CHAPTER 5

Understanding Fault Management

These topics describe the key concepts of Cisco ANA fault management.

Note For details on configuring the registry parameters referred to throughout this guide, see Chapter 18, "Event and Alarm Configuration Parameters."

Introduction

A common problem in the management of large networks is that a single fault manifests itself as multiple alarms in the Network Management System (NMS). This makes manual analysis of faults costly and also diverts attention from major problems. This is a major motivation for applying analysis and correlation in an NMS.

There are many types of problems that threaten service delivery; for example, hardware failures, software failures, and so on. An effective root cause analysis technique must be capable of identifying all these problems automatically. This technique must work accurately for any environment and for any topology, including interrelated logical and physical topologies, with or without redundancy.

Cisco ANA is used for analyzing and managing faults using fault detection, identification and correlation. After a fault is identified, the system uses the auto-discovered virtual network model to perform fault inspection and correlation in order to determine the root cause of the fault.

Event Management

An event is a representation of a distinct incident occurring at a specific point in time. An event is a possible symptom of a *fault*. Examples of events include:

- Port status change
- Connectivity loss between routing protocol processes on peer routers (for example, BGP Neighbor Loss)
- Device reset
- Device becoming unreachable by the management station

Events and Alarms

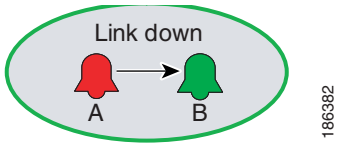
In Cisco ANA NetworkVision and EventVision, events are represented by a small icon in the form of a bell (see Figure 5-1).

Figure 5-1 Example Events

Events have an associated severity. Events with a severity of Critical (red), Major (orange), Minor (yellow), and Warning (sky blue) are said to be flagging events; events with a severity of Cleared (green) are called *clearing* events. Events that are *informational* in nature are marked in dark blue.

The lifecycle of a fault scenario is called an *alarm*. An alarm is characterized by a *sequence* of related events, such as a port down event followed by a port up event. In this guide, an alarm is denoted by an oval (see Figure 5-2).

Figure 5-2 Example of an Alarm



If event A is followed by event B as part of an event sequence, then event A is the *predecessor* of B, and B is A's *successor*.

The last event in the sequence determines the severity/state of the alarm. An alarm that ends with an event that has a severity of cleared is called a *cleared alarm*.

Event Discovery

Network Faults

The Cisco ANA fault management system learns about network faults via network event notifications:

- Incoming Network Event Notifications—SNMP traps and syslog event messages sent asynchronously by network elements are captured by Cisco ANA and processed by the appropriate VNE. Cisco ANA supports SNMP v1, v2 and v3.
- Generated Event Notifications—The VNE generates an event message when it detects a state change in the network element, typically after polling it via Telnet or SNMP. Some event notifications can also be generated by the gateway, such as the VPN Leak event.

  Cisco ANA can be set to generate a TCA notification when a certain device attribute condition is violated. For instance, Cisco ANA can be set to monitor CPU temperature and yield an event notification when it exceeds a certain value. For more information about TCAs, see the *Cisco Active Network Abstraction 3.6.6 Customization User Guide*.

  Generated event notifications are also referred to as *service alarms*.

Expedition

The Cisco ANA fault management system frequently *expedites* (triggers) the polling of specific data from the device, upon receipt of a trap or syslog event notification, or service alarm. Thus, these incoming notifications often yield additional generated event notifications (service alarms) that are key to the subsequent correlation process.

The list of traps and syslog notifications that cause polling expedition is device specific, and varies from VNE to VNE.

Internal Faults

In addition to network faults, the gateway and the units generate so-called system events, indicating Cisco ANA internal faults, such as disk full, unit unreachable, and so on.

Event Identification

After the fault management system becomes aware of a fault via an event notification, it processes the event notification message to identify the event, and creates an internal event object to represent the underlying event. At this stage, Cisco ANA determines the following information:

- Event Functionality Type—Trap event, syslog event, service alarm, and so on.
- Event Type—The event type is an identifier, describing the nature of the fault, such as Link Down.
- Event Subtype—The event subtype is a further clarification of the event type, such as Link Down Due to Admin Down.

  The Event Type and Event Subtype are internal fields that Cisco ANA uses for event processing. Cisco ANA does not externalize these fields.
- Event description strings, including the content of the notification message (for incoming event notifications), and a short description; this text is used to display the event to the operator.
- Event Severity—For more information, see Severity, page 5-4.

Based on the event type and event subtype, an event has numerous additional correlation and metadata attributes that determine how the event will be processed by Cisco ANA. These attributes are further discussed in Chapter 4, "Causality Correlation and Root Cause Analysis." These attributes are defined in the Cisco ANA registry, and are documented in:

- Chapter 16, "Supported Service Alarms"
- *Cisco Active Network Abstraction 3.6.6 VNE Reference Guide*.

Incoming Event Identification

Incoming event notifications (traps and syslogs) are identified by matching the event data to predefined patterns. A trap or syslog is considered supported by Cisco ANA if they have matching patterns and can be properly identified.

