CHAPTER 15

# Working with Tickets

These topics describe the impact analysis of faults, and how to manage tickets that represent fault scenarios of selected devices or network elements:

**Note** For detailed information about alarms and event management, see Chapter 5, "Understanding Fault Management."

- Impact Analysis Options, page 15-2—Describes automatic and proactive impact analysis.
- Impact Report Structure, page 15-2—Describes the structure of the impact report that is generated.
- Severity Values for Affected Parties, page 15-3—Describes the severities used for automatic impact analysis.
- Impact Analysis (Affected Parties) Windows, page 15-3—Describes how the user can view impact analysis information in Cisco ANA NetworkVision.
- Disabling Impact Analysis, page 15-6—Describes enabling and disabling impact analysis for specific alarms, and which alarms support this feature.
- Accumulating Affected Parties, page 15-6—Describes how Cisco ANA NetworkVision automatically calculates the accumulation of affected parties during automatic impact analysis.
- Filtering Tickets by Device, page 15-8, describes how to filter the tickets that are shown in the ticket pane, so that only the tickets of a selected device or network element are displayed.
- Filtering Tickets by Criteria, page 15-8, describes how to filter the tickets that are shown in the ticket pane, according to various criteria.
- Opening Ticket Properties, page 15-10, describes how to view ticket properties.
- Acknowledging a Ticket, page 15-17, describes how to acknowledge tickets using the ticket pane.
- Clearing a Ticket, page 15-18, describes how to clear a ticket.
- Removing a Ticket, page 15-18, describes how to remove a ticket.
- Ticket Status in the Ticket Pane, page 15-19, describes the different ways in which a ticket is displayed in the ticket pane depending on the status or severity of the alarm, and what effect manipulating the ticket has on the way in which the ticket is displayed in the ticket pane.

Cisco ANA NetworkVision enables you to view and acknowledge tickets using the ticket pane. For more information, see Ticket Pane, page 2-11.

# Impact Analysis Options

Impact analysis is available in two modes:

- Automatic impact analysis—When a fault occurs that 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 applies only to specific alarms. Not every alarm initiates automatic impact analysis.

- 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 that determines all the potentially affected edges.

**Note** For more information about fault scenarios which are considered service affecting in an MPLS network and supported by Cisco ANA, see the *Cisco Active Network Abstraction 3.6.6 MPLS User Guide*.

**Note** Each fault that has been identified as potentially service affecting triggers an impact analysis calculation, even if the fault recurs in the network.

# 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 that holds the endpoint. The other details in the location identifier are varied according to the endpoint type, for example VC, VP, and IP interface.
- Business tag properties—Key, name, and type (if attached to the entity).

**Note** For specific information about the report structure in MPLS networks, see the *Cisco Active Network Abstraction 3.6.6 MPLS User Guide*.

# Severity Values for Affected Parties

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 has 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 3.6.6 MPLS User Guide*.

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

# Impact Analysis (Affected Parties) Windows

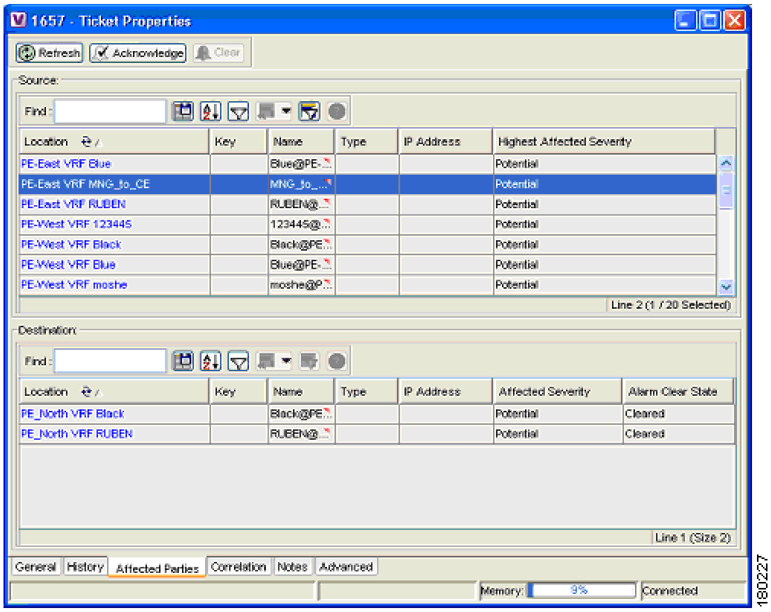
The Impact Analysis windows are available in Cisco ANA NetworkVision and display the list of affected service resources that are embedded in the ticket information. This section describes this list.

## Affected Parties Tab

The Affected Parties tab displays the service resources (pairs) that are affected by an event, an 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 Viewing a Detailed Report for the Affected Pair, page 15-5.

The Affected Parties tab is displayed in Figure 15-1.

