CHAPTER 9

Working with Tickets in Cisco Prime Network Vision

These topics describe how to work with tickets in Prime Network Vision:

What are Tickets?

A ticket represents the complete hierarchy of correlated alarms representing a single specific fault scenario. A ticket points to the root cause alarm that is the top-most alarm in the correlation hierarchy. Examples of alarms are Link Down, Device Unreachable, or Module Out. Some event types are capable of creating tickets. When an event is generated, it is correlated to an existing event, which is correlated to a ticket. If there is no existing ticket, a new ticket is created.

Prime Network identifies the relationship between a root cause alarm and its consequent alarms. It automatically correlates the consequent alarms as children of the root alarm. The ticket pane displays the ticket (the root cause alarm), the aggregated severity of the ticket, and the severity of the root cause alarm. The root cause alarm severity is the top-most severity of its contained alarms. In addition, the ticket pane displays the time at which the original event was detected, the ticket creation time, and a description of the event that caused the ticket creation.

User Roles Required to Work with Tickets in Prime Network Vision

This topic identifies the roles that are required to work with tickets in Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

- For GUI-based tasks (tasks that do not affect elements), authorization is based on the default permission that is assigned to your user account.

- For element-based tasks (tasks that do affect elements), authorization is based on the default permission that is assigned to your account. That is, whether the element is in one of your assigned scopes and whether you meet the minimum security level for that scope.

For more information on user authorization, see the topic on device scopes in the *Cisco Prime Network 4.0 Administrator Guide*.

The following conditions apply when working with tickets in Prime Network Vision:

- If an element that is outside of your scope is the root cause of a ticket that affects an element in your scope, you can view the ticket in Prime Network Vision, but you will not be able to:
  - View inventory by clicking the Location hyperlink.
  - Acknowledge, deacknowledge, clear, add note, or remove the ticket.
- You can acknowledge, deacknowledge, clear, remove, or add notes for a ticket only if you have OperatorPlus or higher permission for the element that holds the root alarm for that ticket.
- If the source or contained sources of the ticket are not in your scope, you cannot view the ticket in the ticket table, view ticket properties, or perform actions on the ticket.
- If the ticket contains a source that is in your scope, but the source is not the root cause, you can view the ticket in the ticket table and view ticket properties, but you cannot perform actions on the ticket.
- If the source of the ticket is in your scope, you can view the ticket in the ticket table, view ticket properties, filter tickets, and perform actions on the ticket.
- By default, users with the Administrator role have access to all managed elements and can perform any action on tickets. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 4.0 Administrator Guide*.

Table 9-1 identifies the roles required to perform the high level tasks:

Table 9-1 Default Roles/Permissions Required for Working with Tickets in Prime Network Vision

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Acknowledge/deacknowledge tickets	—	—	X[1]	X	X
Add notes to a ticket	—	—	X[1]	X	X
Clear and remove tickets	—	—	X[1]	X	X
Clear tickets	—	—	X[1]	X	X
Filter tickets	X	X	X	X	X
Find affected elements	X	X	X	X	X
Remove tickets	—	—	X[1]	X	X
View ticket properties	X	X	X	X	X
View tickets	X	X	X	X	X

[1] In addition, the security level for the device scope must be OperatorPlus or higher for the device that holds the root alarm for a ticket.

