



Cisco Active Network Abstraction Fault Management User's Guide, 3.5

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



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

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

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

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

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Important Notice

Cisco ANA 3.5 is a carrier-class, multi-vendor network and service management platform which builds a real-time virtual model of the network, serving as a live information base for value-added tools and applications for integration into an existing OSS environment.

Cisco ANA 3.5 is a limited release by Cisco Systems of the existing features and functions of the Sheer DNA 4.0.1 software.

As this is a limited release, the naming of the product in the software and the user documentation remains as Sheer DNA.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

Emergencies — 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.

Nonemergencies — psirt@cisco.com

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

1 877 228-7302

1 408 525-6532

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked 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.

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>

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI 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.

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)—Your 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 operation 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 your network is impaired, but 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.

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>

Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://cisoiq.texterity.com/cisoiq/sample/>

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 for networking professionals to 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>

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>

About This Guide

This Reference Guide includes the following chapters:

Chapter 1 Fault Management Overview, page 1, describes the challenge of managing an overabundance of events, and introduces some of the key concepts of Sheer DNA alarm management.

Chapter 2 Correlation Logic, page 11, describes how Sheer DNA performs correlation logic decisions.

Chapter 3 Advanced Correlation Scenarios, page 15, describes specific alarms which use advanced correlation logic on top of the root cause analysis flow.

Chapter 4 Correlation Over Unmanaged Segments, page 19, describes how Sheer DNA performs correlation decisions over unmanaged segments.

Chapter 5 Event and Alarm Configuration, page 21, describes the details of various configurable alarms parameters.

Chapter 6 Impact Analysis, page 29, describes the impact analysis functionality available in Sheer DNA.

Table of Contents

1	Fault Management Overview	1
1.1	The Event Management Challenge.....	1
1.2	Basic Concepts and Terms	2
1.3	Severity Propagation	8
1.4	Sources of Alarms on a Device	8
1.5	Event Processing Overview	9
1.6	Event Suppression	9
1.7	Alarm Integrity.....	10
1.8	Related Documentation.....	10
2	Correlation Logic.....	11
2.1	Root-Cause Correlation Process	11
2.2	Root-Cause Alarms.....	12
2.3	Correlation Flows	13
2.3.1	Network Correlation Flows.....	13
2.3.2	Box-Level Correlation.....	13
2.3.3	Using Weights.....	14
2.3.4	Correlating TCA.....	14
3	Advanced Correlation Scenarios	15
3.1	Correlation to “config” Change	15
3.2	Device Unreachable Alarm	15
3.2.1	Connectivity Test.....	15
3.2.2	Device Fault Identification	15
4	Correlation Over Unmanaged Segments	19
4.1	Cloud VNE	19
4.1.1	Fault Correlation Across the FR/ATM/Ethernet Cloud	19
5	Event and Alarm Configuration Parameters	21
5.1	Alarm Type Definition	21
5.2	Event (Sub-Type) Configuration Parameters	21
5.2.1	General Event Parameters.....	21
5.2.2	Root-Cause Configuration Parameters	22
5.2.3	Correlation Configuration Parameters.....	24
5.2.4	Network Correlation Parameters	25

5.2.5	Flapping Event Definitions Parameters	26
6	Impact Analysis	29
6.1	Impact Analysis Options	29
6.2	Impact Report Structure.....	30
6.3	Affected Severities	30
6.4	Impact Analysis GUI (NetworkVision).....	31
6.4.1	Affected Parties Tab	31
6.4.2	Viewing a Detailed Report for the Affected Pair.....	33
6.5	Enabling\Disabling Impact Analysis	34
6.6	Accumulating Affected Parties.....	34
6.6.1	Accumulating the Affected Parties in an Alarm	35
6.6.2	Accumulating the Affected Parties in the Correlation Tree	36
6.6.3	Updating Affected Severity Over Time.....	36