If the incoming event notification cannot be identified, Cisco ANA creates an event-object of a so-called *generic* type. Generic events are not used in subsequent correlation activity. When a generic event is generated, the raw data is populated in the long description field of the generic event.

The payload structure of a particular trap might differ between SNMP versions and a trap might be supported by Cisco ANA only for a specific SNMP version.

Each supported trap or syslog has a corresponding configuration in the registry that maps it to a specific event type and subtype. The identification process described previously builds the event object based on this configuration. In some cases, the mapping is based on the internal values of the event. For example, the Line Down trap is mapped to event type and subtype as described in Table 5-1.

Table 5-1 Line Down Trap

Trap Internal Value	Event Type	Event Subtype
Status=down	Line Down trap	Line Down trap
Status=up	Line Down trap	Line Up trap

Traps are mapped to event type and subtype regardless of the SNMP versions in use.

Event Dropping

Upon identification, the event type determines whether it will continue to be processed or dropped.

Events that are dropped at this stage are not stored in the Cisco ANA database, and do not participate in correlation. Dropping events at this stage is important in order to prevent Cisco ANA from being overwhelmed by large numbers of insignificant event notifications.

Severity

Each event has an assigned severity. Events broadly fall into three severity categories:

- Flagging—Indicative of a fault: Critical, Major, Minor, or Warning
- Clearing—Indicative of a fault that has been resolved: Cleared
- Informational—Info

For example, a Link Down event might be assigned critical severity, while its corresponding Link Up event will have a cleared severity.

The last event in the sequence determines the severity of an alarm (an event sequence). Exceptions to this rule include bookkeeping events (see Bookkeeping Events, page 5-10) that do not change the severity of the sequence (the alarm).

Event Source Association

Event identification is followed by *source association*. Cisco ANA examines and parses the event notification message in order to pinpoint the precise entity that is the location, or source, of the event. Rather than simply relate the event to the managed element as a whole, the association code determines the precise source of the event. The source corresponds to an object in the VNE model. The event is populated with the unique IMO identifier of that object (the OID).

See Chapter 17, "Source OIDs of Alarms Generated by Cisco ANA," for more details.

For instance, the source of a neighbor loss event would be the relevant IP interface of the managed element. Correctly associating an event to its closest source is an important step for the subsequent correlation actions.

Source Association Fallback

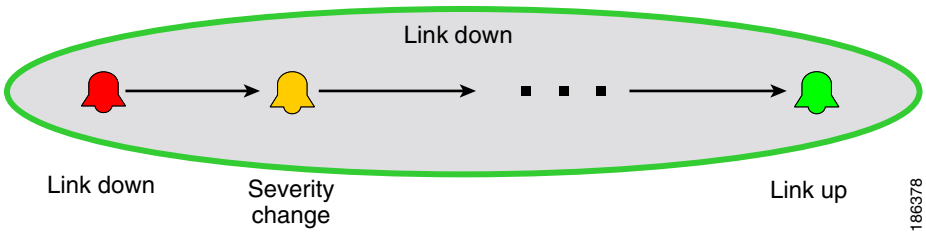
In some cases, the event source might not be in the internal VNE model at the time of the event notification. For instance, when a new module is inserted, it takes some time for Cisco ANA to poll all its interfaces and build up (populate) the model. If the new event notification is handled before the model is fully populated, the association logic might fail to find and retrieve the entity that is the correct source of the trap. A retry mechanism minimizes the occurrence of such a race condition, but if it persists, the association logic will fall back to the managed element entity (the network element) that is the source of the new event. An additional identifier (the *alarm differentiator*), representing the intended source, is later used in the correlation logic. See also alarm differentiator in Chapter 17, "Source OIDs of Alarms Generated by Cisco ANA."

Event Correlation and Alarms

Event correlation is the term used to describe the process of relating an event to other events. Cisco ANA distinguishes two types of relations between events:

- A sequence of events. Events that have the same type and the same source are considered part of an event sequence, or an alarm. An alarm represents the complete lifecycle of a fault (see Figure 5-3).

Figure 5-3 Event Sequence

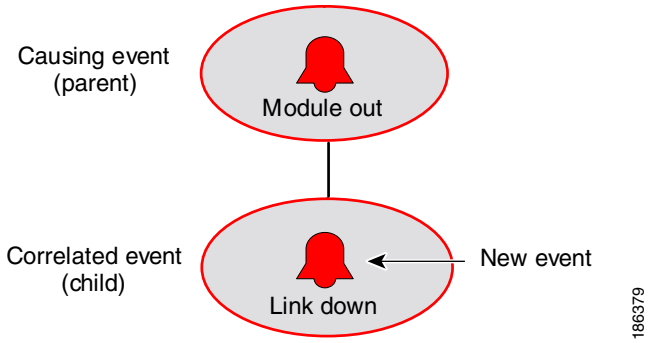


For more information, see Relating a New Event to an Event Sequence, page 5-6.