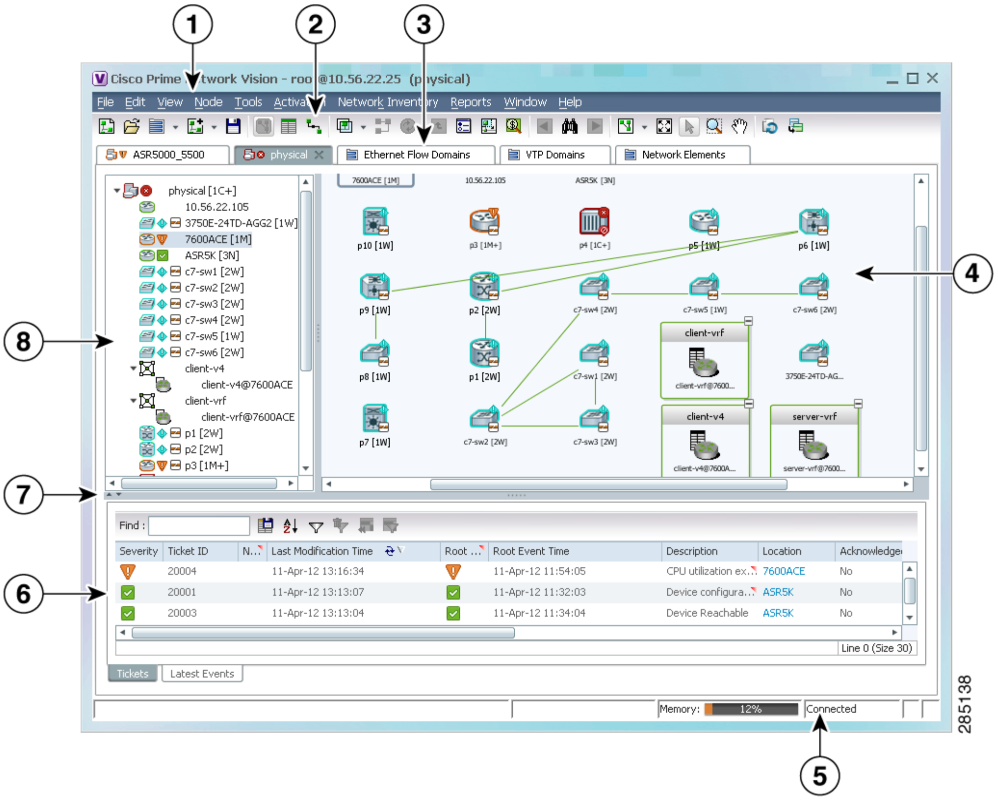
Viewing Tickets and Network Events for Elements in a Map

The ticket pane, located below the navigation and content panes in the Prime Network Vision window, displays tickets and network events specific to the elements in the currently displayed map (see Figure 9-1). You can view or hide the ticket pane by clicking the arrows displayed below the navigation pane.

The ticket pane contains two tabs:

- Tickets tab—Lists all the tickets relevant to the elements in the map and allows you to manage them. See Managing Tickets in the Tickets Tab, page 9-4 for details of the information displayed and the actions available from the Tickets tab.
- Latest Events tab:
  - Lists network events that were created for the elements in the map from the time the map was opened.
  - Shows network events that Prime Network recognizes and is able to process (actionable events). Some of these events might be correlated into tickets.
  - An hourglass in the Status column indicates that processing of the event is in progress. A check mark indicates that the event has been processed.
  - If an event has been correlated into a ticket, the ticket ID will appear in the table and you can click the link to access the ticket properties.
  - Events are removed from the Latest Events tab after 6 hours or when a maximum of 15000 events is reached, in which case the oldest events are removed first.

Figure 9-1 Prime Network Vision Window



Severity	Ticket ID	N...	Last Modification Time	Root ...	Root Event Time	Description	Location	Acknowledge
!	20004		11-Apr-12 13:16:34	!	11-Apr-12 11:54:05	CPU utilization ex...	7600ACE	No
✓	20001		11-Apr-12 13:13:07	✓	11-Apr-12 11:32:03	Device configura...	ASR5K	No
✓	20003		11-Apr-12 13:13:04	✓	11-Apr-12 11:34:04	Device Reachable	ASR5K	No

1	Menu bar	**5**	Status bar
2	Toolbar	**6**	Ticket pane
3	Inventory and map tabs	**7**	Hide/Display ticket pane
4	Content pane	**8**	Navigation pane

Managing Tickets in the Tickets Tab

Table 9-2 describes the functions that are available from the Tickets tab in the ticket pane.

Table 9-2 Ticket Pane Available Functions

Function	Related Documentation
Acknowledge a ticket.	Acknowledging/Deacknowledging a Ticket, page 9-15
Clear a ticket.	Clearing a Ticket, page 9-15
Clear and remove a ticket.	Clearing and Removing Tickets, page 9-16
Filter and view all tickets that meet specific criteria.	Filtering Tickets by Criteria, page 9-7

Table 9-2 Ticket Pane Available Functions (continued)

Function	Related Documentation
Locate the elements or links affected by the ticket in the map or links view.	Finding Affected Elements, page 9-15
Remove a ticket.	Removing a Ticket, page 9-16
View all tickets or only the filtered tickets of a selected element.	Filtering Tickets by Network Element, page 9-6
View tickets.	Viewing Tickets and Network Events for Elements in a Map, page 9-3
View ticket properties, including the history, correlated alarms, severity of the root cause alarm, and affected parties.	Viewing Ticket Properties, page 9-9

Table 9-3 describes the information displayed in the ticket pane.