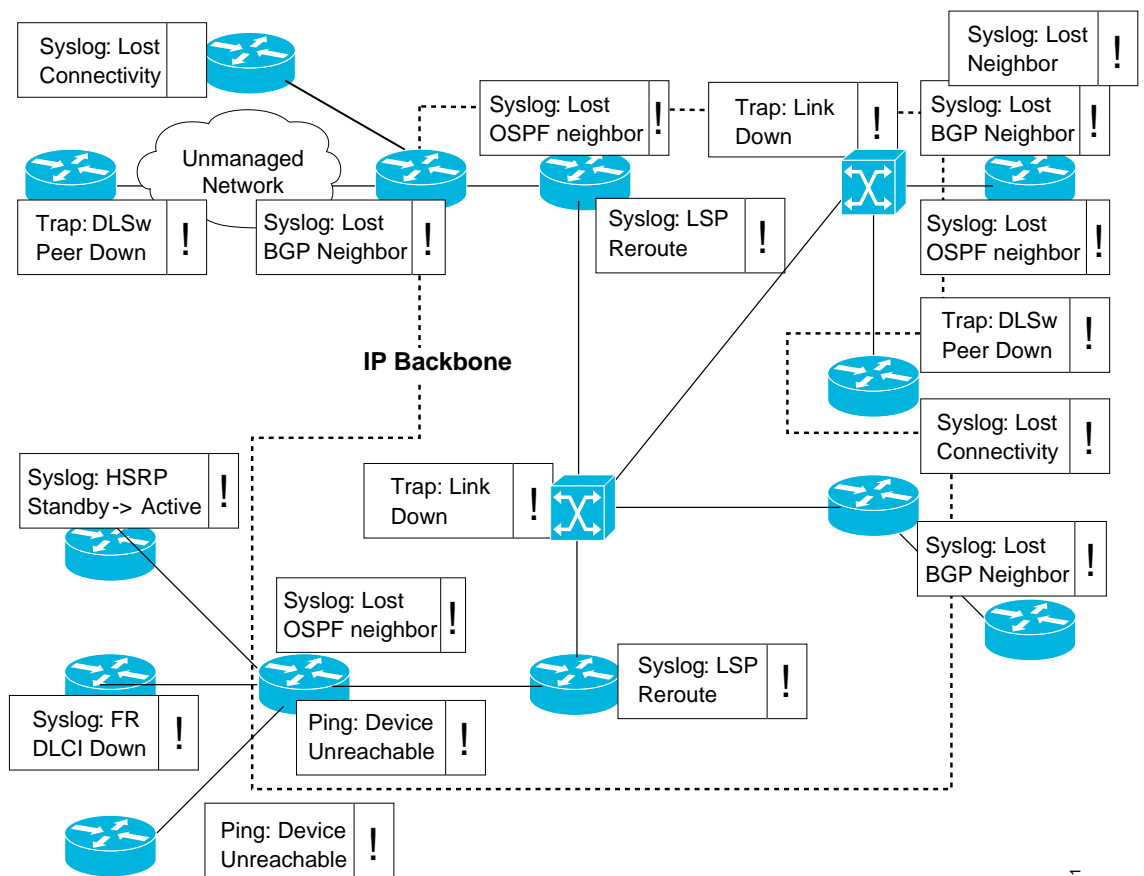
List of Figures

Figure 1: Event Flood	1
Figure 2: Event Sequence Example	3
Figure 3: Repeating Event Sequence	4
Figure 4: Flapping Event	5
Figure 5 Root-Cause Correlation Hierarchy Example.....	5
Figure 6: Sequence association vs. Root-cause analysis.....	7
Figure 7: Root-cause correlation process.....	12
Figure 8: Root-cause vs. Due-to-cause	23

1 Fault Management Overview

1.1 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.



154391

Figure 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.

Sheer DNA 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.

1.2 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 DNA database once and never change.

The collected events are displayed in the Sheer EventVision. Please refer to the Cisco ANA EventVision Guide, 3.5 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*.

Link-Down event sequence

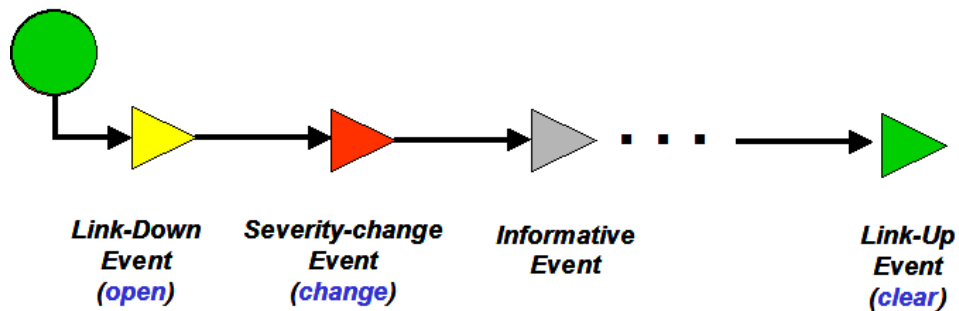


Figure 2: Event Sequence Example

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.

