Cisco Active Network Abstraction Fault Management User's Guide, 3.5.1

Corporate 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: 408 526-4100

Text Part Number: OL-10892-02

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

Cisco Active Network Abstraction Fault Management User's Guide, 3.5.1

CONTENTS

About This Guide

This Reference Guide includes the following chapters:

Chapter 1, "Fault Management Overview" describes the challenge of managing an overabundance of events, and introduces some of the key concepts of Cisco ANA alarm management.

Chapter 2, "Correlation Logic" describes how Cisco ANA performs correlation logic decisions.

Chapter 3, "Advanced Correlation Scenarios" describes specific alarms which use advanced correlation logic on top of the root cause analysis flow.

Chapter 4, "Correlation Over Unmanaged Segments" describes how Cisco ANA performs correlation decisions over unmanaged segments.

Chapter 5, "Event and Alarm Configuration Parameters" describes the details of various configurable alarm parameters.

Chapter 6, "Impact Analysis" describes the impact analysis functionality available in Cisco ANA.

Appendix A, "Supported Service Alarms" provides the list of service alarms that are supported in Cisco ANA 3.5.1.

Appendix B, "Supported Traps and Syslogs" provides the list of Cisco traps and syslogs that are supported in Cisco ANA 3.5.1.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific:	+61 2 8446 7411
Australia:	1 800 805 227
EMEA:	+32 2 704 55 55
USA:	1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Fault Management Overview

This chapter describes the challenge of managing an overabundance of events, and introduces some of the key concepts of Cisco ANA alarm management.

The Event Management Challenge describes the event management challenge and how this challenge is met.

Basic Concepts and Terms describes the basic concepts and terms used throughout this guide.

Severity Propagation describes the concept of severity and how severity is propagated.

Sources of Alarms on a Device describes the four basic alarm sources that indicate problems in the network.

Event Processing Overview describes the process for identifying and processing raw events.

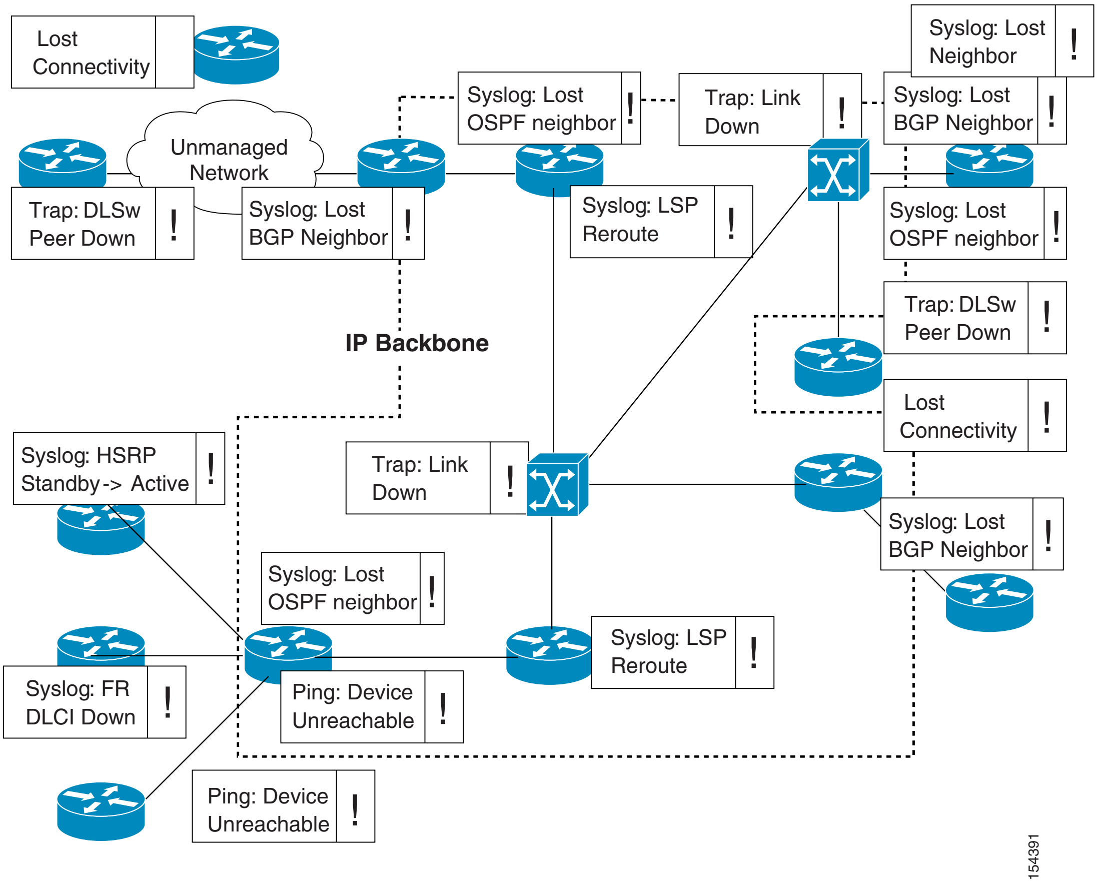
Event Suppression describes enabling or disabling port down/up and link down/up alarms on a selected port.

Alarm Integrity describes what happens when a VNE shuts down that has associated open alarms.

The Event Management Challenge

The challenge of dealing effectively with events and alarms is to know how to understand and efficiently process and organize bulks of raw events that may be generated as a result of single root-cause events.

Figure 1-1 Event Flood



Meeting the event management challenge is done by correlating related events into a sequence that represents the alarm lifecycle, and using the network dependency model to determine the causal inter-relationship between alarms.

Cisco ANA offers extensive fault analysis and management capabilities that ensure quick and accurate fault detection, isolation and correlation capabilities. Once a fault is identified, the system uses the auto-discovered virtual network model to perform fault inspection and correlation in order to determine the root cause of the fault and, if applicable, to perform service impact analysis.

Basic Concepts and Terms

Alarm

An *Alarm* represents a scenario which involves a fault occurring in the network or management system. Alarms represent the complete fault lifecycle, from the time that the alarm is opened (when the fault is first detected) until it is closed and acknowledged. Examples of alarms include:

- Link down
- Device unreachable

- Card out
- An alarm is composed of a sequence of events, each representing a specific point in the alarm’s lifecycle.

Event

An *Event* is an indication of a distinct occurrence that occurred at a specific point in time. Events are derived from incoming traps/notifications and from detected status changes. Examples of events include:

- Port status change
- Connectivity loss between routing protocol processes on peer routers (e.g. BGP neighbor loss)
- Device reset
- Device becoming reachable by the management station
- User acknowledgement of an alarm

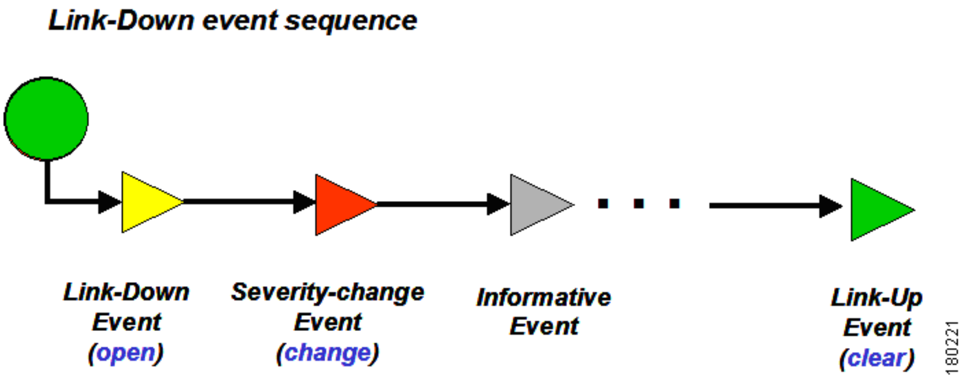
Events are written to the Cisco ANA database once and never change.

The collected events are displayed in the Cisco ANA EventVision. Please refer to the Cisco ANA EventVision Guide for more information.

Event Sequence

An *Event Sequence* is the set of related events, which composes a single alarm. For example, *Link down – Ack – Link up*.

Figure 1-2 Event Sequence Example



Typically, a complete event sequence includes three mandatory events:

- Alarm Open (in this example, a Link Down event).
- Alarm Clear (in this example, a Link Up event).
- Alarm Acknowledge

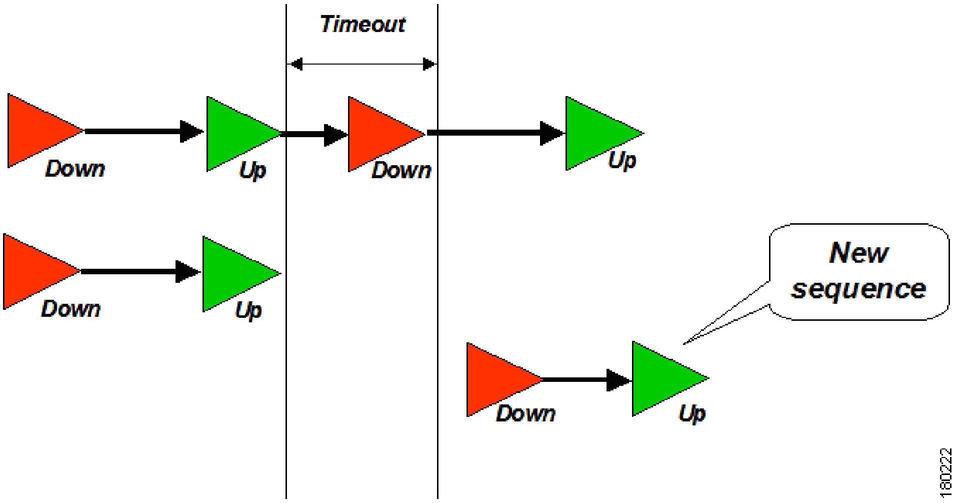
Optionally, there can be any number of Alarm Change events, which can be triggered by new severity events, affected services update events, etc.

Note The event types that will belong to each sequence can be configured in the system registry.
An event sequence can consist of a single event (for example, “Device Reset”)
The set of events that should participate in Cisco ANA alarm processing can be configured in the system registry.

Repeating Event Sequence

If a new opening event arrives within a (configurable) timeout after the clearing event (of the same alarm), the alarm is updatable and a Repeating Event Sequence is created, i.e.the event is attached to the existing sequence, and updates its severity accordingly. If the new opening event occurs after the timeout, it opens a new alarm (new event sequence).

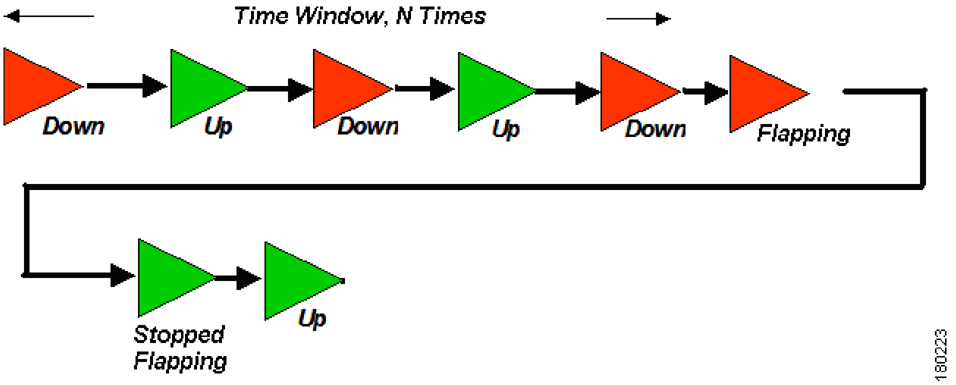
Figure 1-3 Repeating Event Sequence



Flapping Events

If a series of events that are considered to be of a same sequence occurs in the network in a certain configurable time-window a certain (configurable) amount of times, the VNE may (upon configuration) reduce further the number of event, and will issue a single event which will be of type “Event Flapping”. Only when the alarm “stabilizes”, i.e. the event frequency is reduced, another update to the event sequence will be issued as “Event stopped flapping”, and then another update will be issued with the most up-to-date event state.