Table 9-3 Ticket Information Displayed in the Ticket Pane

Field Name	Description
Severity	Severity of alarm, represented by an icon. The icon and its color indicate the alarm severity and thereby the impact of the alarm on the network. For more information about severity, see Map View, page 2-8. • Red—Critical • Orange—Major • Yellow—Minor • Light Blue—Warning • Green—Cleared • Medium Blue—Informational • Dark Blue—Indeterminate
Ticket ID	Ticket identifier, assigned sequentially. Click the hyperlinked entry to view ticket properties, and to acknowledge, clear, or refresh the ticket. For more information, see Chapter 9, "Working with Tickets in Cisco Prime Network Vision."
Notes	An icon in this column indicates that a note has been added for the ticket. Click on the icon to read the note and add your own note, if necessary.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Root Cause	Severity of the root cause alarm, represented by a bell icon. The color indicates the severity of the root cause alarm, as described in the Severity field.
Root Event Time	Date and time that the event that created the root cause alarm of the ticket was detected.
Description	Description of the event that caused the ticket creation.
Location	Entity that triggered the ticket, as a hyperlink that displays the relevant location in the inventory.

Table 9-3 Ticket Information Displayed in the Ticket Pane (continued)

Field Name	Description
Element Type	The type of element that triggered the root event, e.g., Cisco 7606.
Acknowledged	Whether the ticket is acknowledged or has been modified: Yes, No, or Modified. If the ticket is acknowledged, this field also displays the user who acknowledged the ticket; for example, Yes(root).
Creation Time	Date and time (per the database) that the ticket was created.
Event Count	Number of events associated with the ticket.
Affected Devices Count	Number of devices affected by the ticket, including the sources of the alarm and their subsequent alarms.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event. For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event. Ticket reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Windows Properties window displays one reduction count for each event listed.
Alarm Count	Total number of alarms associated with the ticket, including the root alarm.

The ticket details in the ticket pane change automatically as new information arrives. For example, Port Down is updated to Port Up.

By default, the tickets in the ticket pane are sorted according to the last modification time.

The Find field enables you to search for information in the ticket pane table according to the selected column. For more information about the buttons displayed in Prime Network Vision tables and table functionality, see Filtering and Sorting Tabular Content, page 2-42.

Filtering Tickets by Network Element

Prime Network Vision enables you to filter the tickets that are shown in the ticket pane so that you see only the tickets that have the selected network element as the root cause.

If the selected network element is alarmed due to an operation that occurred on a different VNE, element, or link, no tickets are displayed.

To view tickets that have a specific network element as the root cause, do either of the following:

- If the network element icon is at the largest size, click the **Filter Tickets** button.
- Right-click the required network element in the navigation pane or a map and choose **Filter Tickets**.

In response:

- The ticket pane displays only the tickets that have the selected network element as the root cause.
- The Filter button in the ticket pane toggles to indicate that a filter has been applied.

Click **Clear Filter** in the ticket pane to view all tickets.