Notes:

1. The event types that will belong to each sequence can be configured in the system registry.
2. An event sequence can consist of a single event (for example, “Device Reset”)
3. The set of events that should participate in DNA 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).

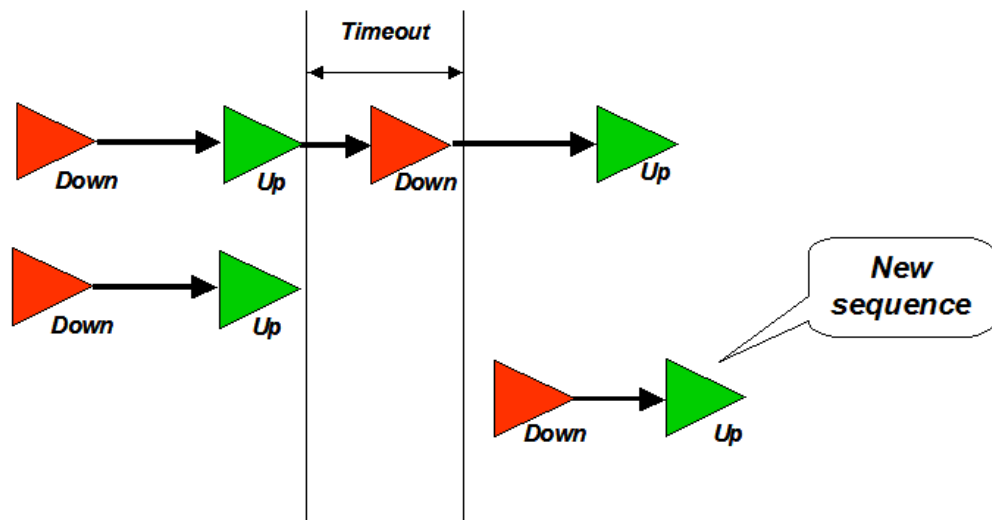


Figure 3: Repeating Event Sequence

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.

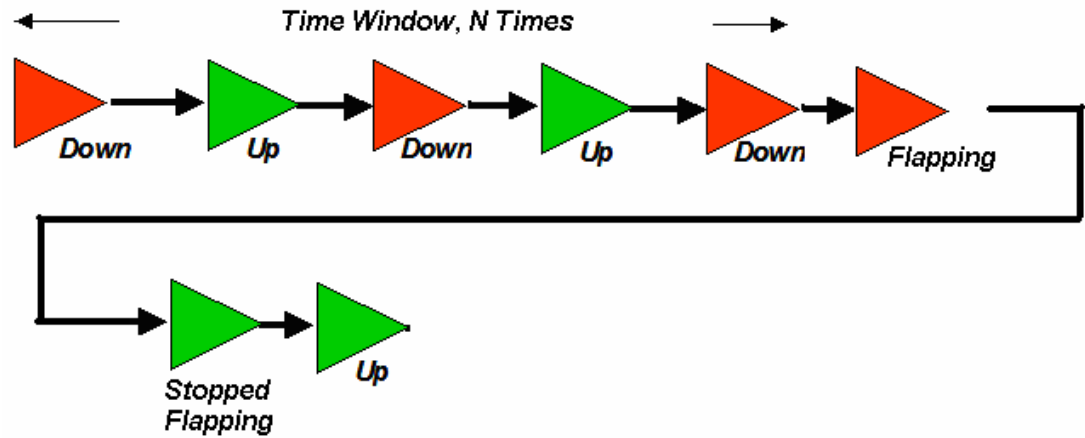


Figure 4: Flapping Event

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).

