
```

Status Change on Any ABR

```
[Any Router ABR Status Change: any single ABR Status change].
```

Status Change on Any ASBR

```
[Any Router ASBR Status Change: any single ASBR status change].
```

Excessive Availability Flapping on Any Router

```
[Excessive Availability Flapping on Any Router: at least <number> availability flaps
within <number> secs].
```

Excessive ABR Status Flapping on Any Router

```
[Excessive ABR Status Flapping on Any Router: at least <number> status flaps within
<number> secs].
```

Excessive ASBR Status Flapping on Any Router

```
[Excessive ASBR Status Flapping on Any Router: at least <number> status flaps within
<number> secs].
```

Area Count Change on Any Router

```
[Any Router Area Count Change: at least <number> area count change(s) within <number>
seconds].
```

Any Change on Any Router

```
[Any Router Any Change: at least <number> change(s) within <number> seconds].
```

Transit Network Wildcard Alarms

You can set an alarm on any transit network to receive notifications about changes to the Transit network

The following Transit network wildcard alarms are provided in Alarm Monitor:

Any Transit Network Availability Change

```
[Any Transit Network Availability Change: any single Availability change].
```

Excessive Availability Flapping on Any Transit Network

```
[Excessive Availability Flapping on Any Transit Network: at least <number>
Availability flap(s) within <number> seconds].
```

Designated Router (DR) Change on Any Transit Network

```
[Any Transit Network DR Change: at least <number> DR change(s) within <number>
seconds].
```

Router Count Change on Any Transit Network

```
[Any Transit Network Routers Count Change: at least <number> Router Count change(s)
within <number> seconds].
```

Designated Router Interface Change on Any Transit Network

```
[Any Transit Network DR Interface Change: at least <number> change(s) within <number>
seconds].
```

Any Change on Any Transit Network

```
[Any Transit Network Any Change: at least <number> change(s) within <number> seconds].
```

Advertisement Alarms

The Advertisement Wildcard Alarms consist of the following:

Stub Route Wildcard Alarms

You can set an alarm on any stub route to receive notifications about changes to the route.

The following Stub Route Wildcard alarms are provided in Alarm Monitor:

Any Stub Route Availability Change

```
[Any Stub Route Availability Change: any single Availability change].
```

Excessive Availability Flapping on Any Stub Route

```
[Excessive Availability Flapping on Any Stub Route: at least <number> availability
flap(s) within <number> seconds].
```

Metric Change to Any Stub Route

```
[Any Stub Route Metric Change: at least <number> Metric change(s) within <number>
seconds].
```

Any Change on Any Stub Route

```
[Any Stub Route Any Change: at least <number> change(s) within <number> seconds].
```

External Route Wildcard Alarms

You can set an alarm on any external route to receive notifications about changes to the route.

The following external route wildcard alarms are provided in Alarm Monitor:

Any Availability Change on Any External Route

[Any External Route Availability Change: any single Availability change].

Excessive Availability Flapping on Any External Route

[Excessive Availability Flapping on Any External Route: at least <number> Availability flap(s) within <number> seconds].

Any Metric Change on Any External Route

[Any External Route Metric Change: at least <number> Metric change(s) within <number> seconds].

Any Route Type Change on Any External Route

[Any External Route Type Change: at least <number> Type change(s) within <number> seconds].

Any Change on Any External Route

[Any External Route Any Change: at least <number> changes within <number> seconds].

Route Alarms

The Route Wildcard Alarms consist of the following:

Core Route Wildcard Alarms

You can set an alarm on any core route to receive notifications about changes to the route.

The following external route wildcard alarms are provided in Alarm Monitor:

Any Availability Change on Any Core Route

```
[Any Core Route Availability Change: any single Availability change].
```

Excessive Availability Flapping on Any Core Route

```
[Excessive Availability Flapping on Any Core Route: at least <number> Availability
flap(s) within <number> seconds].
```

Any Redundancy Change on Any Core Route