*Figure 15-1 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, 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 and provide 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, see the *Cisco Active Network Abstraction 3.6.6 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, see the *Cisco Active Network Abstraction 3.6.6 MPLS User Guide*.
- Highest Affected Severity—The highest 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 list of all the endpoints where the services between them and the selected endpoint have been affected is displayed in the Destination area. For example, in Figure 15-1 when the PE-East row is selected in the Source area, there are two pairs:

- PE-East VRF (Source area) and PE_North VRF Black (Destination area)
- PE-East VRF (Source area) and PE_North VRF R (Destination area)

The following 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 in Viewing a Detailed Report for the Affected Pair, page 15-5.
- Alarm Clear State—For each pair, an indication of the clear state of the alarm. The following states exist:
  - Not Cleared—One or more alarms for this pair have not been cleared.
  - Cleared—All the related alarms for this pair have been cleared.

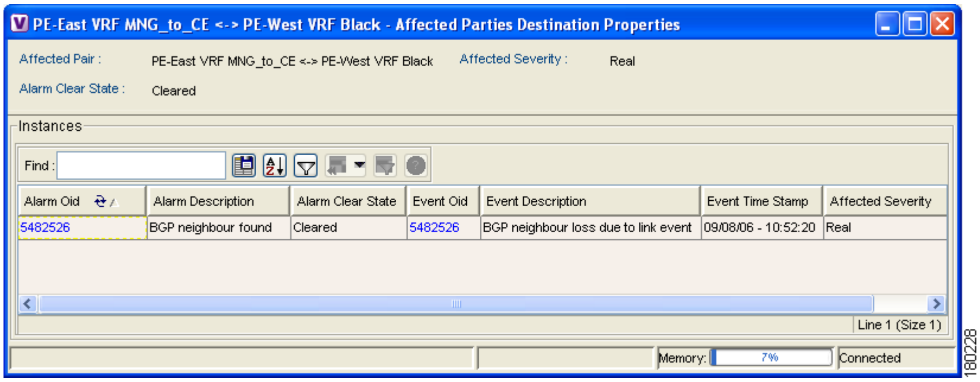
In addition, for every affected pair, you can view a detailed report that includes a list of the events that contributed to this affected pair.

## Viewing a Detailed Report for the Affected Pair

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

The Affected Parties Destination Properties dialog box is displayed.

***Figure 15-2 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

Find :

| 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—For each pair, an indication of the clear state of the alarm. The following states exist:
  - Not Cleared—One or more alarms for this pair have not been cleared.
  - 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 15-5.
- 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—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.

Impact analysis for 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

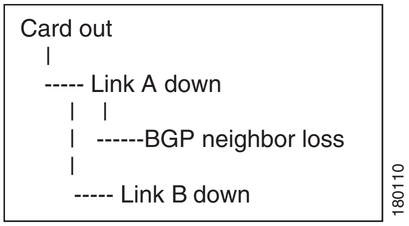
This section describes how Cisco ANA  NetworkVision automatically calculates the accumulation of affected parties during automatic impact analysis. This information is embedded in the ticket along with all the correlated faults.

In the following example, these alarm types 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 15-3 Correlation Tree Example*



```
Card out
  |
  ----- Link A down
     |    |
     |   ------BGP neighbor loss
     |
     ----- Link B down
```

Cisco ANA 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 Figure 15-3:

- 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 recurring 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 recurring affected pairs are displayed only 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 because in some cases, the effect 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.

# Filtering Tickets by Device

Cisco ANA NetworkVision enables you to filter the tickets that are shown in the ticket pane so that only the tickets of a selected device or network element are displayed.

To filter tickets for a specific network element:

**Step 1** Right-click the required device or network element in the tree pane or map pane of the Cisco ANA NetworkVision window to display the Device shortcut menu.

**Step 2** Select **Filter Tickets**. The ticket pane displays the tickets of the selected device or network element only.

**Note** The Filter button in the ticket pane toggles to indicate that a filter has been applied.

The filter can be removed to display all the tickets in the system. For more information about removing a filter, see Filtering Tickets by Criteria, page 15-8.