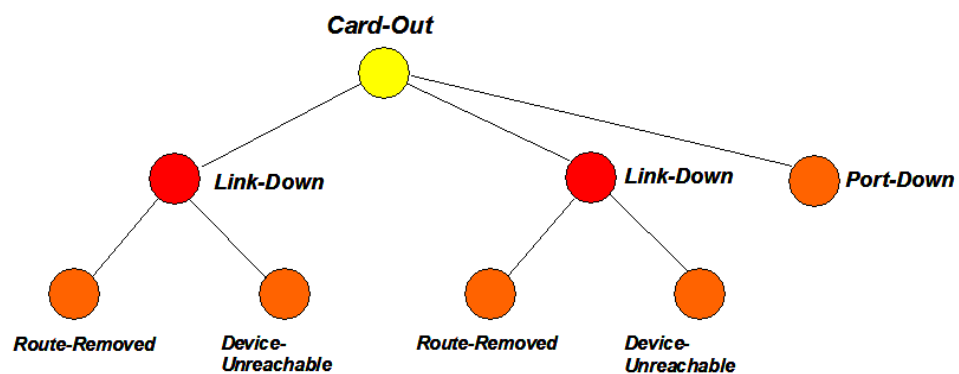


Figure 5 Root-Cause Correlation Hierarchy Example

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 Sheer NetworkVision and Sheer 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 DNA 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:

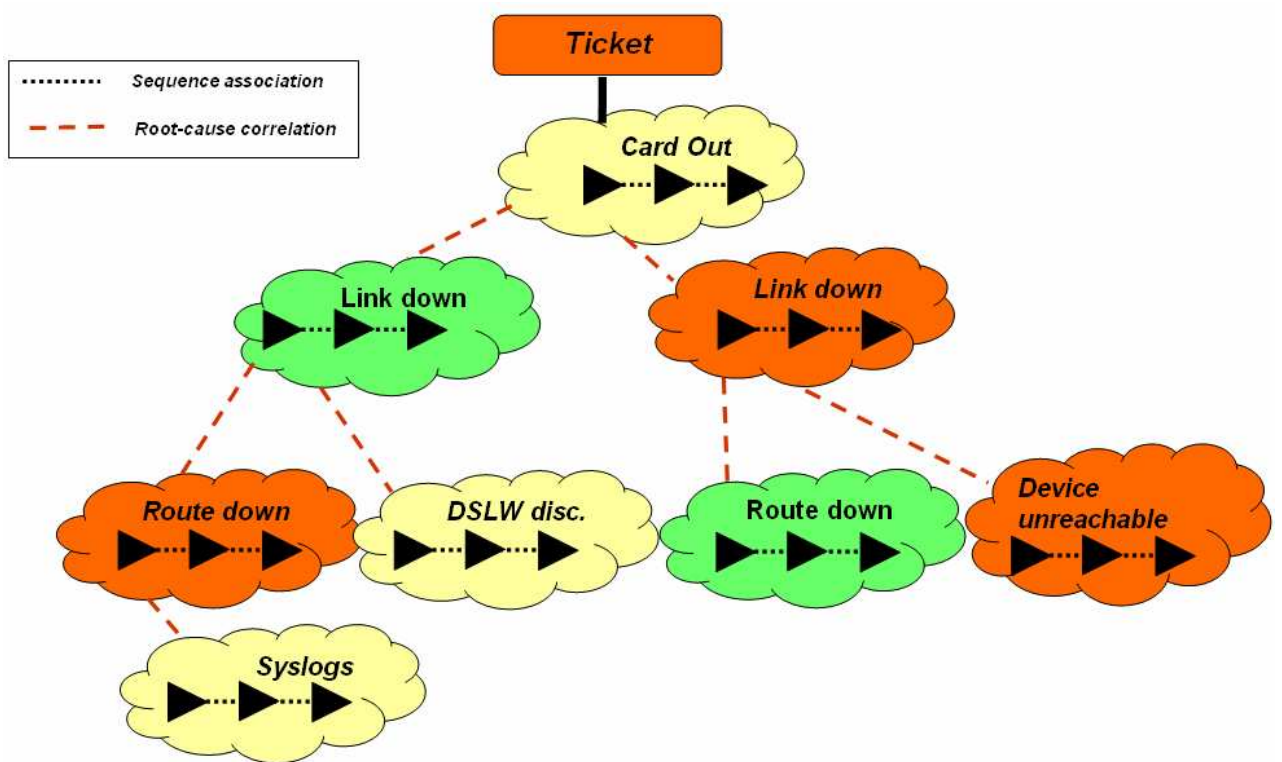


Figure 6: Sequence association vs. Root-cause analysis

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.