Figure 1-4 Flapping Event

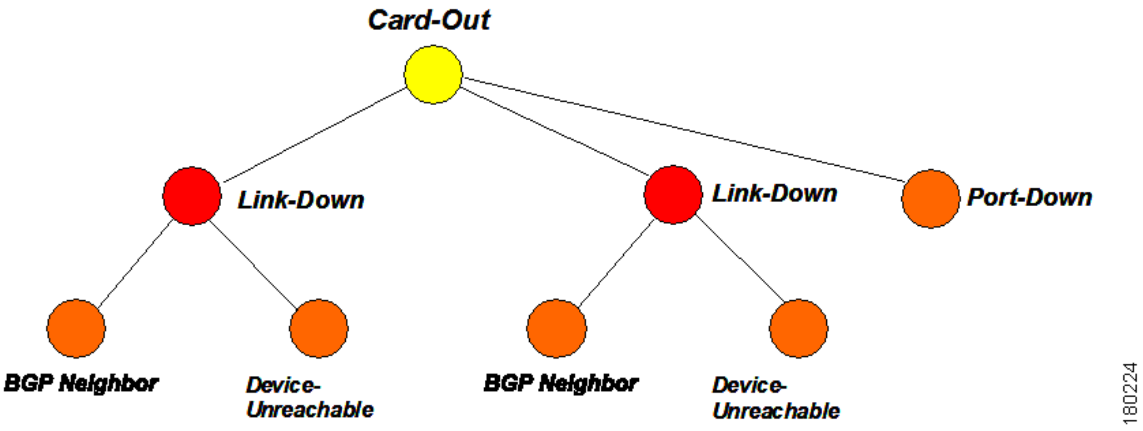


Correlation by Root-Cause

Root-cause correlation is determined between *alarms* (i.e. between event sequences). It represents a causal relationship between an alarm and the consequent alarms that occurred because of it.

For example, a Card-out alarm can be the root-cause of several Link-down alarms, which in turn can be the root-cause of multiple Route-lost and Device unreachable alarms, and so on (a consequent alarm can serve as the root-cause of other consequent alarms).

Figure 1-5 Root-Cause Correlation Hierarchy Example



Ticket

A *Ticket* represents the complete alarm correlation tree of a specific fault scenario. It can be also identified by the topmost ("root of all roots") Alarm. Both Cisco ANA NetworkVision and Cisco ANA EventVision display tickets and allow drilling down to view the consequent alarm hierarchy.

From an operator's point of view, the managed entity is always a complete ticket. Operations such as Acknowledge, Force-clear or Remove are always applied to the whole ticket. The ticket also assumes an overall, propagated severity.

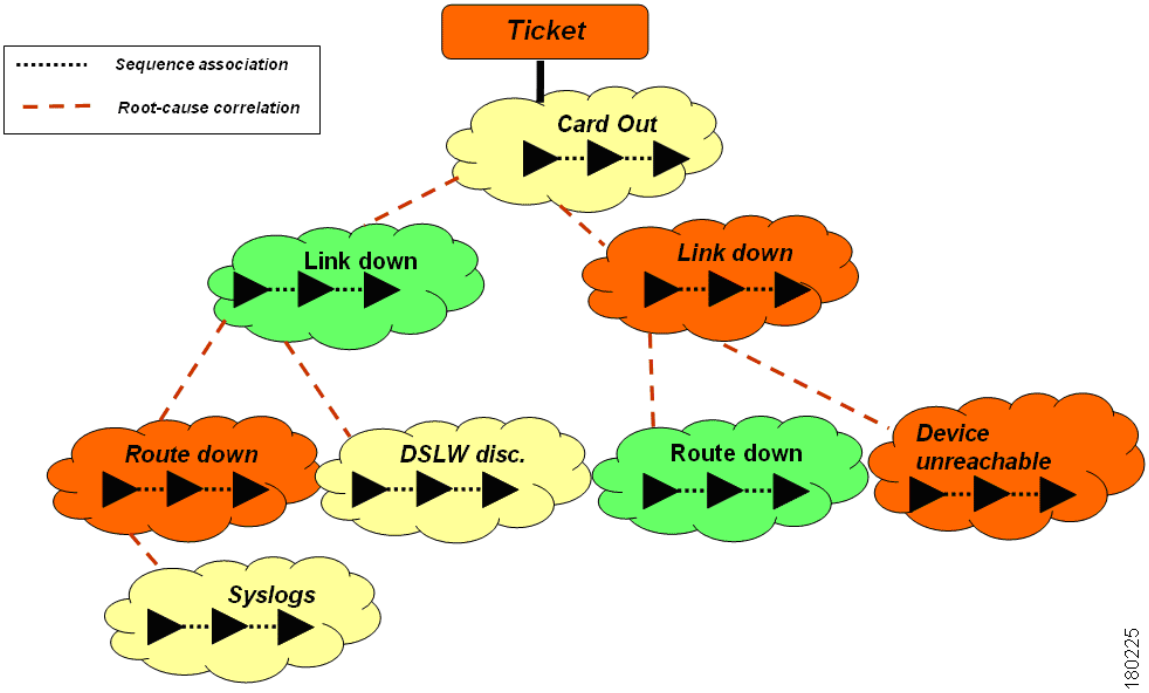
Sequence Association vs. Root-Cause Analysis

It is important not to confuse between the two types of relationships in Cisco ANA alarm management:

- ***Sequence Association*** is the association between events, which creates the event sequences (i.e. alarms).
- ***Root-Cause Analysis*** is the association between alarms (event sequences), which represents the root-cause relationship.

The following figure shows how both types of relations are implemented in the ticket hierarchy:

Figure 1-6 Sequence Association vs. Root-Cause Analysis



In the above figure, the “clouds” represent alarms, which are correlated into a hierarchy according to root-cause. Within each alarm is its respective event sequence, representing the lifecycle of the alarm.

Severity Propagation

Each event has an assigned severity (user-configurable). For example, a Link-up event may be assigned *Critical* severity, while its corresponding Link-up event will have *Normal* severity.

The propagated severity of the alarm (i.e. the whole event sequence) is always determined by the last event in the sequence. Thus, in the above example, when the Link-down alarm is open it will have Critical severity, and when it clears it move to Normal severity. An exception to this rule is the informational event (severity level of *Info*) such as “User acknowledge” event, which does not change the propagated severity of the sequence (i.e. the alarm).

Each ticket assumes the propagated severity of the alarm with the *topmost severity*, within all the alarms in the correlation hierarchy (at any level).

Note Each alarm **does not** assume propagated severity of the correlated alarms beneath it. Each alarm assumes its severity only from its internal event sequence (as described above), while the ticket assumes the highest severity among all the alarms in the correlation tree.

Sources of Alarms on a Device

There are four basic sources for alarms which indicate a problem in the network that are currently supported by the platform:

- Service Alarms—Alarms that are generated by the Cisco ANA VNE as result of polling (e.g. SNMP, Telnet). Usually such alarms are configured to be 'Root-Cause' alarms (e.g. Link-Down, Card-Out, Device-Unreachable). Service alarms can also be generated by the Gateway, for example. the `vpn leak` alarm.
- SNMP Traps—Traps that sent by the network elements and captured by the Cisco ANA platform. The Cisco ANA platform supports SNMP v1, and v2 traps. The traps are then forwarded to the specific VNEs for further processing and correlation logic.
- Syslogs—Syslog messages that sent by the network elements and captured by the Cisco ANA platform. The Syslogs are then forwarded to the specific VNEs for further processing and correlation logic.
- TCA—Threshold Crossing Alarms. Cisco ANA can be used to set a Threshold Crossing Alarm (TCA) for soft properties. The TCA can be enabled to assign a condition to the property, which will trigger an alarm when violated. The alarm conditions could be:
  - Being equal or not equal to a target value
  - Exceeding a defined value range (defined by max and min thresholds, including hysteresis), e.g. CPU level of a device
  - Exceeding a defined rate (calculated across time), e.g. bandwidth or utilization rate of a link.

For information about TCA alarms, refer to the *Cisco ANA Customization User's Guide*.

Event Processing Overview

Cisco ANA provides a customizable framework for identifying and processing raw events. The raw events are collected into the Event Manager, forwarded to their respective VNE, and then processed as follows:

Step 1 The event data is parsed to determine its source, type, and alarm-handling behavior.

Step 2 If the event type is configured to try and correlate, the VNE attempts to find a compliant cause alarm. This is done in the VNE fabric.

Step 3 The event fields are looked up and filled.

Step 4 The event is sent to the Cisco ANA Gateway, where:

- The event is written as-is to the event database.
- If the event is alarm-able (belongs to an alarm), it is attached to its respective event sequence, and correlated to the respective root-cause alarm within the ticket.(or open a new sequence and/or new ticket).

- If the event is Marked as Ticketable, and it did not correlate to any other Alarm a new Ticket will be opened, where the alarm that triggered the Ticket will be the root cause of any alarms in the correlation tree.

Event Suppression

The user can enable or disable the port down/up and link down/up alarms on a selected port. By default, alarms are enabled on all ports. When the alarms are disabled on a port, no alarms will be generated for the port and they will not be displayed in the *Ticket* pane. Using the advanced tools (Registry Editor) it is possible to enable or disable Service Alarms on network entities other then ports, such as the MPBGP (for enabling/disabling BGP neighbor down service alarm.), or the MPLS TE Tunnel (for TE-Tunnel down service alarm) etc. It is also possible to enable or disable alarm specific types, without regard to a specific network entity.

To disable/enable a port alarm:

Refer to the *Cisco Active Network Abstraction NetworkVision User's Guide* for information about disabling or enabling a port alarm.

Alarm Integrity

When the VNE shuts down and still has open alarms associated with it, “fixing” events which occur during the down period will be consolidated when the VNE is reloaded.

Related Documentation

For more information, refer to the following publications:

- Cisco Active Network Abstraction NetworkVision User's Guide
- Cisco Active Network Abstraction Customization User's Guide
- Cisco Active Network Abstraction EventVision User's Guide
- Cisco Active Network Abstraction MPLS User's Guide

CHAPTER 2

Correlation Logic

This chapter describes how Cisco ANA performs correlation logic decisions.

Root-Cause Correlation Process describes the root-cause correlation concept.

Root-Cause Alarms describes the root-cause alarm and weights concepts.

Correlation Flows describes network and box-level correlation flows.

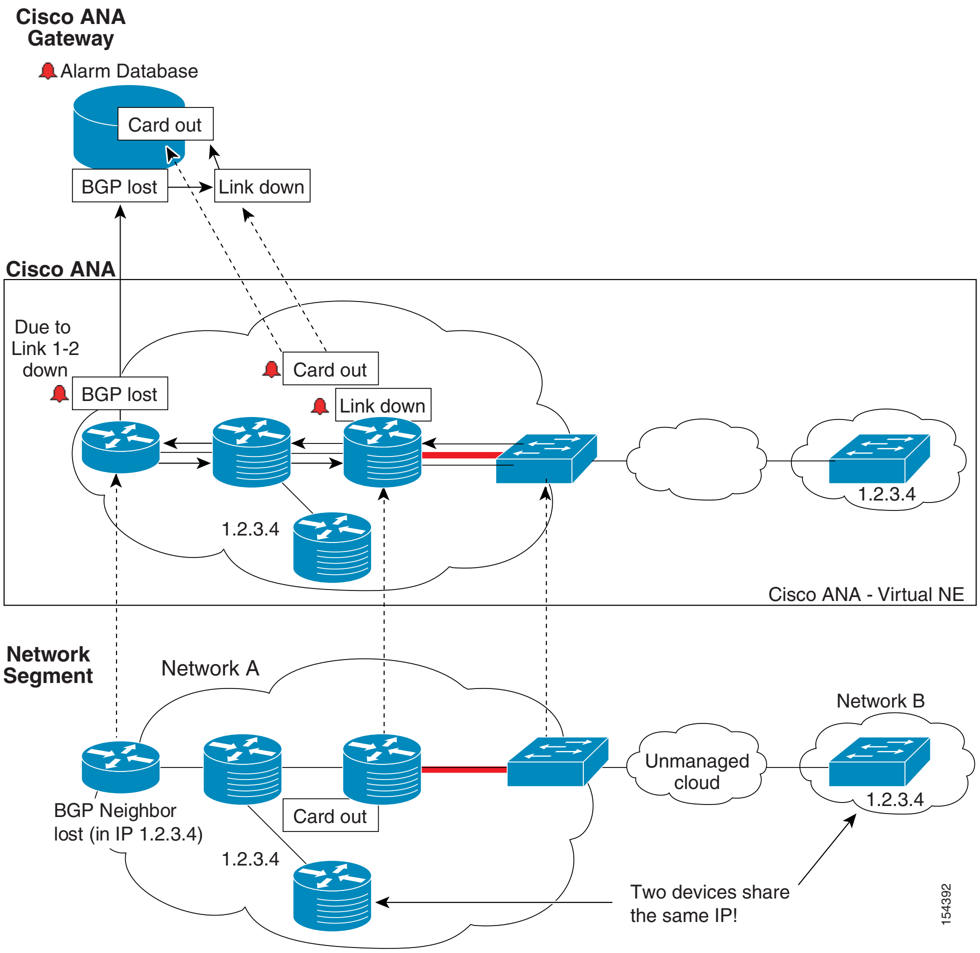
Root-Cause Correlation Process

Root-cause correlation is implemented in various stages within the Cisco ANA VNEs. Initially, the system tries to find the root-cause alarm. When a VNE detects a fault (and opens an alarm), it attempts to find another open alarm within the same device, which qualifies as the root-cause of the new alarm. For example, in the case of a “link down syslog” alarm , the VNE will look for a root-cause alarm within the device, for example, “link down”. When such a root-cause is found and qualified, the correlation relationship is set in the alarm DB. This process is named *Box-Level Correlation*.