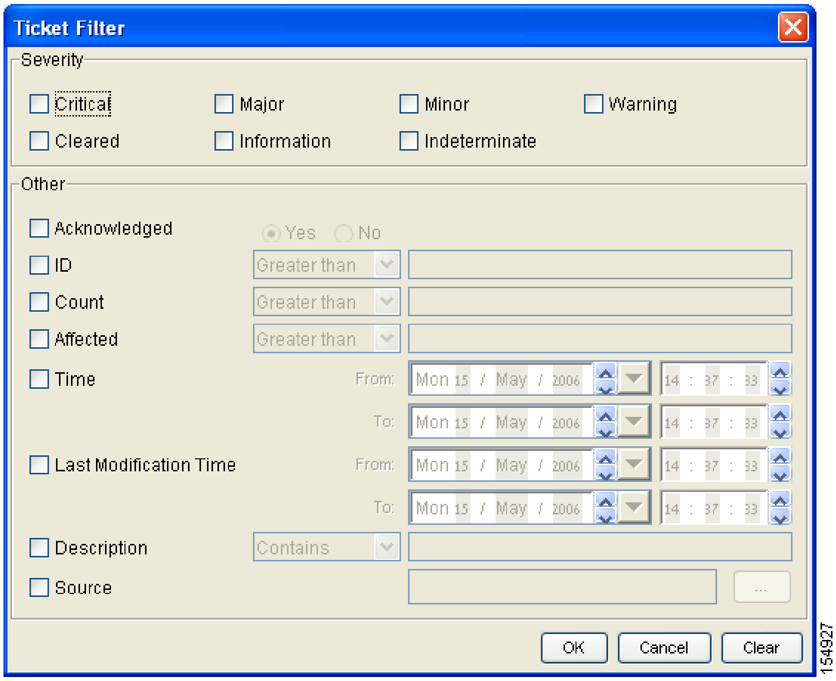
# Filtering Tickets by Criteria

Cisco ANA NetworkVision enables you to define a filter for the tickets displayed in the ticket pane according to various criteria; for example, tickets can be filtered according to the number of affected parties or acknowledged tickets.

To define the ticket filter:

**Step 1** Click Ticket Filter icon in the ticket pane toolbar. A dialog box similar to Figure 15-4 is displayed.

***Figure 15-4 Ticket Filter Dialog Box***



Ticket Filter

Severity

□ Critical □ Major □ Minor □ Warning
□ Cleared □ Information □ Indeterminate

Other

□ Acknowledged ● Yes ○ No
□ ID Greater than
□ Count Greater than
□ Affected Greater than
□ Time From: Mon 15 / May / 2006 14 : 37 : 33
To: Mon 15 / May / 2006 14 : 37 : 33
□ Last Modification Time From: Mon 15 / May / 2006 14 : 37 : 33
To: Mon 15 / May / 2006 14 : 37 : 33
□ Description Contains
□ Source ...

The Severity area in the Ticket Filter dialog box enables the user to filter the tickets displayed in the ticket pane by selecting one or more options. For more information about severities, see Network Element Status Indicators, page 2-13.

The check boxes displayed in the Other area reflect the columns displayed in the ticket pane and enable the user to filter the tickets according to any of these criteria. For more information about the columns displayed in the ticket pane, see Ticket Pane, page 2-11.

The Source check box (selected by default) enables the user to filter the tickets that are shown in the ticket pane so that only the tickets of a selected device or network element are displayed by selecting a source.

**Step 2** Select the required filter values.

**Step 3** Click **OK**. The filtered tickets are displayed in the ticket pane according to the defined criteria.

**Note** The Ticket Filter button in the ticket pane toggles to indicate that a filter has been applied.

To remove the ticket filter:

**Step 1** Click the Ticket Filter icon in the ticket pane toolbar. The Ticket Filter dialog box is displayed.

**Step 2** Click **Clear**. The selected options in the Ticket Filter dialog box are cleared.

**Step 3** Click **OK**. All the tickets are displayed in the ticket pane.

# Opening Ticket Properties

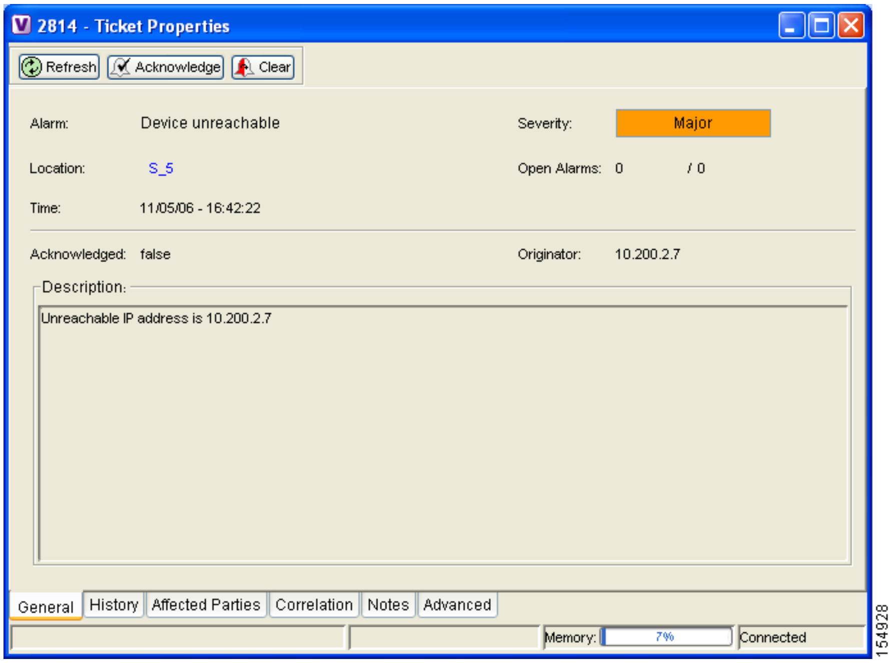
The properties of a selected ticket can be viewed by displaying the Ticket Properties dialog box. For example, you can view alarm severity, correlated alarms, active alarms, alarm history or the source of the alarm.