1.3 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-down 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, that 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.

1.4 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 Sheer 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).
- SNMP Traps – Traps that sent by the network elements and captured by the Sheer platform. The Sheer 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 Sheer platform. The Syslogs are then forwarded to the specific VNEs for further processing and correlation logic.
- TCA – Threshold Crossing Alarms. Sheer DNA 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*, 3.5.

1.5 Event Processing Overview

Sheer DNA 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:

1. The event data is parsed to determine its source, type, and alarm-handling behavior.
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.
3. The event fields are looked up and filled.
4. The event is sent to the DNA 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.

1.6 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 than 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, 3.5* for information about disabling or enabling a port alarm.

1.7 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.

1.8 Related Documentation

For more information, refer to the following publications:

- *Cisco Active Network Abstraction NetworkVision User's Guide, 3.5*
- *Cisco Active Network Abstraction Customization User's Guide, 3.5*
- *Cisco Active Network Abstraction EventVision User's Guide, 3.5*
- *Cisco Active Network Abstraction MPLS User's Guide, 3.5*

2 Correlation Logic

2.1 Root-Cause Correlation Process

Root-cause correlation is implemented in two stages within the Sheer DNA VNEs. Initially, 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 new Link-down alarm, the VNE will look for a root-cause alarm within the device, e.g. a Card-out alarm (on the specific card instance that hosts the faulty link). When such a root-cause is found and qualified, the correlation relationship is set in the alarm DB. This process is named *Local 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 DNA 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.

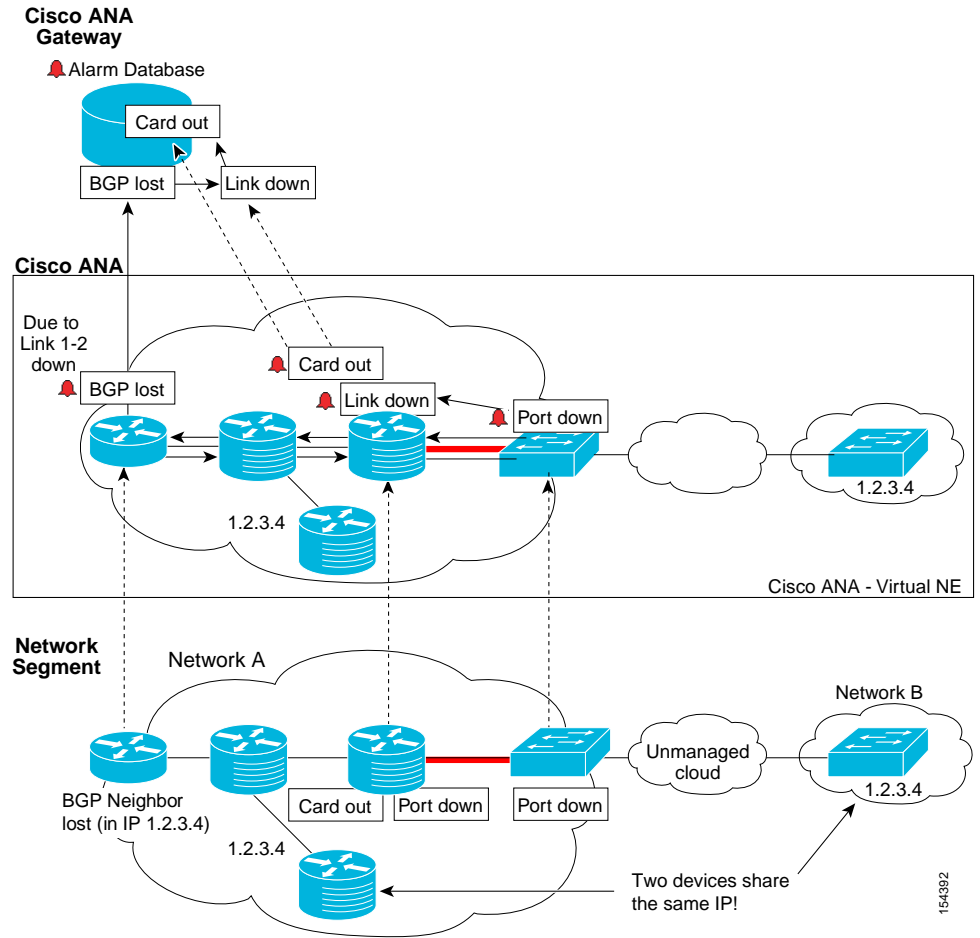


Figure 7: Root-cause correlation process

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

2.2 Root-Cause Alarms

Potential Root-Cause alarms have a determined weight according to the specific event customization. Refer to *Event and Alarm Configuration Parameters* 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.

