CHAPTER 7

Impact Analysis

This chapter describes the impact analysis functionality:

- 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—Describes how the user can view impact analysis information in Cisco ANA NetworkVision.
- 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 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, refer to the *Cisco Active Network Abstraction MPLS User Guide*.

Note 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 the automatic impact analysis. For more information about proactive impact analysis, refer to the *Cisco Active Network Abstraction NetworkVision User Guide*.

Impact Report Structure

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

Each endpoint has the following details:

- **Endpoint physical or logical location**—An endpoint can be a physical entity (for example, a port) or a logical one (for example, a subinterface). The impact report contains the exact location of the entity. All the location identifiers start with the ID of the device which holds the endpoint. The other details in the location identifier are varied according to the endpoint type, for example VC, VP, IP interface.
- **Business tag properties**—Key, name, type (if attached to the entity).

Note For specific information about the report structure in MPLS networks, refer to the *Cisco Active Network Abstraction MPLS User 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 see the Cisco Active Network Abstraction MPLS User Guide.

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

Impact Analysis GUI

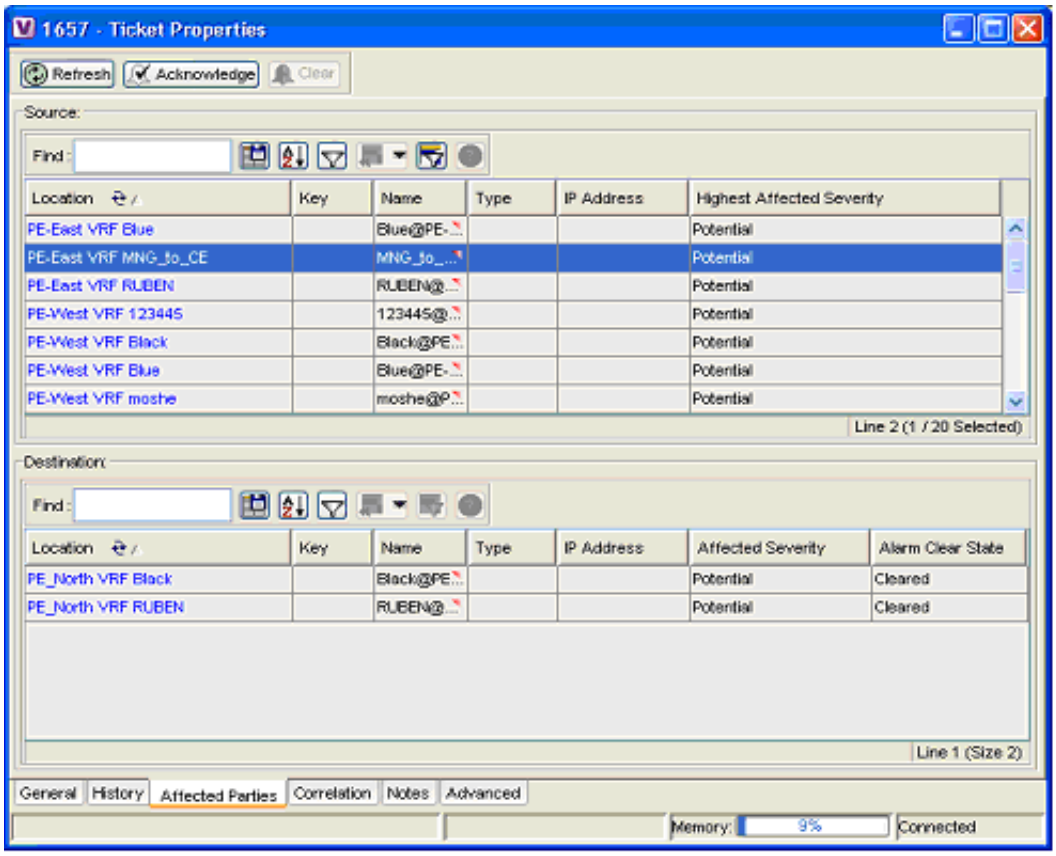
The Impact Analysis GUI is available in Cisco ANA NetworkVision and displays the list of affected service resources which are embedded in the ticket information. This section describes this list.

Affected Parties Tab

The Affected Parties tab displays the service resources (affected pairs) that are affected (automatic impact analysis) for an event, an alarm, or a ticket depending on which properties window is opened. In the case of an alarm or a ticket, NetworkVision automatically calculates the accumulation of affected parties of all the subsequent events. For more information about accumulating affected parties, see Viewing a Detailed Report For the Affected Pair, page 7-4.