To open ticket properties, do one of the following:

- Double-click the required ticket in the ticket pane.
- Right-click a ticket in the ticket pane, and choose **Properties**.

Figure 15-5 shows the Ticket Properties dialog box.

***Figure 15-5 Ticket Properties Dialog Box***



Alarm: Device unreachable

Severity: Major

Location: S_5

Open Alarms: 0 / 0

Time: 11/05/06 - 16:42:22

Acknowledged: false

Originator: 10.200.2.7

Description:

Unreachable IP address is 10.200.2.7

Memory: 7%

Connected

The information displayed in the Ticket Properties dialog box corresponds with the information displayed in the ticket pane. The ID number displayed in the header corresponds to the ID number of the ticket selected in the ticket pane.

The Ticket Properties dialog box is divided into the following areas:

- Tabbed Pane, page 15-11
- Toolbar, page 15-17

# Tabbed Pane

The Ticket Properties dialog box is divided into the following tabs:

- General—General information about the selected ticket. See General Tab, page 15-11.
- History—The history of the ticket. See History Tab, page 15-12.
- Affected Parties—The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket. See Affected Parties Tab, page 15-13.
- Correlation—All the alarms that are correlated to the selected ticket. See Correlation Tab, page 15-15.
- Notes—Enables you to add notes to the selected ticket. See Notes Tab, page 15-16.
- Advanced—All the affected devices, correlation, duplication and reduction counts for the selected ticket. In addition, it provides any other additional information available about the ticket. See Advanced Tab, page 15-16.

## General Tab

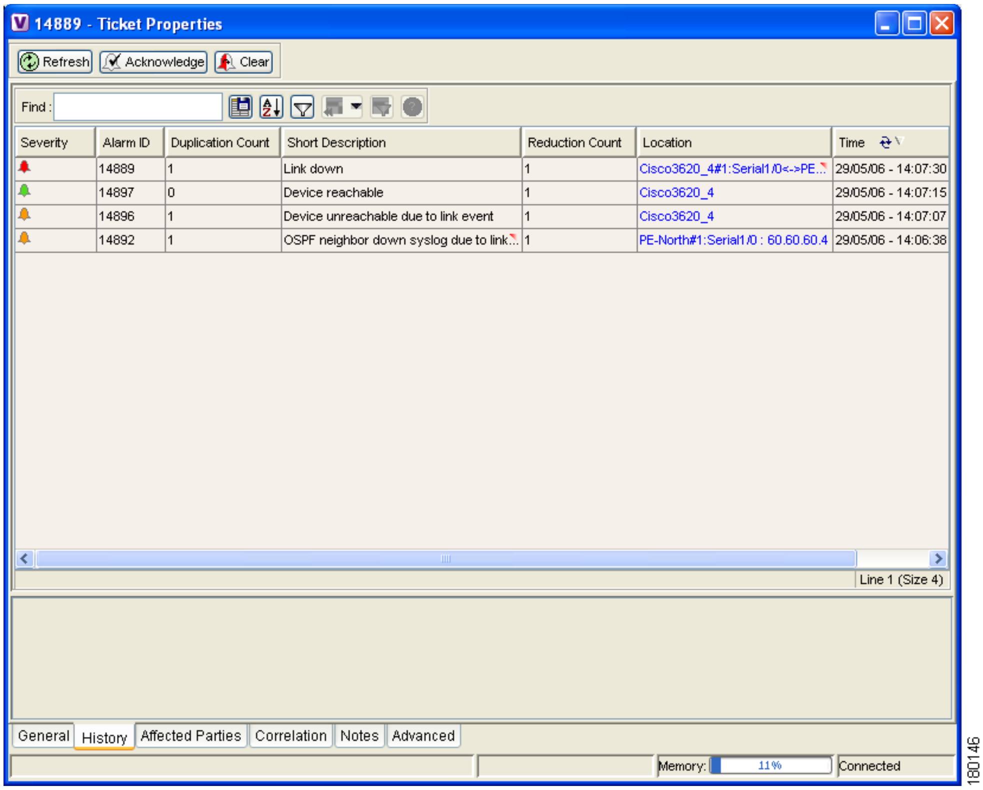
The following fields are displayed in the General tab and provide information about the compiled alarm:

- Alarm—The supported root-cause alarm name, for example, link down.
- Location—The entity that triggered the root-cause alarm, as a hyperlink that opens the relevant location.
- Severity—Displays the severity that was propagated from all the correlated alarms. For more information. See Map View, page 2-5.
- Time—The date and time when the initial root-cause alarm was generated. The time is taken from Cisco ANA.
- Open Alarms—The number of correlated alarms for the ticket that are open. For example, 3 / 4. Four relates to the total number of correlated alarms for the ticket. Three indicates the number of alarms that have not been cleared; therefore, there is one alarm that is cleared.
- Acknowledged—The status of the ticket that is being handled: acknowledged (true) and unacknowledged (false).
- Description—The detailed description of the ticket.