A more difficult scenario is finding the root-cause in a different device, which could be many network hops away. In the above example, the Link-down alarm could cause multiple “BGP Neighbor down” alarms throughout the network. In such cases, the BGP Neighbor down is configured by default to actively go and search for a root-cause in other VNEs, by initiating an *Network Correlation Flow*. In this example, the VNE that detected the BGP Neighbor down uses the network topology model maintained in the Cisco ANA fabric to trace the path to its lost neighbor. During this trace it will encounter the faulty link, and qualify it as the BGP Neighbor down root-cause.

The following figure illustrates the local and active correlation processes.

Figure 2-1 Root-Cause Correlation Process



The correlation mechanisms are highly configurable (per alarm), as described in the following sections.

Root-Cause Alarms

Potential Root-Cause alarms have a determined weight according to the specific event customization. Refer to the Event and Alarm Configuration Parameters section for additional information about setting the weights. For example, a ‘Link-Down’ alarm is configured to allow other alarms to correlate to it, thus when a ‘Link-Down’ event is recognized other alarms that occur in the network may choose to correlate to it, hence identifying it as the cause for their occurrence. However an event that is configured to be the cause for other alarms can in its turn correlate to another alarm. The topmost alarm in the correlation tree is the Root-cause for all the alarms.

Correlation Flows

The VNEs utilize their internal DCM (Device Component Model) in order to perform the actual correlation. This action is considered to be a ‘correlation flow’. There are two basic correlation mechanisms used by the VNE:

- Box Level correlation (correlation in the same VNE)
- Network correlation (correlation across VNEs).

Each event can be configured to:

- Not correlate at all
- Perform Box-level correlation
- Perform Box-level correlation and Network correlation should the Box-level correlation fail.

For more information about these parameters, see the Event and Alarm Configuration Parameters section.

Network Correlation Flows

Network problems and their effects are not always restricted to one network element. This means that a certain event could have the capability of correlating to an alarm several hops away. To actually do so the correlation mechanism within the VNE uses an active correlation flow that runs on the internal VNEs DCM model and ‘tries’ to correlate along a specified network path to an alarm. This is similar to the Cisco ANA PathTracer operation when it traces a path on the DCM model from point ‘A’ to point ‘Z’ with the distinction of trying to correlate to a Root-Cause alarm along the way, rather than just tracing a path. This method is usually applicable for problems in the Network layer and above (OSI Network Model) that might be caused due to a problem up or down stream. An example is an OSPF Neighbor Down event caused by a Link Down problem in an up stream router. Another important distinction between Cisco ANA PathTracer and the correlation flow is that the correlation flow may run on a historical snapshot of the network.

Box-Level Correlation

In contrast to Network Correlation Flows when the Root-Cause problem is on the ‘box’ level the attempts to correlate other events are restricted to the specific VNE. This means that the correlation flow doesn’t cross the DCM models of more than one VNE. An example is a Port Down syslog event correlating to a Port Down event. An exception for this behavior is the Link Down alarm. Since a ‘Link’ entity connects two End points in the DCM model, it involves the DCM of two different VNEs, but on each VNE the events are correlated to their own ‘copy’ of the link-down event.

Using Weights

In cases where there are multiple potential root-causes along the same service path, Cisco ANA enables the user to define a priority scheme (weight) which can determine the actual root-cause.

The correlation system will use the following information to identify more precisely the root-cause alarm:

- *weight*: -2—weightless. The flow will not collect weightless alarms and no network correlation to the alarm is possible.

- *weight*: -1—max weight. The correlation flow will stop if it encounters a max weight alarm, and will choose that alarm as the root-cause.
- *weight*: >=0 The correlation flow will collect the alarm, but will not stop.

The correlation mechanism will choose the alarm with the highest weight as the root-cause for the alarm that triggered the network correlation flow.

Correlating TCA

TCAs participate in the correlation mechanism and can correlate or be correlated to other alarms.

Advanced Correlation Scenarios

This chapter describes the specific alarms which use advanced correlation logic on top of the root cause analysis flow.

Device Unreachable Alarm describes the "device unreachable" alarm, its correlation and provides various examples.

HSRP Alarms describes the HSRP alarms and provides various examples.

IP Interface Failure Scenarios describes the "ip interface status down" alarm and its correlation. In addition, it describes the "all ip interfaces down" alarm, its correlation and provides several examples.

Device Unreachable Alarm

Connectivity Test

Connectivity tests are used to verify connectivity between the Cisco ANA VNEs and managed network elements. The connectivity is tested per each protocol through which the VNE polls the device. The supported protocols for connectivity test are SNMP, Telnet and ICMP.

Device unreachable alarm will be issued if one or more of the connectivity test fails. i.e. the device does not respond on this protocol. The alarm will be cleared when all the protocol connectivity test are passed successfully.

Note The ICMP connectivity test is enabled in the Cisco ANA Manage.

Device Fault Identification

When a network element stops responding to queries from the management system, one of two things has happened:

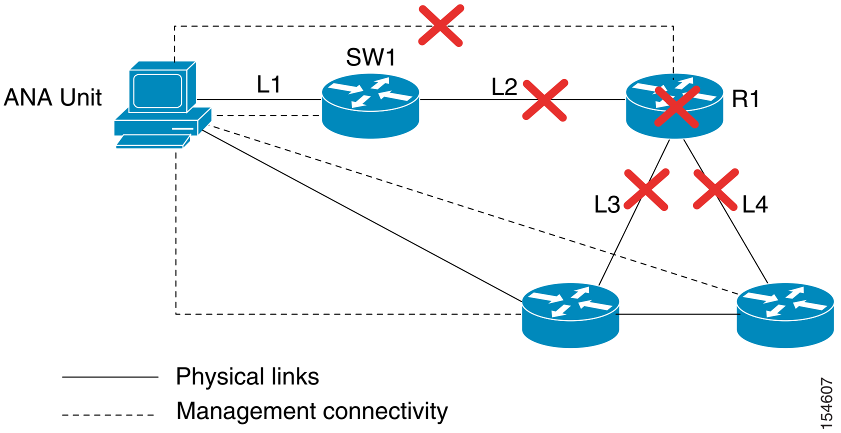
- Connectivity to that device is lost
- The device itself crashes/restarts

Cisco ANA implements an algorithm that uses additional data to heuristically resolve the ambiguity and declare the Root-Cause correctly. Refer to the examples that follow.

Device Unreachable Example 1

In this example, the router (R1) goes down. As a result the links: L2, L3, and L4 go down in addition to the R1 session.

Figure 3-1 Device Unreachable Example 1



In this case the system will provide the following report:

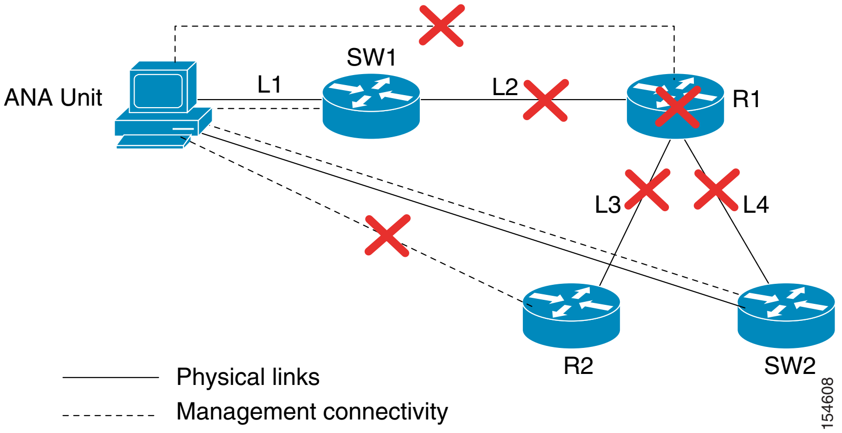
- Root-Cause—Device Unreachable.(R1)
- Correlated events:
  - L2 down
  - L3 down
  - L4 down

Device Unreachable Example 2

In this example, the router (R1) goes down. As a result the links: L2, L3, L4 go down as well as the R1 session. The router R2, accessed by the link L3 is also unreachable.

Note No Link down alarm is displayed for L3 as its state cannot be determined.

Figure 3-2 Device Unreachable Example 2



Note If the device has a single link, and it is being managed through that link (in-band management), there is no way to determine if the device is unreachable due to link down, or the link is down because the device is unreachable. In this case Cisco ANA shows that the device unreachable due to link down.

In this case the system will provide the following report:

- Root-Cause—Device Unreachable.(R1)
- Correlated events:
  - L2 down
  - Device Unreachable (R2)
  - L4 down

HSRP Alarms

When an active Hot Standby Router Protocol (HSRP) group's status changes a service alarm is generated and a syslog is sent.

Table 3-1 HSRP Service Alarms

Alarm	Is-ticketable	Is-correlation-allowed	Correlated to	Severity
Primary HSRP interface is not active / Primary HSRP interface is active	Yes	No	Can be correlated to several other alarms, for example, link down	Major
Secondary HSRP interface is active / Secondary HSRP interface is not active	Yes	No	Can be correlated to several other alarms, for example, link down	Major

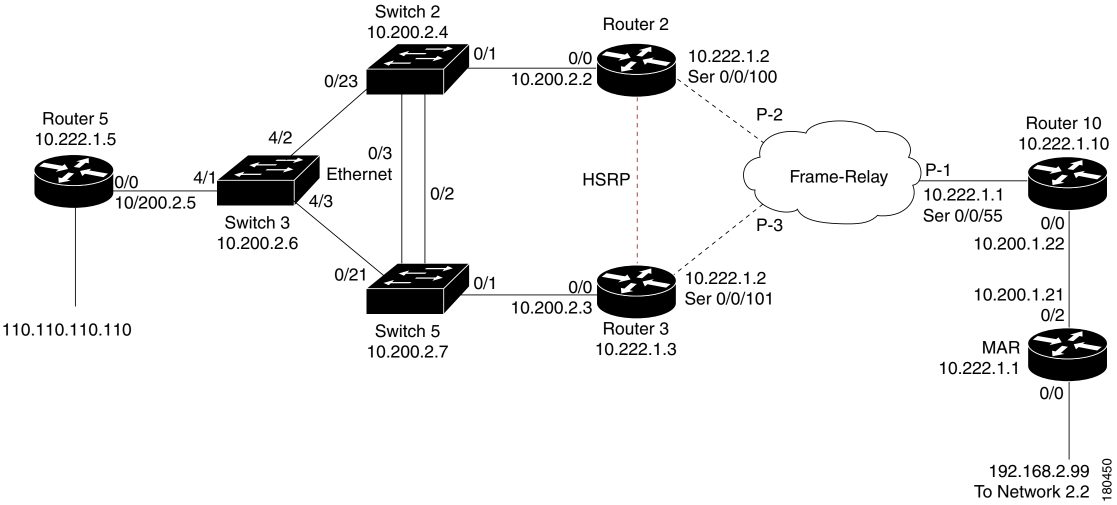
Note HSRP group information can be viewed in the Inventory window of Cisco ANA NetworkVision.

HSRP Example 1

In this example the link between Router 2 and Switch 2 is shut down (causing the HSRP standby group on Router 3 to become active), and a link down service alarm is generated. The Primary HSRP group on Router 2 is not active anymore. A service alarm is generated and correlated to the link down alarm. Router 2 also sends a syslog which is correlated to the link down alarm.

The secondary HSRP group, configured on Router 3 now changes from standby to active. This network event triggers an IP based active flow with the destination being the virtual IP address configured in the HSRP group. When the flow reaches its destination a service alarm is generated and correlated to the link down alarm. Router 3 also sends a syslog which is correlated to the link down alarm.

Figure 3-3 HSRP Example 1



In this case the system provides the following report:

- Root-Cause—Link down (Router 2-Switch 2)
- Correlated events:
  - Primary HSRP interface is not active (source: Router 2)
  - `%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Speak` (source: Router 2)
  - Secondary HSRP interface is active (source: Router 3)
  - `%STANDBY-6-STATECHANGE: Ethernet0/0 Group 1 state Standby -> Active` (source: Router 3)

HSRP Registry Parameters

The following “hsrp group status changed” parameters can be controlled through the Registry for both primary and secondary service alarms:

- flow-delay

- time-stamp-delay

The following “hsrp syslog” parameter can be controlled through the Registry for both primary and secondary HSRP status change syslogs:

- expiration-time

Note For more information about these parameters see the Event and Alarm Configuration Parameters chapter.