2.3 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, please refer to *Event and Alarm Configuration Parameters*.

2.3.1 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 Sheer PathTracer operation when it trace 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.

2.3.2 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.

2.3.3 Using Weights

In cases where there are multiple potential root-causes along the same service path, Sheer DNA 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.

2.3.4 Correlating TCA

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

3 Advanced Correlation Scenarios

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

3.1 Correlation to “config” Change

“Configuration Change” is an alarm that is triggered by a syslog or trap. By default that alarm will not generate a new ticket (in case there is no root-cause alarm to correlate to), and will issue simply as an event. However, if an alarm will run a correlation flow through a VNE which has a “Configuration change” alarm waiting, then the “Configuration Change” will be issued as a Ticket, and the alarm will correlate to it with high probability. By default the “Configuration Change” alarm has the highest weight, second only to link down, i.e. if it does not encounter a “link down” alarm. This is due to that fact that in many case the reason for events occurring in the network are actual configuration changes done by the user on the Network Element itself.

3.2 Device Unreachable Alarm

3.2.1 Connectivity Test

Connectivity tests are used to verify connectivity between the Sheer DNA 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 Sheer DNA Manage.

3.2.2 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

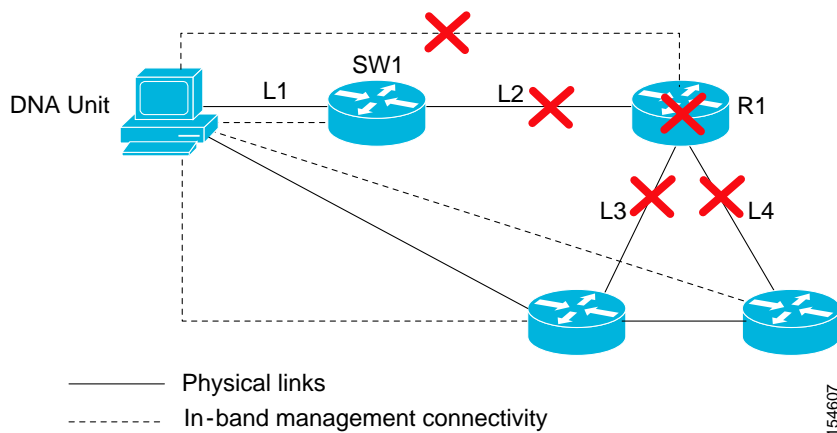
Sheer DNA implements an algorithm that uses additional data to heuristically resolve the ambiguity and declare the Root-Cause correctly. For example:

Example 1:

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

In this case the system will provide the following report:

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

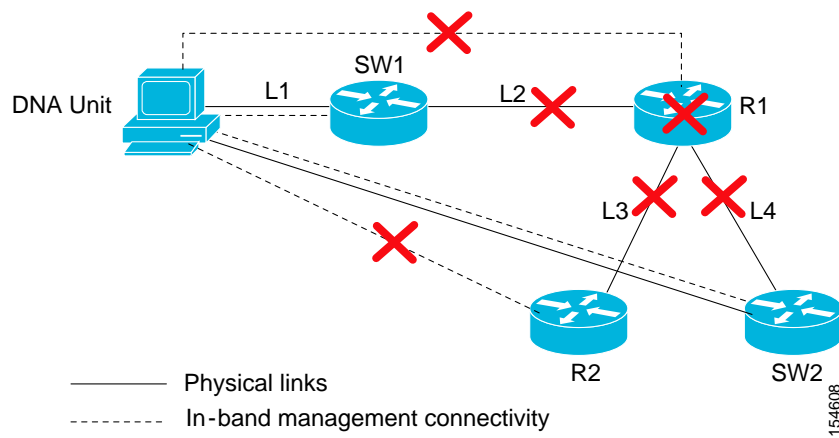
**Example 2:**

In the following figure, 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.