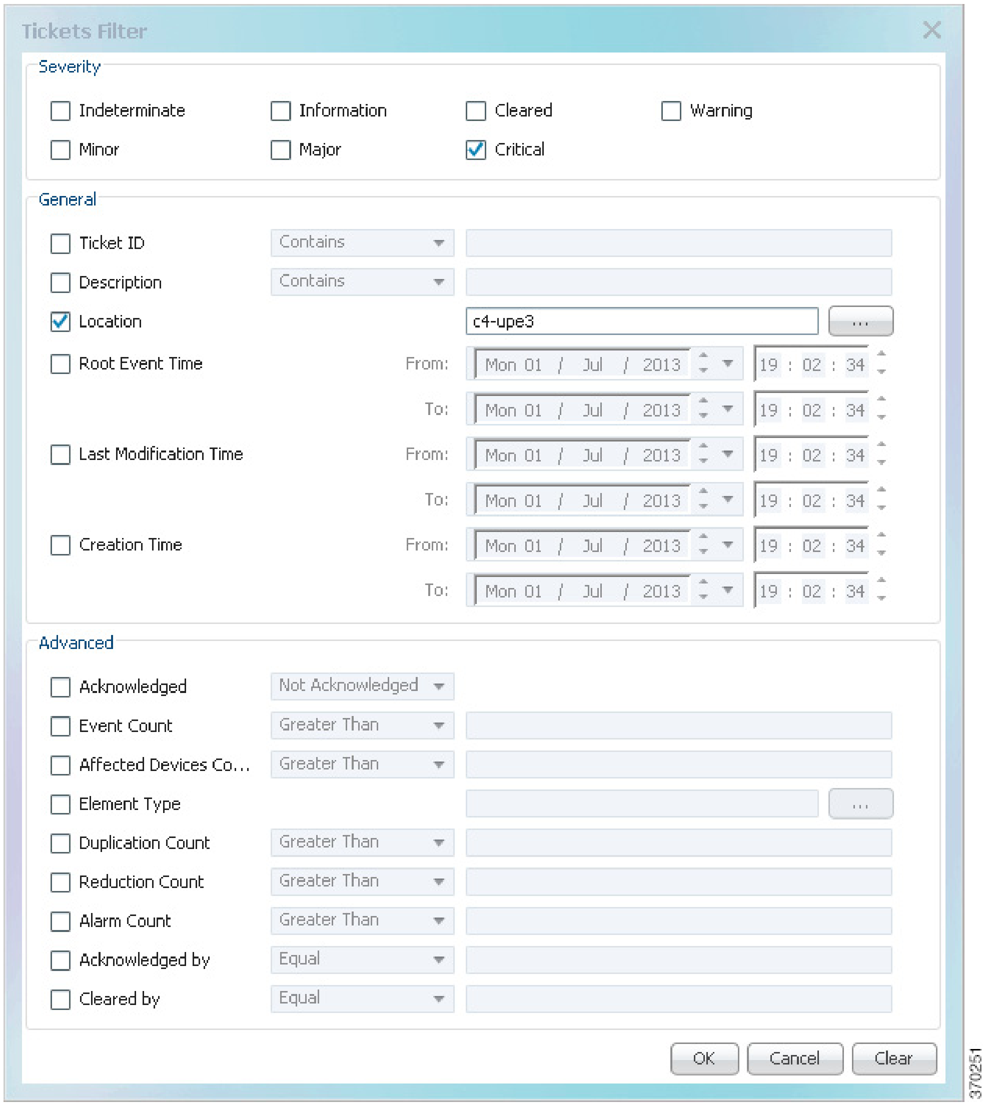
Filtering Tickets by Criteria

Prime Network Vision 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 a ticket filter:

Step 1 Click **Ticket Filter** in the ticket pane toolbar. The Ticket Filter dialog box is displayed (Figure 9-2).

Figure 9-2 Ticket Filter Dialog Box



Tickets Filter

Severity

□ Indeterminate □ Information □ Cleared □ Warning

□ Minor □ Major ☑ Critical

General

□ Ticket ID Contains

□ Description Contains

☑ Location c4-upe3 ...

□ Root Event Time From: Mon 01 / Jul / 2013 19 : 02 : 34

To: Mon 01 / Jul / 2013 19 : 02 : 34

□ Last Modification Time From: Mon 01 / Jul / 2013 19 : 02 : 34

To: Mon 01 / Jul / 2013 19 : 02 : 34

□ Creation Time From: Mon 01 / Jul / 2013 19 : 02 : 34

To: Mon 01 / Jul / 2013 19 : 02 : 34

Advanced

□ Acknowledged Not Acknowledged

□ Event Count Greater Than

□ Affected Devices Co... Greater Than

□ Element Type ...

□ Duplication Count Greater Than

□ Reduction Count Greater Than

□ Alarm Count Greater Than

□ Acknowledged by Equal

□ Cleared by Equal

Step 2 Specify the filter criteria by using the following steps and the information in Table 9-4:

a. Check the check box for each criterion to use for filtering.

b. As needed, choose the operator for the filter, such as Contains or Does Not Contain.

c. Supply the specific information to apply to the filter, such as the time, a string, or one or more IP addresses.

Table 9-4 Prime Network Ticket Filter Options

Field	Description
Severity	Severity to be included in the filter.
General	
Ticket ID	Ticket identifier to be included or excluded when filtering.
Description	String in the ticket description to include or exclude.
Location	Network elements to include.
Root Event Time	Beginning and ending dates and times of the range for the root event time to apply to the filter.
Last Modification Time	Beginning and ending dates and times of the range for the ticket last modification time to apply to the filter.
Creation Time	Beginning and ending dates and times of the range for the ticket creation time to apply to the filter.
Advanced	
Acknowledged	Ticket acknowledgement status to include in the filter: Acknowledged, Not Acknowledged, or Modified.
Event Count	Event count value to use for filtering.
Affected Devices Count	Number of affected devices to use for filtering.
Element Type	Filter by the type of device that triggered the root event.
Duplication Count	Duplication count value to use for filtering.
Reduction Count	Reduction count value to use for filtering.
Alarm Count	Alarm count value to use for filtering.
Archived	Archive status to use for filtering: True or False.
Acknowledged By	Username of the person who acknowledged the ticket.
Cleared By	Username of the person who cleared the ticket.

Step 3 Click **OK**. The 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 a ticket filter:

Step 1 Click **Ticket Filter** 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.