IP Interface Failure Scenarios

This section includes the following:

- IP Interface Status Down Alarm
- All IP Interfaces Down Alarm
- IP Interface Failure Examples

IP Interface Status Down Alarm

Alarms related to subinterfaces, for example, Line Down trap, Line Down syslog, and so on are reported on IP Interfaces configured above the relevant subinterface, this means that actually in the system subinterfaces are represented by the IP interfaces configured above them. All events sourcing from subinterfaces without a configured IP are reported on the underlying Layer1.

An “ip interface status down” alarm is generated when the status of the ip interfaces (whether it is over an interface or a sub interface) changes from “Up” to “Down”, or any other non-operational state. All events sourcing from the subinterfaces correlate to this alarm. In addition an “All ip interfaces down” alarm is generated when all of the ip interfaces above a physical port change state to “Down”.

Table 3-2 IP Interface Status Down Alarm

Name	Description	Is-ticketable	Is-correlation-allowed	Correlated to	Severity
Interface status down/up	Sent when an IP interface changes oper status to “down”	Yes	Yes	Link Down/Device unreachable/Configuration changed	Major

The alarm's description includes the full name of the IP interface, e.g. Serial0.2 (including the identifier for the sub interface if it is a sub interface) and the source of the alarm source points to the IP interface (and not to Layer1).

All syslogs and traps indicating changes in sub interfaces (above which an IP is configured) correlate to the “ip interface status down” alarm (if this alarm was supposed to be issued). The source of these events is the IPInterface. Syslogs and traps that indicate problems in Layer1 (that do not have a subinterface qualifier in their description) are sourced to Layer1.

Note In case a syslog/trap is received from a subinterface that does not have an IP configured above it, the source of the created alarm is the underlying Layer1.

For example:

- Line down trap (for sub interface)
- Line down syslogs (for sub interface)

For events that occur on subinterfaces:

- When sending the information northbound, the system uses the full sub interface name in the interface name in the source field, as described in the ifDesc/ifName OID (e.g. Serial0/0.1 and not Serial0/0 DLCI 50).
- The source of the alarm is the IPInterface configured above the subinterface.
- If there is no IP configured, the source is the underlying Layer1.

In case the main interface goes down, all related sub-interfaces traps and syslogs are correlated as child tickets to the main interface parent ticket.

The following technologies are supported:

- Frame Relay/HSSI
- ATM
- Ethernet, Fast Ethernet, Gigabit Ethernet
- POS
- CHOC

Correlation of Syslogs/Traps

When receiving a trap/syslog for the sub interface level, immediate polling of the status of the relevant IP interface occurs and a polled parent event (for example, “ip interface status down”) is created. The trap/syslog is correlated to this alarm.

Where there is a multipoint setup, and only some circuits under an IP interface go down and this does not cause the state of the IP interface to change to “down”, then no “ip interface status down” alarm is created. All of the circuit down syslogs correlate by flow to the possible root cause, for example “Device unreachable” on a CE device.

All IP Interfaces Down Alarm

- When all of the IP interfaces configured above a physical interface change their state to “down”, the “All ip interfaces down” alarm is sent.
- When at least one of the IP interfaces changes its state to “up”, a clearing alarm is sent, namely, the “active ip interfaces found” alarm.
- The “ip interface status down” alarm for each of the failed IP interfaces is correlated to the “All ip interfaces down” alarm.

Note When an “all ip interfaces down” alarm is cleared by the “active ip interfaces down” alarm but there are still correlated “ip interface status down” alarms for some IP interfaces, the severity of the parent ticket is the highest severity among all of the correlated alarms. For example, if there is an uncleared “interface status down” alarm, the severity of the ticket remains Major, despite the fact that the “Active ip interfaces found” alarm has a Cleared severity.

Table 3-3 All IP Interfaces Down

Name	Description	Is-ticketable	Is-correlation-allowed	Correlated to	Severity
All ip interfaces down/Active ip interfaces found	Sent when all of the IP interfaces configured above a physical port change their oper status to "down"	Yes	Yes	Link Down/Configuration Change	Major

The "All ip interfaces down" alarm is sourced to the Layer1 component. All alarms from "the other side", for example, "device unreachable" correlate to the "All ip interfaces down" alarm.

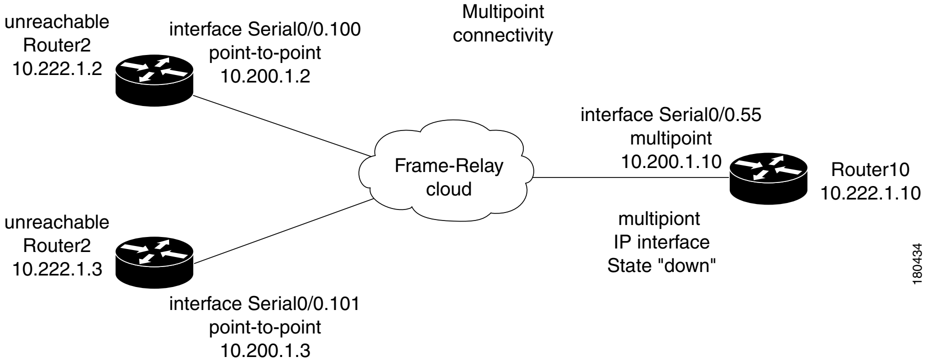
IP Interface Failure Examples

Note In all of the examples that follow it is assumed that the problems that result in the unmanaged cloud or the problems that occurred on the other side of the cloud (for example, an "unreachable" CE device from the point of view a PE device) cause the relevant IP interfaces' state to change to "down". This in turn causes the "ip interface status down" alarm to be sent.
If this is not the case, as in some Ethernet networks, and there is no change to the state of the IP interface, all of the events on the sub interfaces that are correlation flow capable, will try to correlate to other possible root causes, including "cloud problem".

Interface Example 1

In this example there is multipoint connectivity between a PE and number of CEs through an unmanaged Frame Relay network. All of the CEs (Router2 and Router3) have logical connectivity to the PE through a multipoint sub interface on the PE (Router10). The "Keep Alive" option is enabled for all circuits. A link is disconnected inside the unmanaged network that causes all the CEs to become unreachable.

Figure 3-4 Interface Example 1



The following failures are identified in the network:

- A "device unreachable" alarm is generated for each CE
- An "ip interface status down" alarm is generated for the multipoint IP interface on the PE

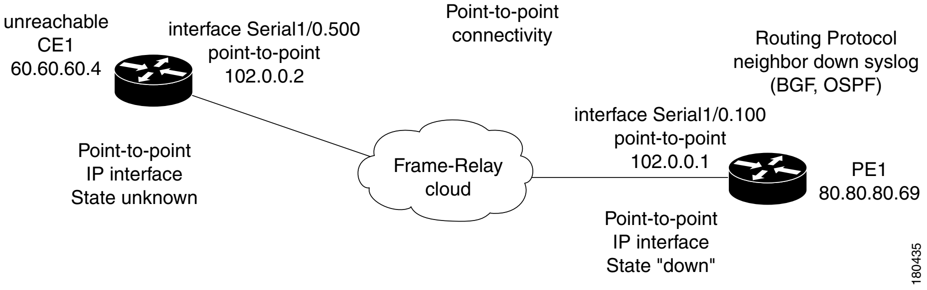
The following correlation information is provided:

- The root cause is IP sub-interface down
- All of the "device unreachable" alarms are correlated to the "ip interface status down" alarm on the PE

Interface Example 2

In this example there is point-to-point connectivity between a PE and a CE through an unmanaged Frame Relay network. CE1 became unreachable, and the status of the IP interface on the other side (on the PE1) changed state to "down". The "Keep Alive" option is enabled. The interface is shut down between the unmanaged network and CE1.

Figure 3-5 Interface Example 2



The following failures are identified in the network:

- A "device unreachable" alarm is generated on the CE
- An "ip interface status down" alarm is generated on the PE

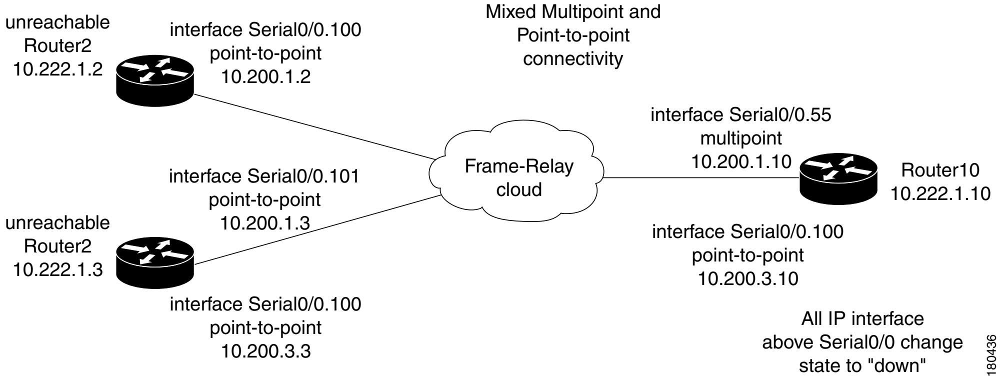
The following correlation information is provided:

- The root cause is "device unreachable"
  - The "ip interface status down" alarm is correlated to the "device unreachable" alarm
  - The syslogs and traps for the related sub interfaces are correlated to the "ip interface status down" alarm

Interface Example 3

In this example there is a failure of multiple IP interfaces above the same physical port (mixed point-to-point and multipoint Frame Relay connectivity). CE1 (Router2) has a point-to-point connection to PE1 (Router10). CE1 and CE2 (Router3) have multipoint connections to PE1. The IP interfaces on PE1 that are connected to CE1, and CE2 are all configured above Serial0/0. The "Keep Alive" option is enabled. A link is disconnected inside the unmanaged network that has caused all of the CEs to become unreachable.

Figure 3-6 *Interface Example 3*



The following failures are identified in the network:

- All of the CEs become unreachable
- An "ip interface status down" alarm is generated for each IP interface above Serial0/0 that has failed

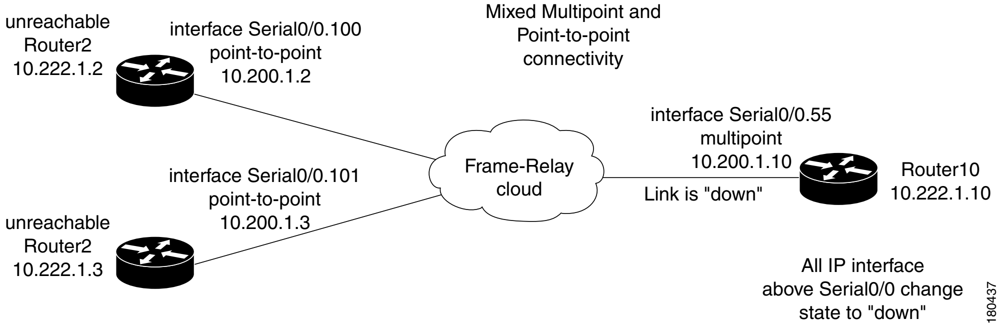
The following correlation information is provided:

- The root cause is "All IP interfaces down" on Serial0/0 port
  - The "ip interface status down" alarms are correlated to the "All IP interfaces down" alarm
  - The "device unreachable" alarms are correlated to the "All IP interfaces down" alarm
  - The syslogs and traps for the related subinterfaces are correlated to the "All IP interfaces down" alarm

Interface Example 4

In this example there is a link down. In a situation where a link down occurs, whether it involves a cloud or not, the link failure is considered to be the most probable root cause for any other failures. In this example, a link is disconnected between the unmanaged network and the PE.

Figure 3-7 *Interface Example 4*



The following failures are identified in the network:

- A "link down" alarm is generated on Serial0/0
- A "device unreachable" alarm is generated for each CE
- An "ip interface status down" alarm is generated for each IP interface above Serial0/0

- An “All interfaces down” alarm is generated on Serial0/0

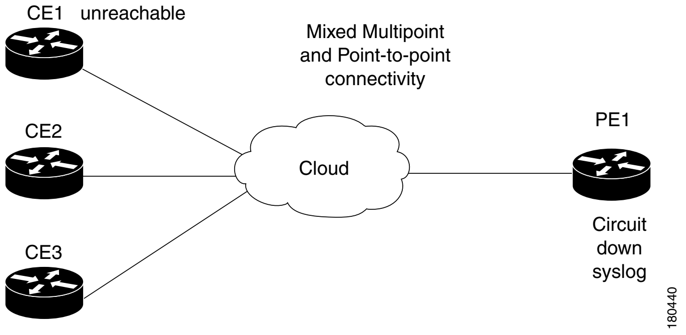
The following correlation information is provided:

- The “device unreachable” alarms are correlated to the “link down” alarm
- The “ip interface status down” alarm is correlated to the “link down” alarm
- The “All interfaces down” alarm is correlated to the “link down” alarm
- All of the traps and syslogs for the sub interfaces are correlated to the “link down” alarm

Interface Example 5

In this example on the PE1 device that has multipoint connectivity, one of the circuits under the IP interface has gone down and the CE1 device which is connected to it has become unreachable. The status of the IP interface has not changed and other circuits are still operational.