```
[Any Core Route Redundancy Change: at least <number> Metric change(s) within <number>
seconds].
```

Excessive Redundancy Flapping on Any Core Route

```
[Excessive Redundancy Flapping on Any Core Route: at least <number> Availability
flap(s) within <number> seconds].
```

Any Change on Any Core Route

```
[Any Core Route Any Change: at least <number> changes within <number> seconds].
```

External Route Wildcard Alarms

You can set an alarm on any external route to receive notifications about changes to the route.

The following External Route Wildcard alarms are provided in Alarm Monitor:

- Any Availability Change on Any External Route 15-9
- Excessive Availability Flapping on Any External Route on page 15-9
- Any Redundancy Change on Any External Route on page 15-11
- Excessive Redundancy Flapping on Any External Route on page 15-11
- Any Change on Any External Route on page 15-11

Any Availability Change on Any External Route

```
[Any External Route Availability Change: any single Availability change].
```

Excessive Availability Flapping on Any External Route

```
[Excessive Availability Flapping on Any External Route: at least <number> Availability
flap(s) within <number> seconds].
```

Any Redundancy Change on Any External Route

```
[Any External Route Redundancy Change: at least <number> change(s) within <number>
seconds].
```

Excessive Redundancy Flapping on Any External Route

```
[Excessive Redundancy Flapping on Any External Route: at least <number> Availability
flap(s) within <number> seconds].
```

Any Change on Any External Route

```
[Any External Route Any Change: at least <number> changes within <number> seconds].
```

Threshold Alarms

The Threshold Wildcard Alarms consist of the following:

Entity Rate Threshold Wildcard Alarms

You can set entity rate threshold alarms on any of the following entities:

- Router
- External route
- Stub route
- Transit network
- Numbered point-to-point (NP2P) interface
- Unnumbered point-to-point (UP2P) interface
- Transit interface

The following Entity Rate Threshold wildcard alarms are provided in Alarm Monitor:

Percent Threshold Entity Rate Change Wildcard Alarm for Router

```
[Detection of Threshold Rate of Change in Number of Router Entities].
```

Percent Threshold Entity Rate Change Wildcard Alarm for External Route

```
[Detection of Threshold Rate of Change in Number of External Route Entities].
```

Percent Threshold Entity Rate Change Wildcard Alarm for Stub Route

```
[Detection of Threshold Rate of Change in Number of Stub Route Entities].
```

Percent Threshold Entity Rate Change Wildcard Alarm for Transit Network

```
[Detection of Threshold Rate of Change in Number of Transit Network Entities].
```

Percent Threshold Entity Rate Change Wildcard Alarm for Numbered P2P Interface

```
[Detection of Threshold Rate of Change in Number of Numbered P2P Interface Entities].
```

Percent Threshold Entity Rate Change Wildcard Alarm for Unnumbered P2P Interface

```
[Detection of Threshold Rate of Change in Number of Unnumbered P2P Interface
Entities].
```

Percent Threshold Entity Rate Change Wildcard Alarm for Transit Interface

```
[Detection of Threshold Rate of Change in Number of Transit Interface Entities].
```

Event Rate Threshold Wildcard Alarms

You can set event rate threshold alarms on any of the following entities:

- Router
- External route
- Stub route
- Transit network
- Numbered point-to-point (NP2P) interface
- Unnumbered point-to-point (UP2P) interface
- Transit interface

The following Event Rate Threshold wildcard alarms are provided in Alarm Monitor:

Percent Threshold Event Rate Change Wildcard Alarm for Router

```
[Detection of Threshold Rate of Change in Number of Router Events].
```

Percent Threshold Event Rate Change Wildcard Alarm for External Route

```
[Detection of Threshold Rate of Change in Number of External Route Events].
```

Percent Threshold Event Rate Change Wildcard Alarm for Stub Route

```
[Detection of Threshold Rate of Change in Number of Stub Route Events].
```

Percent Threshold Event Rate Change Wildcard Alarm for Transit Network

```
[Detection of Threshold Rate of Change in Number of Transit Network Events].
```

Percent Threshold Event Rate Change Wildcard Alarm for Numbered P2P Interface