## History Tab

The History tab enables you to display the history of the ticket, including all the events. Figure 15-6 shows the History tab.

*Figure 15-6 History Tab*



| Severity | Alarm ID | Duplication Count | Short Description | Reduction Count | Location | Time |
|---|---|---|---|---|---|---|
| ● | 14889 | 1 | Link down | 1 | Cisco3620_4#1:Serial1/0<->PE.. | 29/05/06 - 14:07:30 |
| ● | 14897 | 0 | Device reachable | 1 | Cisco3620_4 | 29/05/06 - 14:07:15 |
| ● | 14896 | 1 | Device unreachable due to link event | 1 | Cisco3620_4 | 29/05/06 - 14:07:07 |
| ● | 14892 | 1 | OSPF neighbor down syslog due to link.. | 1 | PE-North#1:Serial1/0 : 60.60.60.4 | 29/05/06 - 14:06:38 |

The following columns are displayed in the History tab and provide information about the compiled alarm:

- Severity—Displays a severity bell icon, which is colored according to the severity of the alarm.
- Alarm ID—The ID number of the event that changed the ticket.
- Duplication Count—The number of occurrences of the root alarm in a subsequent sequence. For example, Link Down, Link Up, Link Down would equal a duplication count of 2.
- Short Description—A description of the event.
- Reduction Count—The number of alarms displayed under the ticket. For example, nine alarms may be viewed in the History tab accessed from the Cisco ANA NetworkVision ticket pane, whereas only a single ticket is displayed in the ticket pane.
- Location—The entity that triggered the alarm, as a hyperlink that opens the relevant location.
- Time—The date and time when the ticket changed.

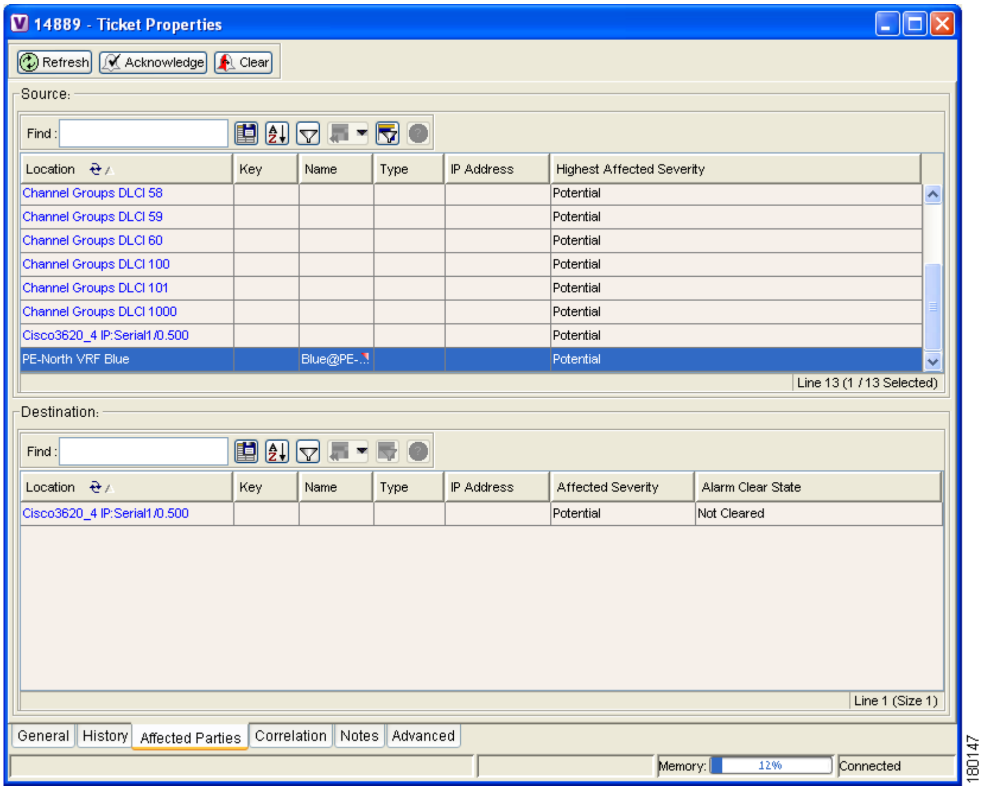
## Affected Parties Tab

When a fault occurs, Cisco ANA automatically calculates the affected parties (automatic impact analysis), for example, when a link goes down, and embeds this information in the ticket along with all the correlated faults. You can view a list of all the endpoints that are affected. For more information about proactive impact analysis, see Impact Analysis Options, page 15-2.