Figure 3-8 General Interface Example



The following failures are identified in the network:

- A “device unreachable” alarm is generated on CE1
- A Syslog alarm is generated notifying the user about a circuit down

The following correlation information is provided:

- “device unreachable” on the CE
  - The Syslog alarm is correlated by flow to the possible root cause, for example, a “device unreachable” alarm on CE1

ATM Examples

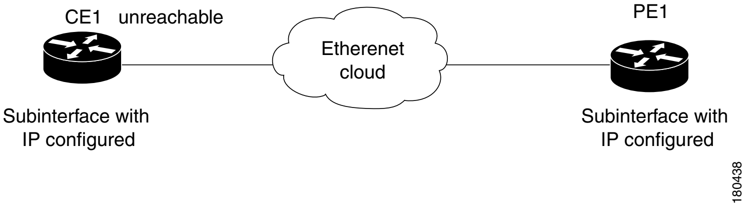
Similar examples involving ATM technology have the same result, assuming that a failure in an unmanaged network causes the status of the IP interface to change to “Down” (ILMI is enabled).

Ethernet, Fast Ethernet, Giga Ethernet Examples

Interface Example 6

In this example there is an unreachable CE due to a failure in the unmanaged network.

Figure 3-9 Interface Example 5


CE1 unreachable
PE1
Etherenet cloud
Subinterface with IP configured
Subinterface with IP configured
180438

The following failures are identified in the network:

- A “device unreachable” alarm is generated on the CE
- A “Cloud problem” alarm is generated

The following correlation information is provided:

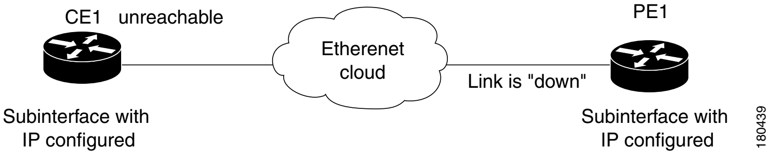
- No alarms are generated on a PE for Layer1, Layer2 or for the IP layers
- The “device unreachable” alarm is correlated to the “Cloud problem” alarm

Note This behavior may change depending on the “correlate-to-cloud”value.

Interface Example 7

In this example there is a link down on the PE that results in the CE becoming unreachable.

Figure 3-10 Interface Example 6


CE1 unreachable
PE1
Etherenet cloud
Link is "down"
Subinterface with IP configured
Subinterface with IP configured
180439

The following failures are identified in the network:

- A “link down” alarm is generated on the PE
- An “ip interface status down” alarm is generated on the PE
- A “device unreachable” alarm is generated on the CE.

The following correlation information is provided:

- “Link down” on the PE
  - The “ip interface status down” alarm on the PE is correlated to the “link down” alarm
  - The “device unreachable”alarm on the CE is correlated to the “link down” alarm on the PE
  - The traps and syslogs for the sub interface are correlated to the “link down” alarm on the PE

Interface Registry Parameters

"ip interface status down"

The following "ip interface status down" parameters can be controlled through the Registry:

- is-correlation-allowed
- severity
- timeout
- expiration-time
- flow-activation-message
- flow-delay
- time-stamp-delay
- weight
- is-ticketable

Note For more information about these parameters see the Event and Alarm Configuration Parameters chapter.

"All ip interfaces down"

The following "All ip interfaces down" parameters can be controlled through the Registry:

- is-correlation-allowed
- is-ticketable
- severity
- activate-flow
- correlate
- timeout
- expiration-time
- weight

Note For more information about these parameters see the Event and Alarm Configuration Parameters chapter.

CHAPTER 4

Correlation Over Unmanaged Segments

This chapter describes how Cisco ANA performs correlation decisions over unmanaged segments, namely, clouds.

Cloud VNE describes managing more than one network segment that interconnects with others, over another network segment which is not managed.

Cloud Problem Alarm describes the “cloud problem” alarm, its correlation and provides an example.

Cloud VNE

In some scenarios Cisco ANA is required to manage more than one network segment that interconnects with others over another network segment which is not managed. In such setups, faults on one device might be correlated to faults on another device that is located on the other side of the unmanaged segment of the network or to unknown problems in the unmanaged segment itself.

A virtual cloud is used for representing unmanaged network segments. It represents the unmanaged segment of the network as a single device that the two managed segments of the network are connected to, and has that device simulate the workings of the unmanaged segment.

Virtual clouds support specific network setups. The types of unmanaged networks that are supported are:

- Frame-Relay
- ATM
- Ethernet.

Fault Correlation Across the FR/ATM/Ethernet Cloud

When a Layer 3 or 2 event (e.g. reachability problem, neighbor change, FR DLCI down, ATM PVC down) occurs, it triggers a flow along the physical and logical path modeled on the VNEs. This is done in order to correlate to the actual root-cause of this fault. If the flow passes over a *cloud* along the ‘path flow’ it marks it as a potential root-cause for the fault. If there is no other root-cause found on the managed devices, then the *cloud* becomes the root-cause. A ticket is then issued and the original event correlates to it.

Cloud Problem Alarm

For some events, when there is no root cause found, a special alarm is created, namely, “cloud problem.” These events are then correlated to the alarm.

- The “cloud problem” alarm has a Major severity and is automatically cleared after a delay.

The following parameter can be controlled through the Registry for each event type:

- correlate-to-cloud

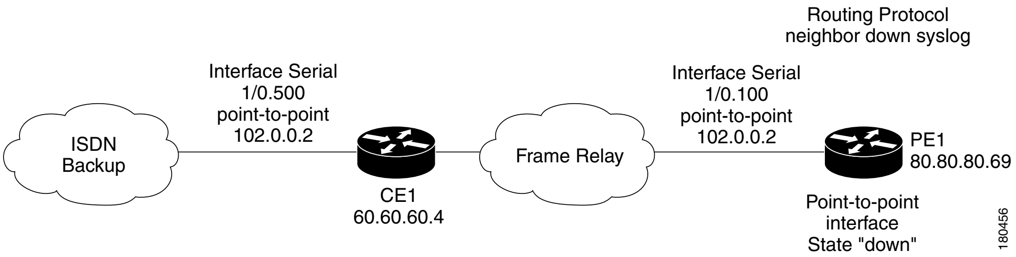
Note For more information about this parameter see the Event and Alarm Configuration Parameters chapter.

Note The “correlate-to-cloud” parameter enables or disables the ability of an alarm to create a "cloud problem" alarm and to correlate to it. The default value is "false" for all alarms in the system, meaning that an alarm does not correlate to the "cloud problem" alarm by default. However, there are several alarms that override the default configuration and are set to "true":
BGP neighbor loss syslog
OSPF neighbor loss syslog
EIGRP syslog
CISCO IGRP syslog.

Cloud Correlation Example

In this example two devices that have OSPF configured are connected through a cloud. A malfunction occurs inside the unmanaged network that causes the “OPSF neighbor down” alarm to be generated. In this case the “OSPF neighbor down” alarm is correlated to the “cloud problem.”

Figure 4-1 Cloud Correlation Example



On the PE1 device,the “OSPF neighbor down” alarm was received and no root cause was detected in any of the managed devices. A disconnected link inside the unmanaged network caused the “OSPF neighbor down” alarm. The following alarms are generated and correlated:

- “Cloud problem” on the Cloud
  - “OSPF neighbor down” on the P1 is correlated to the “Cloud problem” alarm

Event and Alarm Configuration Parameters

This chapter describes the different options that exist to modify the alarm behavior by editing the appropriate alarm parameters in the system registry.

Alarm Type Definition describes the alarm type concept.

Event (Sub-Type) Configuration Parameters describes the event and alarm configuration parameters, and values that can be controlled through the Registry.

The parameters described in the following section are defined per event (sub-type) that belongs to the alarm.

Note Changes to the Registry should only be carried out with the support of Cisco Professional Services.

Alarm Type Definition

The alarm type serves as an identifier which enables group events from different sub-types to share the same type and source in a single event sequence.

The event sub-type is a specific occurrence of fault in the network. For example, link down and link up are two sub-types that share the same type.

Event (Sub-Type) Configuration Parameters

General Event Parameters

Parameter Name	Description	Permitted Values
severity	Severity level of the event.	Either: • CRITICAL • MAJOR • MINOR • WARNING • CLEARED • UNKNOWN • INFO
is-ticketable	Determines whether the alarm will generate a new ticket (in case there is no root-cause alarm to correlate to).	True (ticketable); False (not ticketable)
functionality-type	Determines the event type.	Either: • Service (Sheer-generated) • Syslog • SNMP Trap

Root-Cause Configuration Parameters

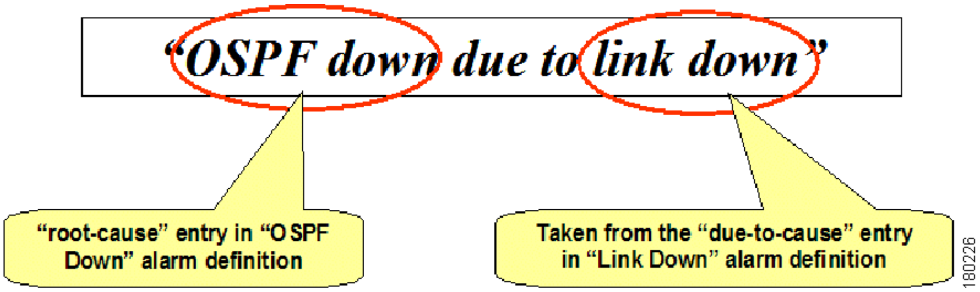
These parameters define the behavior of the alarm when serving as the root-cause of other alarms.

Name	Description	Permitted Values
is-correlation-allowed	Defines whether the alarm may serve as a root-cause, and allow child alarms to correlate to it.	True (correlates) or False (will not correlate)
root-cause (also: short description)	Textual description that describes the event.	User defined text
due-to-cause	Display string that will be given to the consequent alarms (which correlate to this alarm).	User defined text
timeout	Defines time period allowed (in milliseconds) for consequent alarms to correlate to this alarm.	Positive integer

Name	Description	Permitted Values
gw-correlation-timeout	The period of time (in milliseconds) for how long an alarm with the severity 'Clear' or 'Info' (alarms with non-cleared severity are always open for a consequent alarm) is open for sequence.	Positive integer
is-correlation-allowed-when-not-correlated	If and only if this alarm is not correlated to a parent alarm it determines if the alarm may serve as root-cause, and allow child alarms to correlate to it.	True/False

The following figure explains the difference between "Root-cause" and "Due-to-cause":

Figure 5-1 Root-Cause vs. Due-to-Cause


"OSPF down due to link down"
"root-cause" entry in "OSPF Down" alarm definition
Taken from the "due-to-cause" entry in "Link Down" alarm definition
180226

Correlation Configuration Parameters

These parameters define the behavior of the alarm in finding its root-cause alarm.

Name	Description	Permitted values
correlate	Determines whether the alarm should attempt to find and correlate to a root-cause alarm. If this parameter is set to true at least box level correlation will be performed.	True/False
correlate-to-cloud	Determines whether a special alarm is created for some events, when there is no root cause found. These events are then correlated to the alarm.	True/False False for all events except for: • BGP neighbor loss syslog • OSPF neighbor loss syslog • EIGRP syslogs • Cisco IGRP syslogs

Name	Description	Permitted values
send-uncorrelated	Determines whether to continue processing the event even when a root-cause alarm was not found.	True/False
correlation-delay	Period of time (in milliseconds) to wait before attempting to find and correlate to a root-cause – Obsolete Parameter.	Positive integer
expiration-time	Period of time (in milliseconds) required to wait before attempting to find a root-cause. It also controls when an event will become an alarm (if it is ticketable and did not correlate to some other alarm prior to the expiration of this interval)	Positive integer
time-stamp-delay	Used for "normalization" of the event occurrence time. The value (in milliseconds) is subtracted from the event time, to compensate for the time difference with the root-cause alarm). It is also used for running the network correlation against the historic network configuration	Positive integer
drop-event	Whether event should be dropped on VNE level – not forwarded to GW level.	True/False

Network Correlation Parameters

These parameters control the alarm's behavior in initiating an active correlation-search flow.