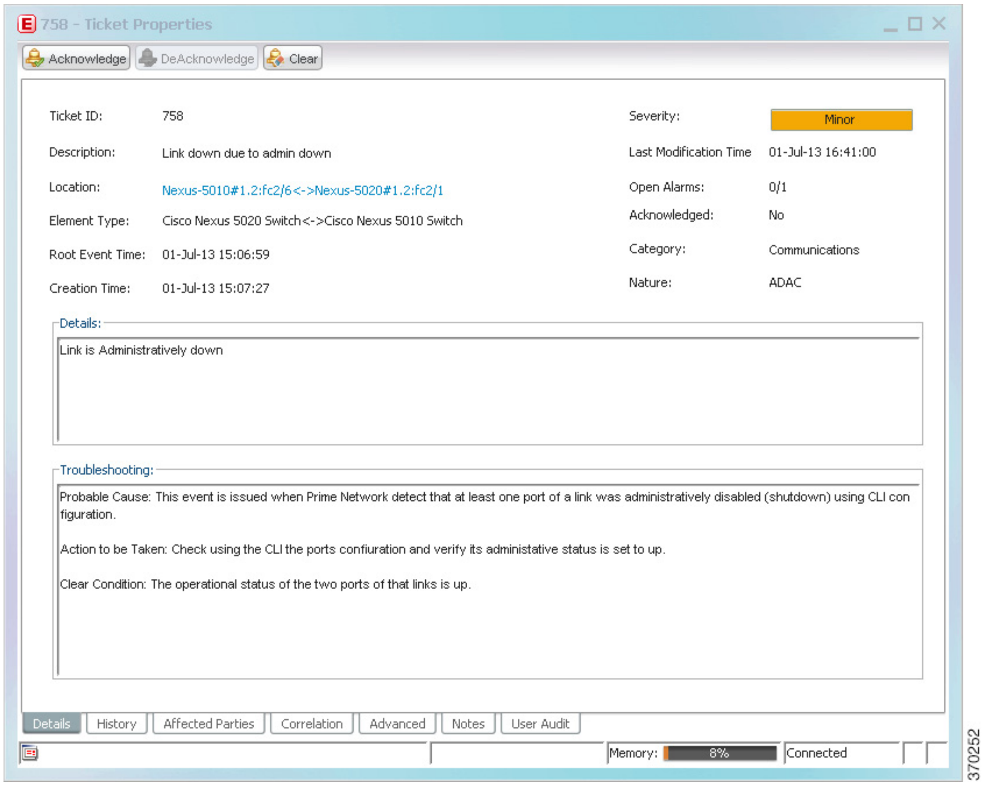
Viewing Ticket Properties

In Prime Network Vision, open the Ticket Properties window in one of the following ways:

- Open the required map and then double-click the required ticket identifier in the ticket pane.
- Open the required map, right-click a ticket in the ticket pane, and choose **Properties**.

Figure 9-3 shows the Ticket Properties window.

Figure 9-3 Ticket Properties Window



Ticket ID:	758	Severity:	Minor
Description:	Link down due to admin down	Last Modification Time	01-Jul-13 16:41:00
Location:	Nexus-5010#1.2:fc2/6<->Nexus-5020#1.2:fc2/1	Open Alarms:	0/1
Element Type:	Cisco Nexus 5020 Switch<->Cisco Nexus 5010 Switch	Acknowledged:	No
Root Event Time:	01-Jul-13 15:06:59	Category:	Communications
Creation Time:	01-Jul-13 15:07:27	Nature:	ADAC

Details:

Link is Administratively down

Troubleshooting:

Probable Cause: This event is issued when Prime Network detect that at least one port of a link was administratively disabled (shutdown) using CLI configuration.

Action to be Taken: Check using the CLI the ports confiuration and verify its administative status is set to up.

Clear Condition: The operational status of the two ports of that links is up.

The information displayed in the Ticket Properties window corresponds with the information displayed in the Prime Network Vision ticket pane or the Prime Network Vision window. The ID number displayed in the header corresponds to the ID number of the ticket selected in the ticket pane.

The Ticket Properties window contains the following components:

- Details Tab, page 9-10
- Details Tab, page 9-10
- History Tab, page 9-11
- Affected Parties Tab, page 9-11
- Correlation Tab, page 9-13
- Advanced Tab, page 9-13
- Notes Tab, page 9-14
- User Audit Tab, page 9-14

Details Tab

Table 9-5 describes the information that is displayed in the Details tab about the ticket.