```
[Detection of Threshold Rate of Change in Number of Numbered P2P Interface Events].
```

Percent Threshold Event Rate Change Wildcard Alarm for Unnumbered P2P Interface

```
[Detection of Threshold Rate of Change in Number of Unnumbered P2P Interface Events].
```

Percent Threshold Event Rate Change Wildcard Alarm for Transit Interface

```
[Detection of Threshold Rate of Change in Number of Transit Interface Events].
```

Error Alarms

Interface Conflict Error Wildcard Alarms

```
[Any Interface Conflict Error: at least <number> changes within <number> seconds].
```

Service and Service Path Wildcard Alarms

You can set an alarm on any unicast or multicast service, unicast service path, or SSM Multicast Group to receive notifications about changes.

Unicast Service Wildcard Alarms

The following service wildcard alarms are provided in Alarm Monitor:

Unicast Any Service Availability Change

```
[Any Service Availability Change: any single service availability change].
```

Unicast Availability Flap Alarm on Any Service

```
[Excessive Reachable Flapping on Any Service: at least <number> Reachable flap(s)
within <number> secs].
```

Unicast Any Service Conformity Change

```
[Any Service Availability Change: any single availability change].
```

Unicast Conformity Flap Alarm on Any Service

```
[Excessive Conformity Flapping on Any Service: at least <number> conforming flap(s)
within <number> secs].
```

Unicast Any Change on Any Service Alarm

```
[Any Service Any Change: at least <number> change(s) within <number> secs].
```

Unicast Service Path Wildcard Alarms

You can set an alarm on any service path to receive notifications about changes on any service path.

The following service path wildcard alarms are provided in Alarm Monitor:

Unicast Any Service Path Availability Change

```
[Any Service Path Availability Change: any single availability change].
```

Unicast Availability Flap Alarm on Any Service Path