The Affected Parties tab is displayed below.

Figure 7-1 Affected Parties Tab



The Affected Parties tab is divided into two areas, 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 subinterface (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 Guide*.
- **Type**—The business tag type.
- **IP Address**—If the affected element is an IP interface, the IP address of the subinterface site is displayed. For more information, refer to the *Cisco Active Network Abstraction Managing MPLS User 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 among these. The affected pair can have one of the following severities:
  - Potential
  - Real
  - Recovered
  - N/A—From the 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**—There are one or more alarms that have not been cleared for this pair.
  - **Cleared**—All 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.

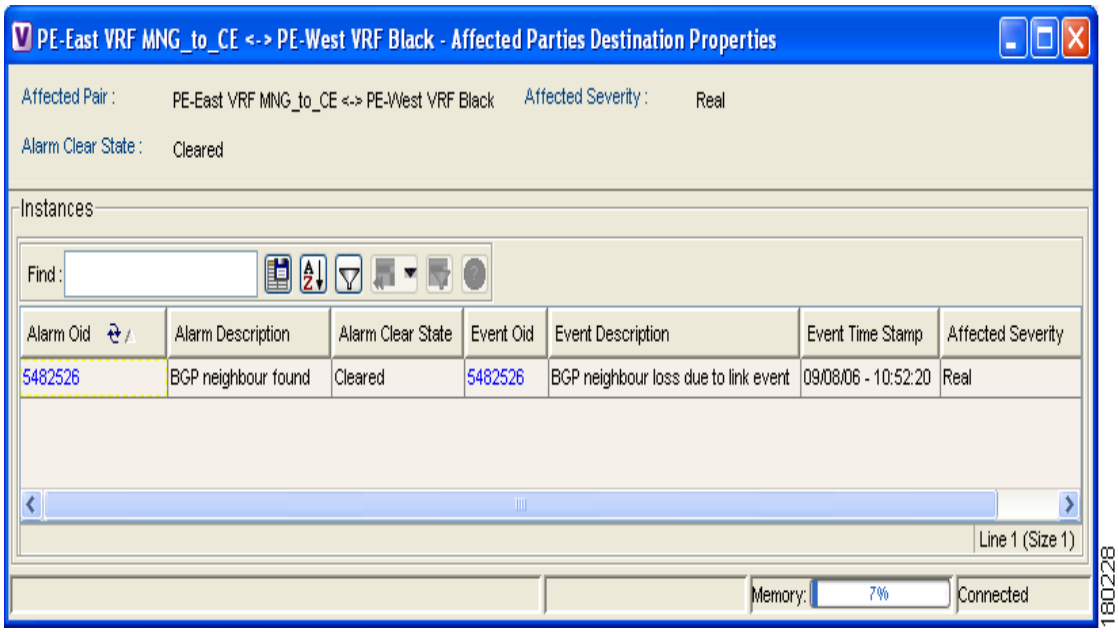
Viewing a Detailed Report For the Affected Pair

You can view a detailed report for every affected pair in NetworkVision. 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, refer to the *Cisco Active Network Abstraction NetworkVision User Guide*.

The Affected Parties Destination Properties dialog box is displayed.

Figure 7-2 Detailed Report For the Affected Pair



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 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 Viewing a Detailed Report For the Affected Pair, page 7-4.
- **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.

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 can be disabled:

- Link down
- Port down
- Dropped or discarded packets
- MPLS black hole
- BGP neighbor loss
- MPLS TE tunnel down
- L2 tunnel down

Accumulating Affected Parties

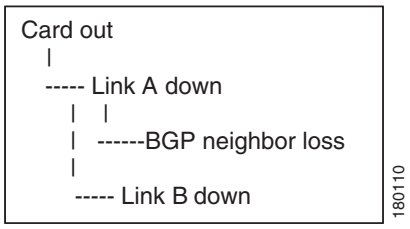
This section describes how NetworkVision automatically calculates the accumulation of affected parties during automatic impact analysis. This information is embedded in the ticket along with all the correlated faults.

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 and BGP neighbor loss).

An event sequence is correlated to each of these alarms.

Figure 7-3 Correlation Tree Example



NetworkVision provides a report of the affected parties for each type of alarm. 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. It also 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, 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 edgepoints, and 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 and Y are the OIDs of edgepoints 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 can update the affected severity of the same alarm report over time due because 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 as 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.