Name	Description	Permitted values
activate-flow	Determines whether to initiate Network level correlation.	True/False
flow-delay	Defines the time (in milliseconds) to wait before initiating the network correlation flow. Increasing this value causes the alarm to wait longer before attempting correlation. If this value is too high the correlation will be meaningless as it will show events that happened a very long time ago. Decreasing this value causes the alarm to wait a shorter period of time before attempting correlation.	Positive integer
flow-activation-message	Identifies the flow process functionality	IPBasedActiveFlowTriggerMessage
alarm-min-age	Defines how old (at least) the alarm should be in order to be a root-cause for a specified event.	Positive integer

Name	Description	Permitted values
flow-ttl	How many DCM hops may the flow trace before being stopped	Positive integer
weight	Defines the weight of an alarm as a correlation candidate. The "heavier" the alarm the more likely it will be chosen as root cause.	-2 – weightless or -1 – maximum weight or Positive integer

Note All delays should be smaller than expiration time to allow correlation to take place. Flow activation delay is being counted only when the correlation delay has expired.

Flapping Event Definitions Parameters

These parameters control the alarm's behavior in setrn=mining its flapping state.

Name	Description	Permitted values
Enabled	Is the flapping enabled for this event.	True/False
Flapping interval	The maximum amount of time (in milliseconds) between two alarms which can be considered as a flapping change.	Positive integer
Flapping threshold	After this amount of changes (each change arriving at an interval lower then the "flapping interval"), the event will be considered as flapping.	Positive integer
Update interval	After this interval (in milliseconds) an update will be sent	Positive integer

Name	Description	Permitted values
Clear interval	The amount of time (in milliseconds) an event has to stay in one state to be considered as a normal alarm and not in a flapping state	Positive integer
Update threshold	After this number of flapping alarms, an update will be sent to the Gateway updating the alarm with the number of events received.	Positive integer

Impact Analysis

This chapter describes the impact analysis functionality available in Cisco ANA 3.5.1.

Impact Analysis Options describes automatic and proactive impact analysis.

Impact Report Structure describes the structure of the impact report that is generated.

Affected Severities describes the severities used for automatic impact analysis.

Impact Analysis GUI (Cisco ANA NetworkVision) describes how the user can view impact analysis information in Cisco ANA NetworkVision.

Enabling/Disabling Impact Analysis describes enabling and disabling impact analysis for specific alarm and which alarms support this feature.

Accumulating Affected Parties describes how Cisco ANA NetworkVision automatically calculates the accumulation of affected parties during automatic impact analysis.

Impact Analysis Options

Impact analysis is available in two modes:

- Automatic Impact Analysis – when a fault occurs which has been identified as potentially service affecting, Cisco ANA automatically generates the list of potential and actual service resources that were affected by the fault and embeds this information in the ticket along with all of the correlated faults.

  Note This only applies to specific alarms (not every alarm initiates affected calculation).

- Proactive Impact Analysis – Cisco ANA provides ‘what-if’ scenarios for determining the *possible* affect of network failures. This enables on-demand calculation of affected service resources for every link in the network, thus enabling an immediate service availability check and analysis for potential impact and identification of critical network links. Upon execution of the ‘what-if’ scenario, the Cisco ANA fabric initiates an end-to-end flow, which determines all the potentially affected edges.

Note For more information about fault scenarios which are considered as service affecting in an MPLS network and supported by Cisco ANA please refer to the *Cisco ANA MPLS User's Guide*.

Note As mentioned, each fault which has been identified as potentially service affecting triggers a generation of impact analysis calculation event if it is reoccurring in the network.

This chapter describes mainly the automatic impact analysis. For more information about proactive impact analysis please refer to the *Cisco ANA NetworkVision User's Guide*.

Impact Report Structure

The impact report contains a list of pairs of end-points when the service between them has been affected.

Each end-point has the following details:

- **End-Point Physical\logical location**—An end point can be a physical entity (for example a port) or a logical one (for example a sub-interface). The impact report contains the exact location of the entity. All the location identifiers start with the ID of the device which holds the End-point. The other details in the location identifier are varied according to the end-point type e.g.: VC\VP, IP interface.
- **Business Tag Properties** (If attached to the entity)—Key, Name, Type.

Note For specific information about the report structure in MPLS networks please refer to the *Cisco ANA MPLS User's Guide.*

Affected Severities

In automatic mode, the affected parties can be marked with one of the following severities:

- **Potentially affected**—The service might be affected but its actual state is not yet known
- **Real affected**—The service is affected.
- **Recovered**—The service is recovered. This state relates only to entries that were marked previously as potentially affected. It indicates only the fact that there is an alternate route to the service, regardless of the service quality (level).
- The initial impact report might mark the services as either 'Potentially' or 'Real' affected. As time progresses and more information is accumulated from the network, the system might issue additional reports to indicate which of the potentially affected parties are 'Real' or 'Recovered'.
- The indications for these states are available both through the API and in the GUI.

Note The reported impact severities vary between fault scenarios. For more information about fault scenarios in an MPLS network please refer to the *Cisco ANA MPLS User's Guide*.

Note There is no 'clear' state for the affected services when the alarm is cleared.

Impact Analysis GUI (Cisco ANA NetworkVision)

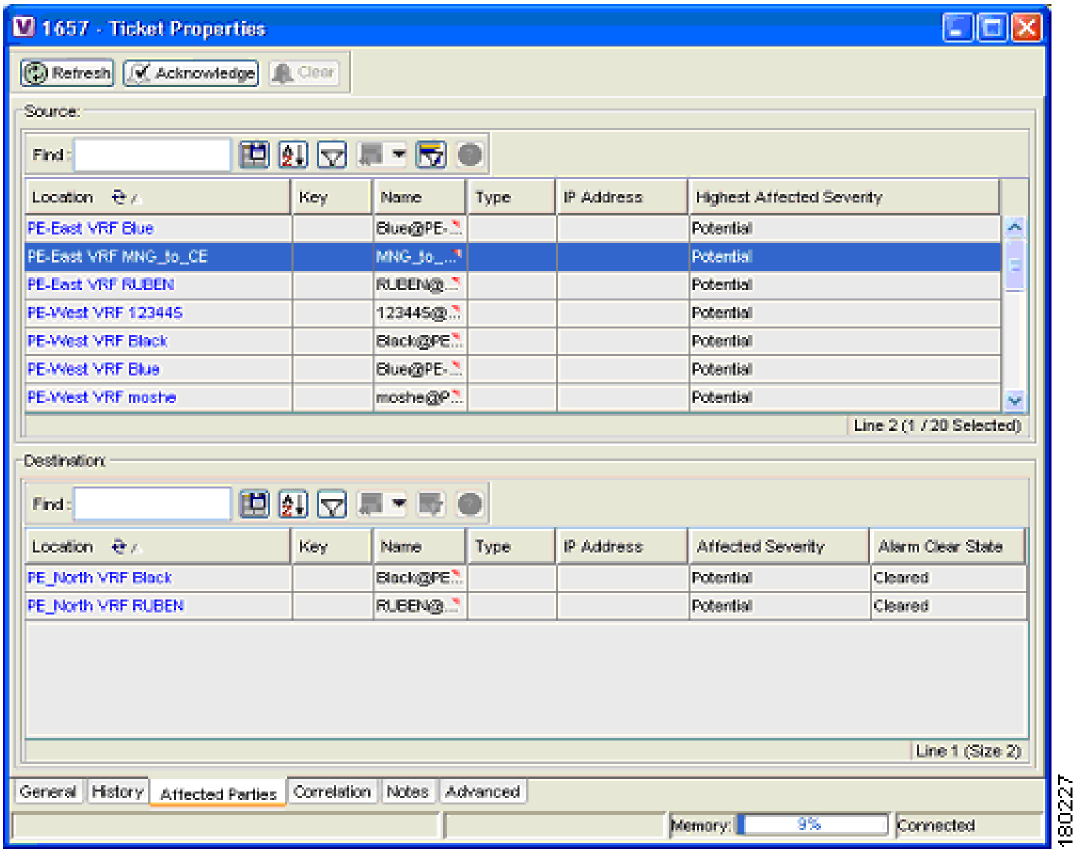
The Impact Analysis GUI available in Cisco ANA NetworkVision displays the list of affected service resources which is embedded in the ticket information. This section describes the GUI presentation of this list.

Affected Parties Tab

The **Affected Parties** tab displays the service resources (affected pairs) that are affected (automatic impact analysis) for Event, Alarm or a ticket (depending on which properties window is opened). In the case of an alarm or a ticket, Cisco ANA NetworkVision automatically calculates the accumulation of affected parties of all the subsequent events. For more information about accumulating affected parties, see the Viewing a Detailed Report for the Affected Pair section.

The **Affected Parties** tab is displayed below.

Figure 6-1 Affected Parties Tab



Source:

Location	Key	Name	Type	IP Address	Highest Affected Severity
PE-East VRF Blue		Blue@PE-...			Potential
PE-East VRF MNG_to_CE		MNG_to_...			Potential
PE-East VRF RUBEN		RUBEN@...			Potential
PE-West VRF 123445		123445@...			Potential
PE-West VRF Black		Black@PE...			Potential
PE-West VRF Blue		Blue@PE-...			Potential
PE-West VRF moshe		moshe@P...			Potential

Line 2 (1 / 20 Selected)

Destination:

Location	Key	Name	Type	IP Address	Affected Severity	Alarm Clear State
PE_North VRF Black		Black@PE...			Potential	Cleared
PE_North VRF RUBEN		RUBEN@...			Potential	Cleared

Line 1 (Size 2)

The **Affected Parties** tab is divided into two areas, namely, **Source** and **Destination**. The **Source** area displays the set of affected elements (A side and Z side). The following columns are displayed in the **Affected Parties** tab providing information about the affected parties:

- **Location**—A hyperlink that opens the Inventory window, highlighting the port with the affected parties.

- **Key**—The unique value taken from the affected element's business tag key (if it exists).
- **Name**—The sub-interface (site) name or business tag name of the affected element (if it exists). For more information, refer to the *Cisco Active Network Abstraction Managing MPLS User's Guide*.
- **Type**—The business tag type.
- **IP Address**—If the affected element is an IP interface the IP address of the sub-interface (site) is displayed. For more information, refer to the *Cisco Active Network Abstraction Managing MPLS User's Guide*.
- **Highest Affected Severity**—The severest affected severity for the affected pair (Destination). The same source can be part of multiple pairs, and therefore each pair can have different affected severities. The highest affected severity reflects the highest one among these. The affected pair can have one of the following severities:
  - **Potential**
  - **Real**
  - **Recovered**
  - **N/A:** From *Links* view this indicates not relevant.

When an affected side (a row) is selected in the **Source** area the selected element's related affected pairs are displayed in the **Destination** area.

The following additional columns are displayed in the **Destination** area table in the Ticket Properties window:

- **Affected Severity**—The severity of the affected pair as calculated by the Client according to the rules defined, above.
- **Alarm Clear State**—An indication for each pair of the clear state of the alarm. The following states exist:
  - **Not Cleared**vThere are one or more alarms that have not been cleared for this pair.
  - **Cleared**—All of the related alarms for this pair have been cleared.

In addition, you can view a detailed report for every affected pair that includes a list of the events that contributed to this affected pair.

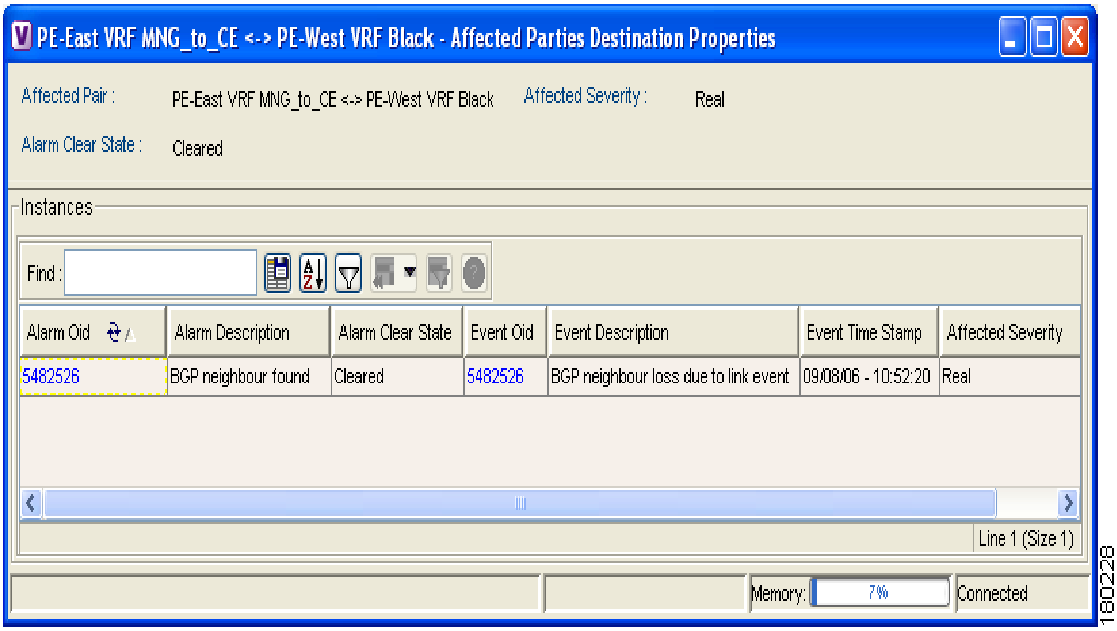
Viewing a Detailed Report for the Affected Pair

Cisco ANA NetworkVision enables you to view a detailed report for every affected pair. The detailed report includes a list of the events that contributed to the affected pair.