The Affected Parties tab displays the service resources (affected pairs) that are affected (automatic impact analysis) by the ticket. For more information about accumulating affected parties, see Filtering Tickets by Device, page 15-8.

The Affected Parties tab is displayed.

***Figure 15-7 Affected Parties Tab***



Source:

| Location | Key | Name | Type | IP Address | Highest Affected Severity |
|---|---|---|---|---|---|
| Channel Groups DLCI 58 | | | | | Potential |
| Channel Groups DLCI 59 | | | | | Potential |
| Channel Groups DLCI 60 | | | | | Potential |
| Channel Groups DLCI 100 | | | | | Potential |
| Channel Groups DLCI 101 | | | | | Potential |
| Channel Groups DLCI 1000 | | | | | Potential |
| Cisco3620_4 IP:Serial1/0.500 | | | | | Potential |
| PE-North VRF Blue | | Blue@PE-.. | | | Potential |

Line 13 (1 / 13 Selected)

Destination:

| Location | Key | Name | Type | IP Address | Affected Severity | Alarm Clear State |
|---|---|---|---|---|---|---|
| Cisco3620_4 IP:Serial1/0.500 | | | | | Potential | Not Cleared |

Line 1 (Size 1)

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 and provide 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, see the *Cisco Active Network Abstraction 3.6.6 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, see the *Cisco Active Network Abstraction 3.6.6 MPLS User Guide*.
- Highest Affected Severity—The highest 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 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:

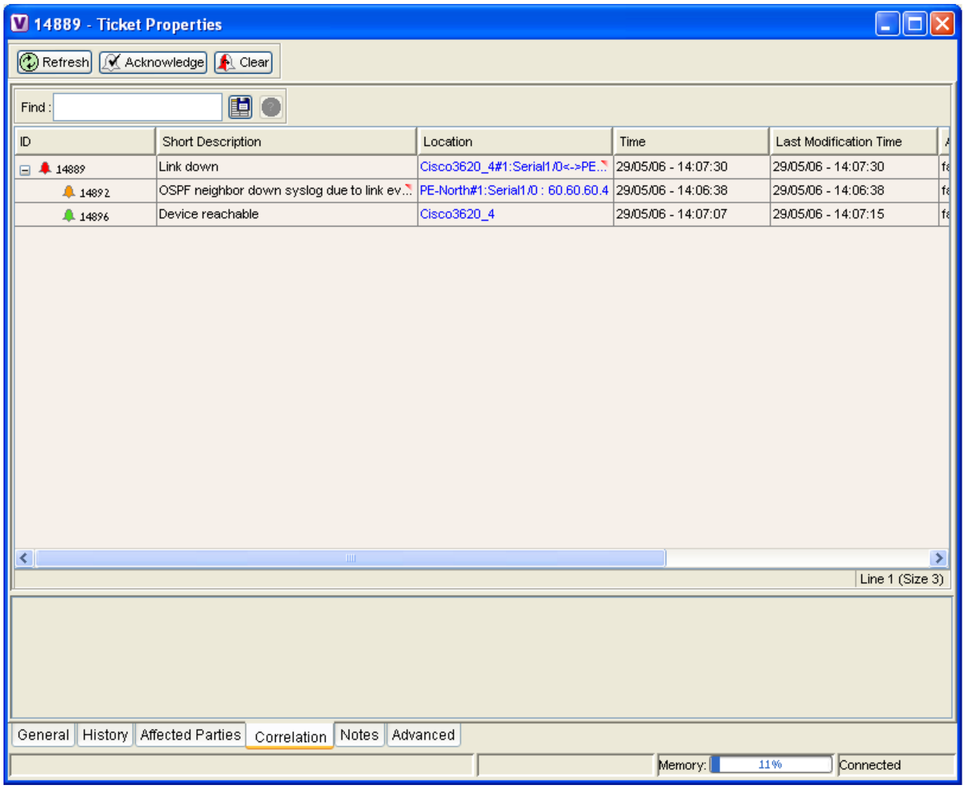
- Affected Severity—The severity of the affected pair as calculated by the client according to the rules defined in Filtering Tickets by Device, page 15-8.
- Alarm Clear State—An indication for each pair of the clear state of the alarm. The following states exist:
  - Not Cleared—One or more alarms for this pair have not been cleared.
  - 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. For more information about viewing a detailed report, see Acknowledging a Ticket, page 15-17.

## Correlation Tab

The Correlation tab displays all the alarms that are correlated to the selected ticket.

*Figure 15-8 Correlation Tab*



Find :

| ID | Short Description | Location | Time | Last Modification Time | A |
|---|---|---|---|---|---|
| ⊟ 14889 | Link down | Cisco3620_4#1:Serial1/0<->PE... | 29/05/06 - 14:07:30 | 29/05/06 - 14:07:30 | fa |
| 14892 | OSPF neighbor down syslog due to link ev... | PE-North#1:Serial1/0 : 60.60.60.4 | 29/05/06 - 14:06:38 | 29/05/06 - 14:06:38 | fa |
| 14896 | Device reachable | Cisco3620_4 | 29/05/06 - 14:07:07 | 29/05/06 - 14:07:15 | fa |

Line 1 (Size 3)

Each branch provides a short description of the alarm, a severity icon, ID, location, and time of the alarm. For more information about the columns displayed in the Correlation tab, see Ticket Pane, page 2-11.