Table 9-5 Event Properties Window - Details Tab

Field	Description
Ticket ID	Ticket identifier.
Severity	Severity propagated from all the correlated alarms.
Description	Description of the ticket.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Location	Entity that triggered the root-cause alarm, as a hyperlink that opens the relevant location. **Note** If the entity that triggered the alarm is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Element Type	The type of device on which the root event occurred, e.g., Cisco Nexus 5020 Switch
Open Alarms	Number of correlated alarms for the ticket that are open, such as 3/4. In this example, four indicates the total number of correlated alarms for the ticket, and three indicates the number of alarms that have not been cleared. Therefore, one alarm has been cleared.
Root Event Time	Date and time that the event that created the root cause alarm of the ticket was detected.
Acknowledged	Whether the ticket is acknowledged or has been modified: Yes, No, or Modified. If the ticket is acknowledged, this field also displays the user who acknowledged the alarm; for example, Yes(root). If a ticket changes after it has been acknowledged, it is marked as Modified. If an acknowledged ticket is deacknowledged, the status changes from Yes to No.
Creation Time	Date and time the ticket was created.
Details	Detailed description of the alarm.
Troubleshooting	Provides information about the probable cause of the last event in the root alarm and the action that should be taken to resolve the problem. In this release, troubleshooting information is provided for service events and for traps on ASR 5000 devices only.

History Tab

The History tab enables you to display the history of the ticket, including all the events. Table 9-6 describes the information that is displayed in the History tab.

Table 9-6 Ticket Properties Window - History Tab

Field	Description
Severity	Severity bell icon, colored according to the severity of the alarm.
Event ID	Event identifier of the specific alarm.
Time	Date and time the event was received by the Event Collector.
Description	Description of the event.
Location	Entity that triggered the alarm, as a hyperlink that opens the relevant location. **Note** If the entity that triggered the alarm is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Element Type	The type of device on which the root event occurred, e.g., Cisco Nexus 5020 Switch
Alarm ID	Alarm identifier.
Ticket ID	Ticket identifier. This field appears in the History tab only in Prime Network Events.
Causing Event ID	Identifier of the causing event for the ticket.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
Detail panel	Long description of the selected event.

Affected Parties Tab

The Affected Parties tab displays the service resources (pairs) that are affected by an event, an alarm, or a ticket. When a fault occurs, Prime Network automatically calculates the affected parties 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.

The Affected Parties tab displays the service resources (affected pairs) that are affected by the ticket.

The Affected Parties tab contains two tables: Source and Destination. Table 9-7 describes the information that is displayed in the Affected Properties tab.

Table 9-7 Ticket Properties Window - Affected Parties Tab

Field	Description
Source Table	
Location	Hyperlinked entry to the port with the affected parties.
Key	Unique value taken from the affected element's business tag key, if it exists.
Name	Subinterface (site) name or business tag name of the affected element, if it exists.
Type	Business tag type.
IP Address	If the affected element is an IP interface, the IP address of the subinterface site.
Affected Status (Agg)	Status for the affected pair (destination). The same source can be part of multiple pairs, and therefore each pair can have a different affected status. The highest affected status reflects the highest among these. The affected status can be one of the following: • Potential • Real • Recovered • N/A—From the links view, this indicates *Not Applicable*.
Destination Table	
Location	Hyperlinked entry to the port with the affected parties.
Key	Unique value taken from the affected element's business tag key, if it exists.
Name	Subinterface name or business tag name of the affected element, if it exists.
Type	Business tag type.
IP Address	If the affected element is an IP interface, the IP address of the subinterface site.
Affected Status	Status of the affected pair as calculated by the client according to the rules defined in Status Values for Affected Parties, page 9-17.
Alarm Clear State	For each pair, an indication of the clear state of the alarm: • Cleared—All related alarms for this pair have been cleared. • Not Cleared—One or more alarms for this pair have not been cleared.

When an affected side is selected in the Source table, the Destination table lists all endpoints with services that have been affected between them and the entry selected in the Source table.

Note The Affected Parties dialog box occasionally displays entries that start with the word *Misconfigured*. Entries that start with Misconfigured indicate that the flow has stopped unexpectedly between the source and destination points. An unexpected termination point can be a routing entity, bridge, or VC switching entity. The significant aspects of Misconfigured entries are:

- Because the link does not terminate as expected, the link is not actually impacted.
- An error might exist in the configuration or status of the termination points. We recommend that you check the configuration and status of the affected termination points.

Correlation Tab

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

Table 9-8 describes the information that is displayed in the Correlation tab.