For information about how to reach a detailed affected report please refer to the *Cisco Active Network Abstraction NetworkVision User's Guide* for more information.

The Affected Parties Destination Properties dialog box is displayed.

Figure 6-2 Detailed Report for the Affected Pair



PE-East VRF MNG_to_CE <-> PE-West VRF Black - Affected Parties Destination Properties

Affected Pair : PE-East VRF MNG_to_CE <-> PE-West VRF Black
Affected Severity : Real
Alarm Clear State : Cleared

Instances

Alarm Oid	Alarm Description	Alarm Clear State	Event Oid	Event Description	Event Time Stamp	Affected Severity
5482526	BGP neighbour found	Cleared	5482526	BGP neighbour loss due to link event	09/08/06 - 10:52:20	Real

Line 1 (Size 1)

Memory: 7% Connected

The following fields are displayed at the top of the Affected Parties Destination Properties dialog box:

- **Affected Pair**—The details of A side and Z side of the affected pair.
- **Alarm Clear State**—An indication for each pair of the clear state of the alarm. The following states exist:
  - **Not Cleared**—There are one or more alarms that have not been cleared for this pair.
  - **Cleared**—All of the related alarms for this pair have been cleared.
- **Affected Severity**—The severity of the affected pair as calculated by the Client according to the rules defined in the Viewing a Detailed Report for the Affected Pair section.
- **Name**—The name of the destination from which you opened the detailed report.

Each row in the **Instances** table represents an event that was reported for the affected pair. The following columns are displayed in the **Instances** table of the Affected Parties Destination Properties dialog box:

- **Alarm OID**—The ID of the alarm to which the event is correlated as a hyperlink to the relevant alarm’s properties.
- **Alarm Description**—A description of the alarm to which the event is correlated.
- **Alarm Clear State**—The alarm’s calculated severity.
- **Event OID**—The ID of the event as a hyperlink to the relevant event’s properties.
- **Event Description**—A description of the event.
- **Event Time Stamp**—The event’s time stamp. The date and time of the event.
- **Affected Severity**—The actual affected severity of the pair that was reported by the selected event.

Enabling/Disabling Impact Analysis

You can disable impact analysis for a specific alarm. This option can be set in the Cisco ANA Registry. If impact analysis is disabled the system will report the event with no impact information. The settings can be changed dynamically during system runtime.

The following alarms support this feature:

- Link Down
- Port Down
- Dropped / Discarded packets
- MPLS Black Hole
- BGP Neighbor Down.
- MPLS TE Tunnel Down
- L2 Tunnel down (Martini)

Accumulating Affected Parties

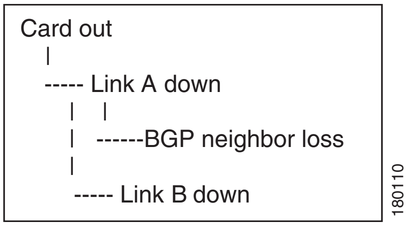
This section describes how Cisco ANA NetworkVision automatically calculates the accumulation of affected parties during automatic impact analysis. This information is embedded in the ticket along with all of the correlated faults.

In the example below the following types of alarms exist in the correlation tree:

- Ticket root-cause alarm (“Card Out”).
- An alarm which is correlated to the root-cause and has other alarms correlated to it (“Link A down”).
- An alarm with no other alarms correlated to it (“Link B down” & “BGP neighbor loss”).

An event sequence is correlated to each of these alarms.

Figure 6-3 Correlation Tree Example



For each type of alarm Cisco ANA NetworkVision provides a report of the affected parties. This report includes the accumulation of:

- The affected parties reported on all the events in the alarm event sequence (this also applies to flapping alarms).
- The affected parties reported on the alarms that are correlated to it.

Each report includes the accumulation of the affected report of all the events in its own correlation tree.

For example, in the diagram:

- “BGP neighbor loss” includes the accumulation of the affected report of its own event sequence.

- “Link A down” includes the accumulation of the report of its own event sequence. In addition, it includes the report of the BGP neighbor loss.

Accumulating the Affected Parties in an Alarm

When there are two events that form part of the same event sequence in a specific alarm the reoccurring affected pairs are only displayed once in the **Affected Parties** tab. Where there are different affected severities reported for the same pair, the pair is marked with the severity that was reported by the latest event, namely, according to the **time stamp**.

Accumulating the Affected Parties in the Correlation Tree

Where there are two or more alarms:

- That are part of the same correlation tree
- That report on the same affected **pair of edge** points and
- That have **different affected severities**

Then the reoccurring affected pairs are only displayed once in the **Affected Parties** tab. Where there are different affected severities reported for the same pair, the pair is marked with the **highest severity**.

In this example X&Y are the OIDs of edge points in the network and there is a service running between them. Both of the alarms “Link B down” and “BGP neighbor loss” report on the pair “X<->Y” as affected:

- “Link B down” reports on “X<->Y” as “Potentially” affected.
- “BGP neighbor loss” reports on “X<->Y” as “Real” affected.

The affected severity priorities are:

- Real – Priority 1
- Recovered – Priority 2
- Potentially – Priority 3

“Card out” reports on “X<->Y” as “Real” affected only once.

Updating Affected Severity Over Time

Cisco ANA has the ability to update the affected severity of the same alarm (report) over time due to the fact that in some cases the affect of the fault on the network cannot be determined until the network has converged.

For example, a “Link Down” alarm creates a series of affected severity updates over time. These updates are added to the previous updates in the system database. In this case the system provides the following reports:

- The first report of a “Link Down” reports on “X<->Y” as **Potentially** affected.
- Over time the VNE identifies that this service is **Real** affected or **Recovered** and generates an updated report.
- The **Affected Parties** tab of the Ticket Properties dialog box displays the latest severity, namely, **Real** affected.

- The Affected Parties Destination Properties dialog box displays both reported severities.

This functionality is currently only available in the link down scenario in MPLS Networks.

Supported Service Alarms

This appendix provides the list of service alarms that are supported by Cisco ANA 3.5.1.

Note If the source of the alarm is an interface with technology, which is not supported by Cisco ANA, then the alarm will not be generated.

Note If the source of the alarm is an entity, which is not modeled by Cisco ANA, (for example, an unsupported module), then the alarm will not be generated.

The columns that are displayed in the tables that follow, relate to the configuration parameters described in this guide. For more information about these parameters see Event (Sub-Type) Configuration Parameters.

The following table lists the supported service alarms:

Table A-1 Service Alarms

Item	Name	Description	is-correlation-allowed	correlate	is-ticketable	severity	weight
1.	Primary HSRP interface is not active/Primary HSRP interface is active	Sent when an active HSRP group member is not active anymore (a link was shut down)	true	true	true	MAJOR	-2
2.	Secondary HSRP interface is active/Secondary HSRP interface is not active	Secondary member of an HSRP group is active	true	true	true	MAJOR	-2
3.	All ip interfaces down/Active ip interfaces found	Sent when all ip interfaces configured above a physical port change oper status to "down"	true	true	true	MAJOR	4000

Table A-1 Service Alarms

Item	Name	Description	is-correlation -allowed	correlate	is-ticketable	severity	weight
4.	Interface status down/up	Sent when an ip interface changes oper status to “down”	true	true	true	MAJOR	3000
5.	Card in / out	Card in / out	true	true	true	MAJOR	maximum
6.	Link down / up	Link down / up	true	true	true	CRITICAL	maximum
7.	Device Unreachable	The device is no longer reachable.	true	true	true	MAJOR	3000
8.	CPU Over Utilized	The device CPU percentage has passed the configured threshold.	true	true	true	MAJOR	1000
9.	Memory Over Utilized	The device memory utilization has passed the configured threshold	true	true	true	MAJOR	1000
10.	Device Unsupported	The device is not supported in ANA.	false	true	true	CRITICAL	-2
11.	Discard Packets	The port discard packets value has passed the configured settings.	true	true	true	MINOR	4000
12.	Dropped Packets	The port dropped packets value has passed the configured settings.	true	true	true	MINOR	4000
13.	Module Unsupported	The module is not supported in ANA.	false	true	true	CRITICAL	-2
14.	Port Flapping	Port changing state frequently.	false	true	true	CRITICAL	5000
15.	Port Down	Port Down	true	true	true	MAJOR	5000
16.	Rx Over Utilized	The percentage of the traffic on the port passed the configured threshold.	true	true	true	MINOR	2000
17.	Tx Over Utilized	The percentage of the traffic on the port passed the configured threshold.	true	true	true	MINOR	2000

Table A-1 Service Alarms

Item	Name	Description	is-correlation-allowed	correlate	is-ticketable	severity	weight
18.	VPN Leak	Upon detection of a link between VPNs the system issue a VPN Leak alarm to alert the user of possible security breach (Disabled by default)	false	true	true	INFO	-2
19.	Cloud Problem	A problem in an unmanned segment	true	false	true	MAJOR	2000
20.	Concurrent Backup & Primary Port	Backup & primary ports are up.	false	false	true	MAJOR	-2
21.	Backup Interface Warning	Warning ticket for backup interface being up after a predefined period of time	false	true	true	INFO	-2
22.	Broken LSP discovered	-	true	true	true	MAJOR	100
23.	MPLS Black hole	-	true	true	true	WARNING	100
24.	Layer 2 Tunnel Down	When a martini tunnel goes down	true	true	true	MINOR	100
25.	MPLS TE Tunnel Down/Flapping	When a Traffic engineering tunnel goes down	true	true	true	MAJOR	500
26.	BGP Neighbor Down	When a BGP neighbor (both BGP routers are managed) is changing state from established	true	true	true	CRITICAL	-2

Supported Traps and Syslogs

This appendix provides the list of Cisco traps and syslogs that are supported in Cisco ANA 3.5.1.

Syslogs Supported by Cisco Devices

Traps Supported by Cisco Devices

Note If the source of the alarm is an interface with technology, which is not supported by Cisco ANA, then the syslogs and traps will not be parsed and will be generated generically.

Note If the source of the alarm is an entity, which is not modeled by Cisco ANA, (for example, an unsupported module), then the syslogs and traps will not be parsed and will be generated generically.

The columns that are displayed in the tables that follow, relate to the configuration parameters described in this guide. For more information about these parameters see Event (Sub-Type) Configuration Parameters.

Syslogs Supported by Cisco Devices

The following table lists the supported proprietary Cisco syslogs .