The following columns are displayed in the Correlation tab and provide information about the alarm as follows:

- ID—The ID number of the alarm. The branches can be expanded and collapsed in order to hide information as needed.
- Short Description—A description of the change in the ticket. The full description is displayed in the lower tab area.
- Location—A hyperlink that opens an Inventory window displaying the selected node along with the affected parties.
- Time—The date and time the alarm was issued.
- Last Modification Time—The date and time when the alarm changed.
- Reduction Count—The number of alarms displayed under the ticket. For example, nine alarms may be viewed in the History tab accessed from the Cisco ANA NetworkVision ticket pane, whereas only a single ticket is displayed in the ticket pane.
- Duplication Count—The number of occurrences of the root alarm in a subsequent sequence. For example, Link Down, Link Up, Link Down would equal a duplication count of 2.

The Find field on the toolbar enables you to search for information in the Correlated Alarms table.

## Notes Tab

The Notes tab enables you to add and save notes for the selected ticket. To add text, enter text in the Notes field and click **Save Notes**. The new text is added to any previously existing text.

**Note**

- Save Notes is only enabled when text is entered in the Notes field.
- The text cannot be edited or removed once you have saved the notes.

## Advanced Tab

The Advanced tab enables you to view all the affected devices, correlation, duplication and reduction counts for the selected ticket. In addition, it provides any other additional information available about the ticket.

The following fields are displayed in the Advanced tab and provide information about the compiled alarm:

- Successor—A hyperlink to the successor event (if it exists), for example, port up.
- Correlator—A hyperlink to the correlator alarm (if it exists).
- Predecessor—A hyperlink to the predecessor event (if it exists), for example, port down.
- Affected Devices—The number of devices affected by the ticket (the sources of the alarm and their subsequent alarms).
- Duplication Count—Displays the number of occurrences of the original root-cause alarm included in the ticket. For example, if the ticket was created by a link-down root-cause alarm, and then the link goes up and down again quickly so that it is included in the same ticket, then the duplication counter displays the number 2, because the root-cause alarm occurred twice.
- Correlation Count—Displays the number of correlated alarms included in the ticket. For example, if in the Correlation tab of the Ticket Properties, there are 3 alarms correlated to the root-cause alarm, then the counter displays the number 3. If there are 2 alarms correlated to the root-cause alarm, and each alarm in turn has 2 alarms correlated to it, then the counter displays the number 4.
- Reduction Count—Displays the number of alarms included in the ticket. For example, nine alarms can be viewed in the History tab of the Ticket Properties window, but only a single ticket is displayed in the ticket pane.

## Toolbar

The Ticket Properties dialog box contains the following tools:

| | |
|---|---|
| | Refreshes the information displayed in the Ticket Properties dialog box. |
| | Acknowledges that the ticket is being handled. The status of the ticket is displayed as true in the ticket pane and in the Ticket Properties dialog box. For more information, see Acknowledged Ticket, page 15-20.<br>If a ticket was acknowledged, and some events were correlated to it afterward, then the ticket is considered to have not been acknowledged.<br>**Note** This button is only enabled if the ticket is not acknowledged. |
| | Requests the relevant Cisco ANA to remove the faulty network element from the Cisco ANA networking inventory. In addition, it sets the ticket to Cleared severity or status (the icon is displayed in green) and automatically changes the acknowledged status of the ticket to true. For more information, see Cleared Ticket, page 15-20.<br>**Note** This button is only enabled if the severity of the alarm is higher than Cleared or Normal. |
| | Saves the notes for the selected ticket.<br>**Note** This button is only enabled when text is entered in the Notes field of the Notes tab. |

# Acknowledging a Ticket

When an alarm occurs, a warning or ticket is displayed in the ticket pane. Cisco ANA NetworkVision enables you to handle the status of a ticket by acknowledging it. This acknowledges the fault.

The change is reported to the Cisco ANA Gateway and all open Cisco ANA NetworkVision applications. Several tickets can be acknowledged at the same time. For more information, see Ticket Status in the Ticket Pane, page 15-19.

**Note** Rule-based alarms can be configured per customer site or upon request.

An acknowledged ticket will change back to not acknowledged when a new event is correlated to it.

**Note** You cannot undo this operation.

To acknowledge a ticket, do one of the following:

- Right-click a ticket in the ticket pane and choose **Acknowledge**.
- Double-click a ticket in the ticket pane and click **Acknowledge**.

For more information, see Ticket Status in the Ticket Pane, page 15-19.