Table 9-8 Ticket Properties Window - Correlation Tab

Field	Description
Alarm Correlation	Alarms correlated with the ticket. Expand or collapse the branch to display or hide information as needed. The severity displayed is the severity of the root alarm.
Short Description	Description of the alarm.
Location	Hyperlinked entry that opens an window displaying the selected node along with the affected parties. **Note** If the entity that triggered the alarm is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Acknowledged	Whether or not the root alarm has been acknowledged: Yes or No.
Last Event Time	Date and time the alarm was last modified.
Detail panel	Long description of the selected entry.

Advanced Tab

The Advanced tab displays the following values for the selected ticket:

- Duplication Count:
  - For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
  - For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
- Reduction Count:
  - For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
  - For tickets, reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Ticket Properties window displays one reduction count for each event listed.
- Affected Devices—The number of devices affected by the ticket.

- Alarm Count—The total number of alarms associated with the ticket, including the root alarm.

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.

After you save a note, it appears in the Previous Notes section of the Notes tab, with the name of the user who added the note and the time it was added. If the user is an external user (for example, a Netcool user), the username will be displayed in the following format:
“Added by prime-networkUserName (as externalUserName)”

The following restrictions apply to the Notes tab:

- You can add notes for a ticket only if both of the following conditions are true:
  - The default permission for your account is OperatorPlus or higher.
  - The security level for the device scope is OperatorPlus or higher for the device that holds the root alarm for that ticket.
- The Notes tab is not available for archived tickets.
- The Save Notes button is enabled only when text is entered in the Notes field.
- The text cannot be edited or removed once you have saved the notes.

User Audit Tab

The User Audit tab enables you to see which ticket-related actions were carried out by which users, and when the action took place.

If the user is an external user (for example, a Netcool user), the username will be displayed in the following format in the User Name column:
“Added by prime-networkUserName (as externalUserName)”

The following actions are reported in the User Audit tab:

- Acknowledge ticket
- Remove ticket (archive)
- Clear ticket

Managing Tickets

The following topics describe how to manage tickets:

- Finding Affected Elements, page 9-15
- Acknowledging/Deacknowledging a Ticket, page 9-15
- Clearing a Ticket, page 9-15
- Removing a Ticket, page 9-16
- Clearing and Removing Tickets, page 9-16

You can acknowledge, clear, remove, or clear and remove a ticket only if both of the following conditions are true:

- The default permission for your account is OperatorPlus or higher.
- The security level for the device scope is OperatorPlus or higher for the device that holds the root alarm for that ticket.

Note When Prime Network is in suite mode, the Acknowledge, Deacknowledge, Add Note, Clear, and Remove functions are disabled.

Finding Affected Elements

To locate elements affected by a ticket in Prime Network Vision, right-click the desired ticket in the ticket pane and then choose **Find Affected Elements**.

Depending on the number of affected elements, the results are displayed in one of the following ways:

- If only one element is affected, it is highlighted in the navigation pane and the content area.
- If multiple elements are affected, they are displayed in the Affected Events window.

Acknowledging/Deacknowledging a Ticket

You can acknowledge a ticket to indicate that the ticket is being handled. The change is reported to the Prime Network gateway and all open Prime Network applications. You can acknowledge multiple tickets at the same time.

If a new event is correlated to an acknowledged ticket, the ticket status becomes “Modified” and the ticket must be acknowledged again.

Acknowledged tickets can be manually deacknowledged.

To acknowledge/deacknowledge a ticket, right-click on the ticket and choose **Acknowledge/Deacknowledge**.

Clearing a Ticket

You can manually clear tickets when the issues they represent have been addressed.

When an open ticket is cleared, the following operations are performed:

- The ticket is acknowledged.
- All non-cleared alarms associated with the ticket are cleared.
- For tickets relating to physical network elements (e.g., link down, card out), the faulty network element is removed from the Prime Network inventory.

After a ticket is cleared, it remains open for one hour (default) before it is archived. Incoming events can be correlated to the ticket during this time, effectively re-opening the ticket. An administrator can lock tickets so that they remain cleared and no new events can be correlated to them. For more information, see the section, “Changing Oracle Database Fault Settings: Clear, Archive, and Purge Fault Data”, in the *Cisco Prime Network 4.0 Administrator Guide*.

To clear one or more tickets, do one of the following:

- Select one or more tickets in the ticket pane, and then right-click and choose **Clear**.
- Double-click a ticket in the ticket pane and click **Clear** in the Ticket Properties window.

To clear and remove a ticket at the same time, select **Clear and Remove** from the right-click menu.