In this case the system will provide the following report:

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

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



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 Sheer DNA shows that the device unreachable due to link down.

4 Correlation Over Unmanaged Segments

4.1 Cloud VNE

In some scenarios Sheer DNA 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.

4.1.1 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.

5 Event and Alarm Configuration Parameters

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

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

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

5.1 Alarm Type Definition

The alarm type serves as an identifier which enables group events from different sub-type to share the same type and source into 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.

5.2 Event (Sub-Type) Configuration Parameters

5.2.1 General Event Parameters

Parameter Name	Description
severity	Severity level of the event, either: <ul style="list-style-type: none"> • 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).

Parameter Name	Description
functionality-type	Determines the event type, either: <ul style="list-style-type: none"> • Service (Sheer-generated) • Syslog • SNMP Trap

5.2.2 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	Determines if the alarm may serve as root-cause, and allow child alarms to correlate to it.	True/False
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	The allowed time period (in milliseconds) for consequent alarms to correlate to this alarm.	Positive integer
gw-correlation-timeout	The period of time (in milliseconds) in which the DNA Gateway will accept the correlation (that has been determined by the VNEs) and set it in the alarm DB. This parameter is also relevant for how long an alarm is open for sequence alarm under the restriction the alarm severity is 'Clear' or 'Info' (Alarms with non-cleared severity are always open for a consequent alarm)	Positive integer

Name	Description	Permitted Values
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”:

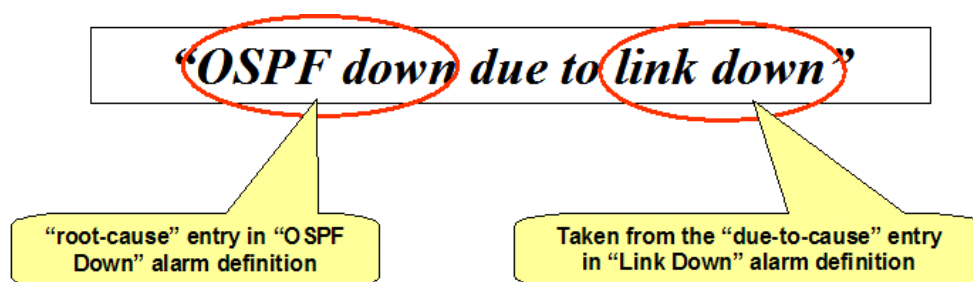


Figure 8: Root-cause vs. Due-to-cause

5.2.3 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
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) to wait before attempting to find a root-cause.	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).	Positive integer
drop-event	Whether event should be dropped on VNE level – not forwarded to GW level.	True/False

5.2.4 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	Time (in milliseconds) to wait (and allow for Box level correlation) before initiating the network correlation flow.	Positive integer
flow-activation-message	Identifies the flow process functionality	<i>IPBasedActiveFlowTriggerMessage</i>
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
flow-ttl	How many DCM hops may the flow trace before being stopped	Positive integer
weight	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.

5.2.5 Flapping Event Definitions Parameters

These parameters control the alarm's behavior in setrnm=ining 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 than 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 amount of changes an update will be allowed to be sent	Positive integer

6 Impact Analysis

This chapter describes the impact analysis functionality available in Sheer DNA 3.5

6.1 Impact Analysis Options

Impact analysis is available in two modes:

- Automatic Impact Analysis – when a fault which has been identified as potentially service affecting occurs Sheer DNA automatically generates the list of potential and actual service resources that were affected by a fault and embeds this information in the ticket along with all of the correlated faults.
- Proactive Impact Analysis – Sheer DNA 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 Sheer DNA 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 Sheer DNA please refer to the Cisco ANA MPLS User’s Guide, 3.5.

Note: As mentioned above, 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, 3.5*.

6.2 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, Routing Entity.
- **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, 3.5*.

6.3 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 real 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, 3.5*.

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

6.4 Impact Analysis GUI (NetworkVision)

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

6.4.1 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, Sheer NetworkVision automatically calculates the accumulation of affected parties of all the subsequent events. For more information about accumulating affected parties, refer to page 33.

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

The screenshot shows the '1657 - Ticket Properties' window with the 'Affected Parties' tab selected. The window is divided into two main sections: 'Source' and 'Destination'. Each section contains a search bar and a table of affected parties.