# Clearing a Ticket

When an alarm occurs, a warning or ticket is displayed in the ticket pane. Cisco ANA NetworkVision enables you to handle the reported ticket by verifying the report of what is faulty and clearing the faulty network element. The change is reported to the Cisco ANA Gateway and all open Cisco ANA NetworkVision applications. This operation cannot be reversed.

**Note** Before using Clear and Remove (which may also be available when you right-click a ticket), be sure you understand the results of *removing* a ticket. Like the clear operation, the remove operation cannot be reversed. See Removing a Ticket, page 15-18.

Clearing an open ticket performs the following operations:

- Sends a request to the Cisco ANA system to remove the faulty network element from the Cisco ANA networking inventory.
- Sets the alarm to Cleared or Normal severity or status by issuing a corresponding Clear alarm.
- Automatically sets the alarm severity or status to acknowledged (true).

**Note** When a Card Out or link-down alarm occurs, the relevant information is displayed in the inventory and maintained in the VNE.

To clear a ticket, do one of the following:

- Right-click a ticket in the ticket pane and choose **Clear**.
- Double-click a ticket in the ticket pane and click **Clear**.

For more information, see Ticket Status in the Ticket Pane, page 15-19.

# Removing a Ticket

When an alarm occurs, a warning or ticket is displayed in the ticket pane. Cisco ANA NetworkVision enables you to completely remove the ticket and all its active alarms and business tags. The change is reported to the Cisco ANA Gateway and all open Cisco ANA NetworkVision applications. In addition, several tickets can be removed at the same time. When a ticket has been cleared or when an 'Up Alarm' occurs, then the ticket can be removed.

**Note** This operation cannot be reversed. A ticket that has been removed can only be viewed using Cisco ANA EventVision.

Removing an alarm performs the following operations:

- Sends a request to the Cisco ANA system to remove the faulty network element from the Cisco ANA networking inventory.
- Archives the ticket and active alarms.
- Removes the ticket from the Cisco ANA NetworkVision ticket pane.
- Notifies all the open Cisco ANA NetworkVision applications of the removal.

**Note** Only tickets with a Cleared/Normal or Information severity can be removed.

To remove a ticket, right-click the ticket in the ticket pane and choose **Remove**.

For more information, see Ticket Status in the Ticket Pane, page 15-19.

In addition, an uncleared ticket (which has a severity higher than Cleared or Normal) can be cleared and removed by right-clicking in the ticket pane and choosing **Clear and Remove**. For more information about the Ticket shortcut menu, see Ticket Shortcut Menu, page 2-26.

# Ticket Status in the Ticket Pane

The appearance of a ticket displayed in the ticket pane depends on the status or severity of the (ticket) alarm and what operations have been performed on the ticket. Tickets detailed in the ticket pane change when:

- A ticket is generated.
- A ticket is cleared.
- A ticket is acknowledged.
- An Up ticket is generated.
- A ticket is cleared and removed.
- A ticket is removed.
- Some other properties are updated, for example, severity, description, counters and so on.

## Generated Ticket

Table 15-1 shows an example of the appearance of the ticket pane when a ticket is generated.

*Table 15-1 Generated Ticket*

| Severity | | Ticket ID | Short Description | Acknowledged |
|---|---|---|---|---|
| 🔔 | (Major) | 27 | Port down | False (Not Acknowledged) |

## Cleared Ticket

Table 15-2 shows an example of the appearance of the ticket pane when a ticket is cleared.

*Table 15-2 Cleared Ticket*

| Severity | | Ticket ID | Short Description | Acknowledged |
|---|---|---|---|---|
| 🔔 | (Normal) | 27 | Cleared due to Force Clear | True (Acknowledged) |

A ticket that has been cleared can then be removed from the ticket pane. For more information, see Removing a Ticket, page 15-18.

When a ticket is cleared, its definition automatically changes to acknowledged in the ticket pane and its definition in the Acknowledged column is True.

## Acknowledged Ticket

Table 15-3 shows an example of the appearance of the ticket pane when a ticket is acknowledged. When a ticket is acknowledged it can then be cleared and the severity changes to Normal.

*Table 15-3 Acknowledged Ticket*

| Severity | | Ticket ID | Short Description | Acknowledged |
|---|---|---|---|---|
| 🔔 | (Major) | 27 | Port up | True |

**Note** When a ticket with an Information severity is acknowledged, the ticket is automatically removed from the Cisco ANA Gateway and from the ticket pane.

## Generated Up Ticket

The cause of the alarm is fixed; therefore an Up ticket is automatically generated with a Normal severity. Table 15-4 shows an example of the appearance of the ticket pane when an Up ticket is generated.

*Table 15-4 Generated Up Ticket*

| Severity | | Ticket ID | Short Description | Acknowledged |
|---|---|---|---|---|
| 🔔 | (Normal) | 27 | Port up | True |

## Clearing and Removing Tickets

Approves the reported faulty ticket and clears the faulty networking entity from Cisco ANA.