Automatic Clearing of Tickets

If the system is set to automatically clear tickets, every minute the system scans for tickets that are not archived, not cleared, and that have not been modified in the last four minutes. If all the ticket's events that are not defined as auto-clear are cleared, the system will automatically clear the ticket.

Note If the root cause event is not cleared, the ticket will not be cleared.

Removing a Ticket

Prime Network Vision enables you to completely remove a ticket and all of its active alarms. The ticket is archived and removed from the ticket pane. The change is reported to the Prime Network gateway and all instances of Prime Network that are open. Only tickets with a status of Cleared or Information can be removed.

Note This operation cannot be reversed. A ticket that has been removed can be viewed only by using Prime Network Events.

When a ticket is removed:

- New alarms that might be related to the ticket, and should therefore be correlated to it, are not correlated to the original ticket because the ticket has been removed from Prime Network Vision.
- Flagging events that are ticketable open new tickets. The ticket's events are shown immediately in the Latest Events tab. The new tickets will be visible in Prime Network Vision two minutes after the flagging event was created (or up to seven minutes in rare cases).

To remove one or more tickets, select the required tickets in the ticket pane, and then right-click and choose **Remove**.

For more information, see Filtering Tickets by Network Element, page 9-6.

Clearing and Removing Tickets

Clearing and removing a ticket:

- Approves the reported faulty ticket.
- Clears the faulty networking entity from Prime Network Vision.
- Archives the ticket.

You can clear and remove multiple tickets at the same time. This operation will attempt to modify any ticket which is not being used by other processes, such as a ticket that is being updated with new network events. In order to clear and remove a highly active ticket, you should select only that ticket. That way, the system will wait until it becomes available for an update before removing it.

To clear and remove one or more tickets, select the required tickets in the ticket pane, and then right-click and choose **Clear and Remove**.

Note When Prime Network detects a large ticket (with more than 150 associated events), a system event is generated requesting the administrator to clear and remove the ticket. If this is not done within 15 minutes, the ticket will be automatically archived. A new ticket will be opened for any additional related incoming events.

Impact Analysis in Prime Network

Impact analysis enables you to identify the network elements and services that are impacted by a network fault or outage.

Prime Network offers two modes of impact analysis:

- Automatic impact analysis—When a fault occurs that has been identified as potentially service affecting, Prime Network 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—Prime Network provides what-if scenarios for determining the possible effect 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, Prime Network initiates an end-to-end flow that determines all the potentially affected edges.

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

Status Values for Affected Parties

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

- Potential—The service might be affected but its actual state is not yet known.
- Real—The service is affected.
- Recovered—The service has recovered. This state applies 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.

Initially, Prime Network might identify the services as either potentially or real affected. As time progresses and more information is accumulated from the network, Prime Network updates the information to indicate which of the potentially affected parties are real or recovered.

The indications for these states are available through both the API and in the GUI.

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

Accumulating Affected Parties

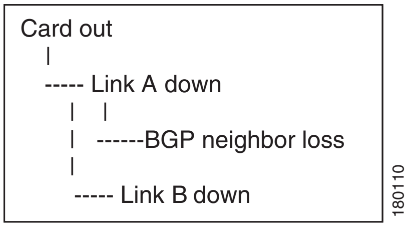
During automatic impact analysis, Prime Network automatically calculates the accumulation of affected parties. This information is embedded in the ticket along with all of the correlated faults.

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 9-4 Correlation Tree Example



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

Prime Network identifies the affected parties for each type of alarm and accumulates the following information:

- The affected parties reported on all the events in the alarm event sequence, including flapping alarms.
- The affected parties reported on the alarms that are correlated to it.

The gathered information includes the accumulation of the affected report of all the events in its own correlation tree.

For example, in Figure 9-4:

- BGP neighbor loss includes the affected parties of all events in its own event sequence.
- Link A Down includes the affected parties of its own event sequence and the accumulated information of the BGP Neighbor Loss event.

Accumulating the Affected Parties in an Alarm

If two events form part of the same event sequence in a specific alarm, the recurring affected pairs are displayed only once in the Affected Parties tab. If different affected severities are 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

If two or more alarms that are part of the same correlation tree report on the same affected pair of edgepoints and have different affected severities, the recurring affected pairs are displayed only once in the Affected Parties tab. If different affected severities are reported for the same pair, the pair is marked with the highest severity.

For example, assume that X and Y are the OIDs of edgepoints in the network, and a service is running between them. Both 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
- Potential—Priority 3

Card Out reports on X < > Y as real, affected only once.

Updating Affected Severity over Time

In some cases, Prime Network updates the affected severity of the same alarm over time because 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 available only in the link-down scenario in MPLS networks.