Source Table:

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

Destination Table:

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

The bottom navigation bar shows tabs for 'General', 'History', 'Affected Parties', 'Correlation', 'Notes', and 'Advanced'. The 'Affected Parties' tab is currently selected. The status bar at the bottom right shows 'Memory: 9%' and 'Connected'.

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:** The service may be affected but its real state is not known.
 - **Real:** The service is affected.
 - **Recovered:** The service was recovered after the network fault. This state only applies to affected pairs that were previously marked as **Potentially Affected** or **Real Affected**.
 - **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, refer to the Affected Severities section above.
- **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.

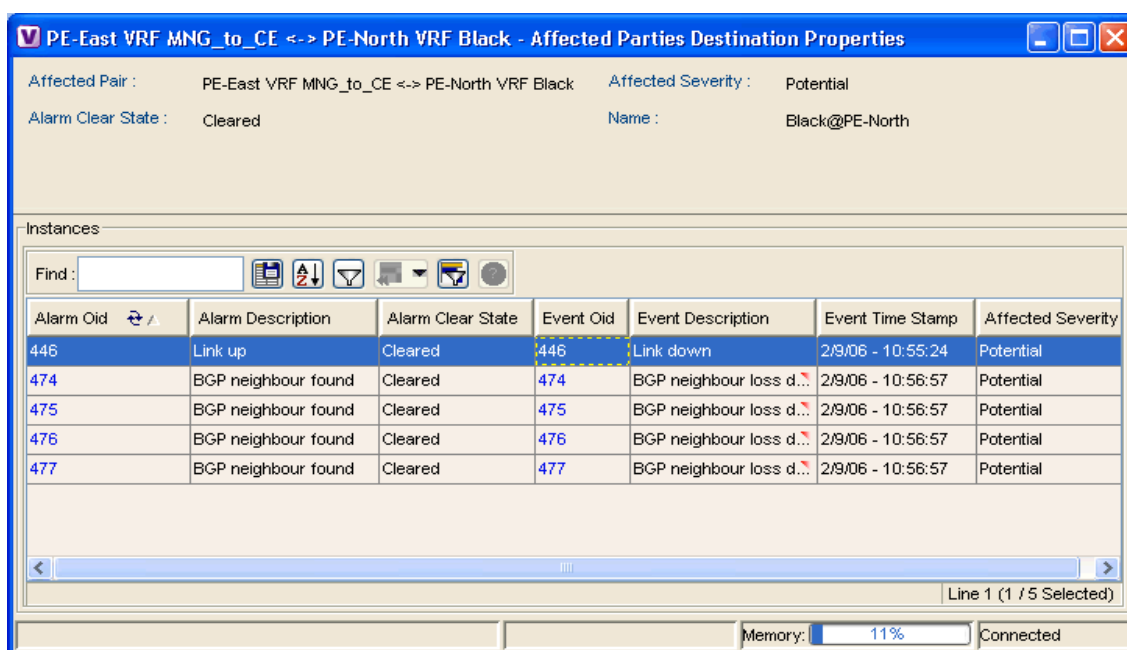
In addition, you can view a detailed report for every affected pair that includes a list of the events that contributed to this affected pair.

6.4.2 Viewing a Detailed Report for the Affected Pair

Sheer 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, 3.5* for more information.

The Affected Parties Destination Properties dialog box is displayed below.



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 on page 33.
- **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.

6.5 Enabling\Disabling Impact Analysis

You can disable impact analysis for a specific alarm. This option can be set in the Sheer 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
- Black Hole
- BGP Neighbor Down.
- MPLS TE Tunnel Down
- L2 Tunnel down (Martini)

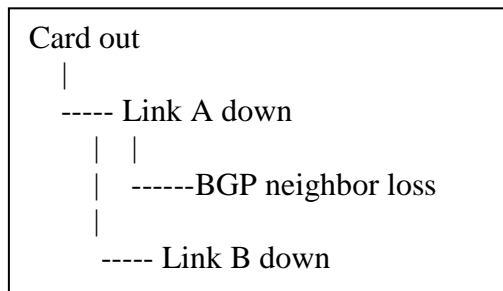
6.6 Accumulating Affected Parties

This section describes how Sheer 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.



For each type of alarm Sheer 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.

6.6.1 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**.

6.6.2 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.

6.6.3 Updating Affected Severity Over Time

Sheer DNA 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.