Table B-1 Cisco Syslogs

Item	Name	Severity	Description	is-correlation-allowed	correlate	is-ticketable
1	DUAL-3-SIA	INFO	The EIGRP router hasn't received a reply to a query from one or more neighbors within the time allotted, so it clears the neighbors that didn't send a reply	false	true	true
2	AMDP2_EF-5-COLL	INFO	Ethernet or Fast Ethernet is seeing multiple collisions. This problem may occur under heavy loads	false	true	false
3	AMDP2_FE-5-LATECOLL	MINOR	Late collisions have occurred on the Ethernet or Fast Ethernet interface	false	true	false

Table B-1 Cisco Syslogs (continued)

Item	Name	Severity	Description	is-correlation-allowed	correlate	is-ticketable
4	BGP-5-ADJCHANGE / BGP-5-ADJCHANGE-vrf	MAJOR	Adjacent BGP neigbour was lost	false	true	true
5	BGP-3-NOTIFICATION	INFO	Handles BGP 3 syslog	false	true	true
6	OIR-6-(REM| INS)CARD	MAJOR	Handle module out syslog	false	true	true
7	DEC21140-5-COLL	MINOR	A Fast Ethernet packet has been dropped because too many attempts to transmit it were stopped by collisions	false	true	false
8	DEC21140-5-LATECOLL	MINOR	A Fast Ethernet packet has been dropped because too many attempts to transmit it were stopped by collisions	false	true	false
9	FR-5-DLCICHANGE	MAJOR	FR DLCI down syslog	false	true	true
10	ISDN-6-LAYER2DOWN	MAJOR	Isdn 6 disconnect	false	true	false
11	Dual-5-NBCHANGE	MAJOR	Handle EIGRP syslog	false	true	true
12	CDP-4-DUPLEX_MISMATCH	INFO	This messages indicates a duplex mismatch problem	false	false	true
13	LANCE-3-BADCABLE	MINOR	The Ethernet cable is not connected	false	true	false
14	LAPB-4-CTRLBAD	MINOR	A received FRMR has reported a frame with an invalid control code	false	true	true
15	ILACC-5-COLL	MINOR	An Ethernet cable is broken or is not terminated, or the transceiver is unplugged	false	true	true
16	ILACC-5-LATECOLL	MINOR	An Ethernet transceiver is malfunctioning, the Ethernet is overloaded, or the Ethernet cable is too long	false	true	true
17	IPX-3-BADIGPSAP	MINOR	A hardware or software error occurred	false	true	true
18	CLNS-5-ADJCHANGE	MAJOR	IS-IS Neighbor Down	false	true	true
19	LANCE-5-COLL	INFO	An Ethernet cable is broken or unterminated, or the transceiver is unplugged	false	true	false
20	LANCE-5-LATECOLL	MINOR	An Ethernet transceiver is unplugged or defective	false	true	true

Table B-1 Cisco Syslogs (continued)

Item	Name	Severity	Description	is-correlation-allowed	correlate	is-ticketable
21	LINEPROTO-5-UP DOWN	MAJOR	Line Down	false	true	false
22	LINK-3-UPDOWN	MAJOR	Link Down 3 Syslog	false/true	true	false
23	LINK-5-CHANGED	MAJOR	Link Down 5 Syslog	false/true	true	false
24	SYS-2-MALLOCFAIL	MINOR	The requested memory allocation is not available from the specified memory pool	false	true	true
25	PQUICC-5-COLL	MINOR	An Ethernet cable is broken or is not terminated	false	true	true
26	PQUICC-5-LATECOLL	MINOR	The Ethernet cable might be too long, or there could be too many repeaters with the result that the delay from one end to the other is too long	false	true	true
27	PQUICC_FE-5-LATECOLL	MINOR	A new network may not have been engineered properly or adding a regenerator to an existing network may have changed the network specifications	false	true	true
28	PQUICC_FE-5-COLL	MINOR	Ethernet or Fast Ethernet is detecting multiple collisions	false	true	true
29	PQUICC_FE-5-LATECOLL	MINOR	Late collisions have occurred on the Ethernet or Fast Ethernet interface	false	true	true
30	SYS-3-CPUHOG	MINOR	The indicated process ran too long without relinquishing the processor	false	true	true
31	PQUICC_ETHER-5-COLL	MINOR	An Ethernet cable is broken or is not terminated	false	true	true
32	QUICC_ETHER-5-LATECOLL	MINOR	A new network may not have been engineered properly or adding a regenerator to an existing network may have changed the network specifications	false	true	true
33	SCHED-3-STUCKMTMR	MINOR	A process can register to be notified when various events occur in the router. This message indicates that a registered timer is expired and its value is unchanged after the process has executed two successive times	false	true	true
34	SYS-5-RELOAD	INFO	Reloading Device	false	true	false
35	SECURITY-1-PORT SHUTDOWN	MINOR	This message indicates that a port has been shut down due to an insecure host sourcing a packet into that port	false	true	true

Table B-1 Cisco Syslogs (continued)

Item	Name	Severity	Description	is-correlation-allowed	correlate	is-ticketable
36	SNMP-5-LINKTRAP	MINOR	This message indicates the type of Link Trap	false	true	true
37	SNMP-5-SNMPAUTHFAIL	MINOR	This message indicates that the switch has received an SNMP message that was not properly authenticated	false	true	true
38	SNMP-5-TOPOTRAP	MINOR	This message indicates that a configured port changed from the learning state to the forwarding state, or from the forwarding state to the blocking state	false	true	true
39	SYS-5-CONFIG_I	INFO	The router's configuration was changed	true	true	true/false
40	SYS-5-RESTART	INFO	Syslog for restarting the device	false	true	true
41	UDLD-3-DISABLE FAIL	MINOR	This message indicates that a fault was detected in the wiring on a fiber Ethernet port, but UDLD could not disable the port	false	true	true
42	UDLD-3-DISABLE	MINOR	This message indicates that a fault has been detected in a fiber Ethernet port connection and that the port has been disabled to prevent other protocols from malfunctioning	false	true	true
43	OSPF-5-ADJCHG	MINOR	This indicates a change in the OSPF neighbor stat	false	true	true
44	UDLD-4-ONEWAY PATH	MINOR	This message indicates that a fault has been detected in a fiber Ethernet connection in a shared media environment and that the connection may cause a possible malfunction	false	true	true
45	STANDBY-6-STATE CHANGE	INFO	HSRP group change notification	false	true	true
46	DTP-5-NONTRUNK PORTON	MINOR	Dtp 5 non port trunk syslog	false	true	true
47	AT-6-NODEWRON G	MINOR	At 6 node wrong	false	true	false
48	SPANTREE-2-RX_ PORTFAST	MINOR	Span tree 2 rx port	false	true	true
49	SPANTREE-2-LOOPGUARDBLOCK	MINOR	Span tree 2 loop guard block	false	true	true
50	SPANTREE-2-LOOPGUARDUNBLOCK	MINOR	Span tree 2 loop guard un block	false	true	true

Table B-1 Cisco Syslogs (continued)

Item	Name	Severity	Description	is-correlation-allowed	correlate	is-ticketable
51	QUICC_ETHER-5-COLL	MINOR	Quicc ether 5 coll	false	true	true
52	ISDN-6-DISCONNECT	MAJOR	Isdn 6 disconnect	false	true	false

Traps Supported by Cisco Devices

The following table lists the supported MIB-II & Cisco proprietary traps. The trapslisted in this table are the most commonly used.

Table B-2 Cisco Traps

Item	Name	Severity	OID	is-correlation-allowed	correlate	is-ticketable
1	Authentication Failure	INFO	1.3.6.1.4.1	false	false	false
2	BGP Trap	MINOR	.1.3.6.1.2.1.15.3.1	false	true	false
3	hdsl2shdsl-dc-continuity-fault	INFO	1.3.6.1.2.1.10.48.0.12	false	true	true
4	Chassis Alarm On	MINOR	1.3.6.1.4.1.9.5.0	true	true	true
5	Chassis Temperature Major Fault	MAJOR	1.3.6.1.4.1.9.5.1.2.13	false	true	true
6	Chassis Temperature Minor Fault	MINOR	1.3.6.1.4.1.9.5.1.2.13	false	true	true
7	Chassis Temperature Other Fault	MINOR	1.3.6.1.4.1.9.5.1.2.13	false	true	true
8	Ent Config Change	INFO	1.3.6.1.2.1.47.2.0.1	false	true	true
9	Fan Down	MAJOR	1.3.6.1.4.1.9.9.13.3.0.4	false	true	true
10	FR Dlci Status Change	INFO	1.3.6.1.2.1.10.32.0.1	false	true	true
11	Line Down Cisco Prop	INFO	1.3.6.1.4.1.9.9.41.2	false	true	false
12	Line Down / Up	MINOR		false	true	false
13	hdsl2shdsl-config-init-failure	INFO	1.3.6.1.2.1.10.48.0.13	false	true	true
14	VRRP Trap Auth Failure	MINOR	1.3.6.1.2.1.68.0.2	false	true	true
15	VRRP Trap New Master	MINOR	1.3.6.1.2.1.68.0.1	false	true	true

Table B-2 Cisco Traps (continued)

Item	Name	Severity	OID	is-correlation-allowed	correlate	is-ticketable
16	Warm Start	INFO		false	true	true
17	Cold Start	INFO		false	true	true
18	dot1qBridge trap	INFO	1.3.6.1.2.1.17.0.2	false	true	false
19	Vlan trunk port dynamic status	INFO	1.3.6.1.4.1.9.9.46.2.0.7	false	true	false
20	dlsw circuit down trap	INFO	1.3.6.1.2.1.46.1.0	false	true	true
21	hdsl2shdsl service fault v2 trap	INFO	1.3.6.1.2.1.10.48.0.11	false	true	true
22	bgp-established-trap _v2	CLEARED	1.3.6.1.2.1.15.7.1	false	false	false
23	bgp-backward-transition-trap_v2	MINOR	1.3.6.1.2.1.15.7.2	false	true	false
24	tcp connection table	INFO	1.3.6.1.4.1.9.2.6.1.1	false	false	dump
25	lts table	INFO	.1.3.6.1.4.1.9.2.9	false	false	dump
26	clogHistoryTable trap	INFO	.1.3.6.1.4.1.9.9.41.1.2.3.1	false	false	dump
27	hdsl2shdsl-local-power-loss	INFO	1.3.6.1.2.1.10.48.0.16	false	true	true
28	hdsl2shdsl-loop-atten-crossing	INFO	1.3.6.1.2.1.10.48.0.1	false	true	true
29	hdsl2shdsl-loopback-failure	INFO	1.3.6.1.2.1.10.48.0.9	false	true	true
30	hdsl2shdsl-no-neighbor-present	INFO	1.3.6.1.2.1.10.48.0.15	false	true	true
31	hdsl2shdsl-perf-crc-anomalies-thresh	INFO	1.3.6.1.2.1.10.48.0.5	false	true	true
32	hdsl2shdsl-perf-los-ws-thresh	INFO	1.3.6.1.2.1.10.48.0.3	false	true	true
33	hdsl2shdsl-perf-los-ws-thresh	INFO	1.3.6.1.2.1.10.48.0.6	false	true	true
34	hdsl2shdsl-perf-ses-thresh	INFO	1.3.6.1.2.1.10.48.0.4	false	true	true
35	hdsl2shdsl-perf-uas-thresh	INFO	1.3.6.1.2.1.10.48.0.7	false	true	true
36	hdsl2shdsl-power-back-off	INFO	1.3.6.1.2.1.10.48.0.10	false	true	true
37	hdsl2shdsl-protocol-init-failure	INFO	1.3.6.1.2.1.10.48.0.14	false	true	true

Table B-2 Cisco Traps (continued)

Item	Name	Severity	OID	is-correlation-allowed	correlate	is-ticketable
38	hdsl2shdsl-snr-margin-crossing	INFO	1.3.6.1.2.1.10.48.0.2	false	true	true
39	hdsl2shdsl-span-invalid-num-repeaters	INFO	1.3.6.1.2.1.10.48.0.8	false	true	true
40	new root trap	INFO	1.3.6.1.2.1.17.0.1	false	true	true
41	ospf-if-auth-failure	INFO	1.3.6.1.2.1.14.16.2.6	false	true	true
42	ospf-if-config-error	INFO	1.3.6.1.2.1.14.16.2.4	false	true	true
43	ospf-if-rx-bad-packet	INFO	1.3.6.1.2.1.14.16.2.8	false	true	true
44	ospf-if-state-change	INFO	1.3.6.1.2.1.14.16.2.16	false	true	true
45	dlsw-trap-tconn-down	MINOR	1.3.6.1.2.1.46.1.0	false	true	true
46	ospf-lsdb-approaching-overflow	INFO	1.3.6.1.2.1.14.16.2.15	false	true	true
47	ospf-lsdb-overflow	INFO	1.3.6.1.2.1.14.16.2.14	false	true	true
48	ospf-max-age-lsa	INFO	1.3.6.1.2.1.14.16.2.13	false	true	true
49	ospf-nbr-state-change	INFO	1.3.6.1.2.1.14.16.2.2	false	true	true
50	ospf-originate-lsa	INFO	1.3.6.1.2.1.14.16.2.12	false	true	true
51	ospf tx retransmit trap	INFO	1.3.6.1.2.1.14.16.2.10	false	true	true
52	ospf-virt-if-auth-failure	INFO	1.3.6.1.2.1.14.16.2.7	false	true	true
53	ospf-virt-if-config-error	INFO	1.3.6.1.2.1.14.16.2.5	false	true	true
54	dlsw-trap-tconn-partner-reject	INFO	1.3.6.1.2.1.46.1.0.1	false	true	true
55	ospf-virt-if-rx-bad-packet	INFO	1.3.6.1.2.1.14.16.2.9	false	true	true
56	ospf-virt-if-state-change	INFO	1.3.6.1.2.1.14.16.2.1	false	true	true
57	ospf-virt-if-tx-retransmit	INFO	1.3.6.1.2.1.14.16.2.11	false	true	true
58	ospf virt nbr state change trap	INFO	1.3.6.1.2.1.14.16.2.3	false	true	true
59	dlsw-trap-tconn-prot-violation	INFO	1.3.6.1.2.1.46.1.0.2	false	true	true

Table B-2 Cisco Traps (continued)

Item	Name	Severity	OID	is-correlation-allowed	correlate	is-ticketable
60	x25-reset	INFO	1.3.6.1.2.1.10.5.0.2	false	true	true
61	dummy-ticket	CLEARED	1.3.6.1.4.1.42	false	true	false