```
[Excessive Reachable Flapping on Any Service Path: at least <number> Reachable flap(s)
within <number> secs].
```

Unicast Any Service Path Conformity Change

[Any Service Path Availability Change: any single availability change].

Unicast Conformity Flap Alarm on Any Service Path

[Excessive Conformity Flapping on Any Service Path: at least <number> conforming flap(s) within <number> secs].

Unicast Any Service Path Loop Alarm

[Any Service Path Loop Alarm: at least <number> change(s) within <number> secs].

Unicast Any Change on Any Service Path Alarm

[Any Service Path Any Change: at least <number> change(s) within <number> secs].

Multicast Service Wildcard Alarms

The following service wildcard alarms are provided in Alarm Monitor:

Multicast Any Service Availability Change

[Any Service Availability Change: any single service availability change].

Multicast Availability Flap Alarm on Any Service

[Excessive Reachable Flapping on Any Service: at least <number> Reachable flap(s) within <number> secs].

Multicast Any Service Conformity Change

[Any Service Availability Change: any single availability change].

Multicast Conformity Flap Alarm on Any Service

[Excessive Conformity Flapping on Any Service: at least <number> conforming flap(s) within <number> secs].

Multicast Any Service Redundancy Change

[Any Service Any Redundancy change: at least <number> change(s) within <number> secs].

Multicast Redundancy Flap Alarm on Any Service

[Excessive Redundancy Flapping on Any Service: at least <number> redundancy flap(s) within <number> secs].

SSM Multicast Group Wildcard Alarms

The following service wildcard alarms are provided in Alarm Monitor:

SSM Multicast Group Any Service Availability Change

[Any Group Availability Change: any single service availability change].

SSM Multicast Group Availability Flap Alarm on Any Service

[Excessive Reachable Flapping on Any Group: at least <number> Reachable flap(s) within <number> secs].

SSM Multicast Group Any Service Conformity Change

[Any Group Conformity Change: any single conformity change].

SSM Multicast Group Conformity Flap Alarm on Any Service

[Excessive Conformity Flapping on Any Group: at least <number> conforming flap(s) within <number> secs].

CHAPTER 16

SNMP Traps

The following chapter provides information about the Alarm MIB, how it is structured and how it can be used in conjunction with your network management system.

Cisco Service Path Analyzer supports alarm export to a syslog host or an SNMP agent.

Exporting Alarms is covered in Chapter 8: Exporting Alarms, in the *Cisco Service Path Analyzer System Administration Guide*.

Setting and Monitoring Alarms is covered in Chapter 8: Setting and Monitoring Alarms, in the *Cisco Service Path Analyzer User Guide*.

Alarm MIB

The Alarm MIB contains a list of each alarm and its associated fields. It is provided on a CD-ROM that comes with your Cisco Service Path Analyzer system.

Trap Fields

RouteDynamics traps contain the following fields:

- **Severity**—[string] critical, high, medium or low.
- **Description—**The text associated with the name of the alarm as well as the text associated with the trigger.

  `Example: Numbered Point to Point Interface 30.5.5.1on Router 30.0.0.5.: Np2p Interface: Source  Any, Area  Any, Interface Any, Destination  Any. Becomes Unavailable. 2 time(s) in 60 second(s).`
- **Info**—The ID of the Alarm and ID of the trigger for which this trap was generated.

  `Example: AlarmId 3/TriggerId 1/Triggered`
- **Eventid**—Text associated with the network events causing the alarm trigger.This text string is variable length and grows with the number of event ids in the trigger.In the form of `<domain>[<internal domain #>]EventId <event number>]`

  `Example: d101[33]/EventId 139,d101[33]/EventId 151`

Object Identifiers (OID)

Path Analyzer OID's all start with `1.3.6.1.4.1.25406`.

How to View Traps

The following procedure will allow you to view Cisco Service Path Analyzer traps from a local machine.

Step 1 Set your local machine as an SNMP trap receiver using the Cisco Service Path Analyzer Management Console.

Exporting Alarms is covered in Chapter 8: Exporting Alarms, in the *Cisco Service Path Analyzer System Administration Guide*.

Step 2 Start the SNMP trap process on your local machine.

For example, on a Linux system: `snmptrapd`

Step 3 Navigate to the directory where your syslog messages are stored.

For example, on a Linux system: `var/log/messages`

Trap Output Sample

The following shows the format of a trap output.

```
Mar 21 14:16:04 localhost snmptrapd[3867]: 2007-03-21 14:16:04 192.168.25.59
[192.168.25.59]: SNMPv2-MIB::sysUpTime.0 = Timeticks: (70227100) 8 days, 3:04: 31.00
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.25406.1.21
SNMPv2-SMI::enterprises.25406.1.2.1 = STRING: "low"    SNMPv2-SMI::enterprises.25406.1.2.2
= STRING: "OSPF External Route 0.0.0.0/0 :External (Exact) Route:  Prefix  0.0.0.0/0.  Route
Withdrawal. 1 time(s) in 60 second(s).SNMPv2-SMI:: enterprises.25406.1.2.3 = STRING:
"AlarmId 2/TriggerId 2/Triggered"  SNMPv2-SMI:: enterprises.25406.1.2.4 = STRING:
"ospf[49]/EventId 144,"


Mar 21 14:16:43 localhost snmptrapd[3867]: 2007-03-21 14:16:43 192.168.25.59 [
192.168.25.59]: SNMPv2-MIB::sysUpTime.0 = Timeticks: (70231000) 8 days, 3:05:10.00
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.25406.1.21
SNMPv2-SMI::enterprises.25406.1.2.1 = STRING: "low"    SNMPv2-SMI:: enterprises.25406.1.2.2
= STRING: ":External (Exact) Route:  Prefix  0.0.0.0/0.  Route Withdrawal. 1 time(s) in 60
second(s)." SNMPv2-SMI:: enterprises.25406.1.2.3 = STRING: "AlarmId 2/TriggerId 2/Cleared"
SNMPv2-SMI:: enterprises.25406.1.2.4 = STRING: "ospf[49],"
```