- A hierarchy of event sequences (alarms), representing *causality.*

  Causality correlation is the process of relating an event to an existing alarm in a causality relationship (see Figure 5-4).

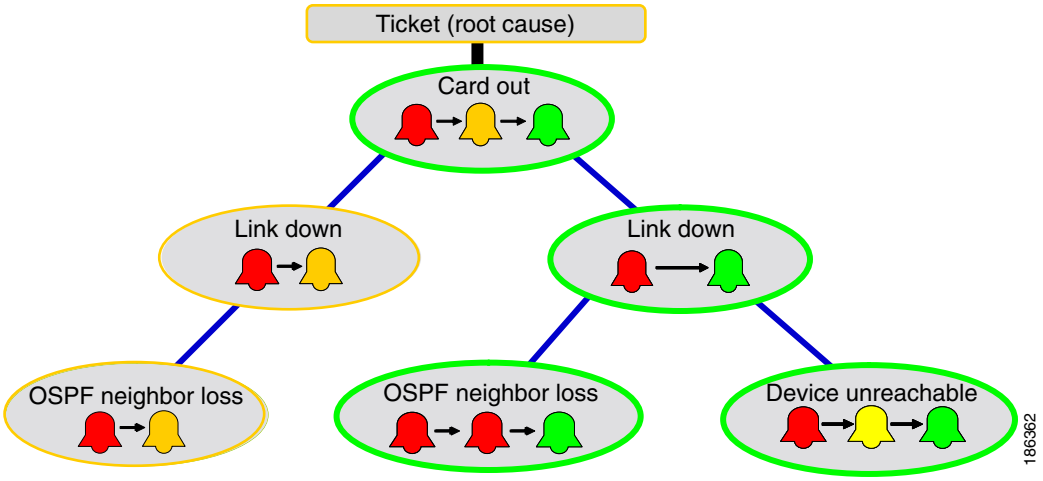
Figure 5-4 Causality Correlation



Causality correlation creates a hierarchy, and the top-most cause is called the *root cause*.

In Figure 5-5, the Link Down alarm is the cause for OSPF Neighbor Loss alarm, and Card Out is the cause for Link Down and the root cause for all the other alarms as well.

Figure 5-5 Root Cause Analysis



For more information about event correlation, see Chapter 4, "Causality Correlation and Root Cause Analysis."

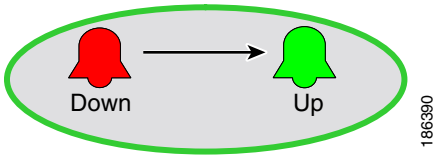
Relating a New Event to an Event Sequence

Cisco ANA associates a new event to an existing event if it identifies an existing event with the following criteria:

- The existing event has the same event type and source as the new event
- The existing event does not have a successor

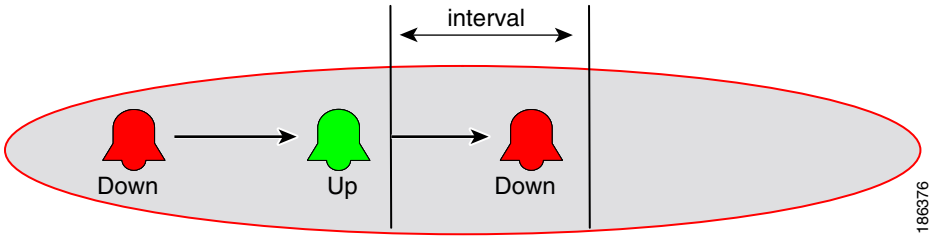
- The existing event is not archived
- One of the following two conditions:
  - The existing event's severity is not cleared. This is the normal case of an open alarm being updated, and is illustrated in Figure 5-6.

Figure 5-6 Updating an Alarm



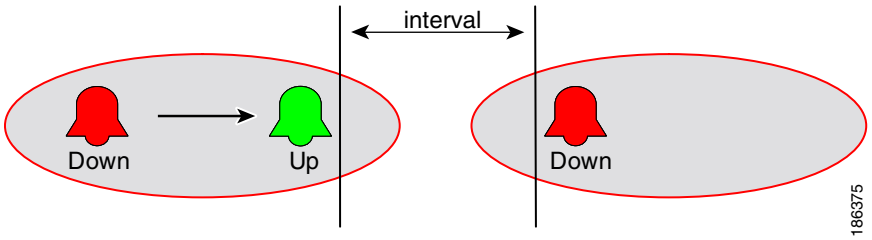
  - The existing event has *cleared* severity, and the new event arrives within a short time interval after the clearing event. The interval is configurable per event type using the gw-correlation-timeout parameter (default 20 minutes). Cisco ANA considers the new event to be an extension of the existing fault despite the fact that is was already cleared. This is illustrated in Figure 5-7.

Figure 5-7 Extending a Cleared Alarm



If the new event arrives later, cannot be associated, and is ticketable (see Ticketable Event, page 5-9), a new alarm will be created, as illustrated in Figure 5-8.

Figure 5-8 Creating New Alarm



Flapping Events

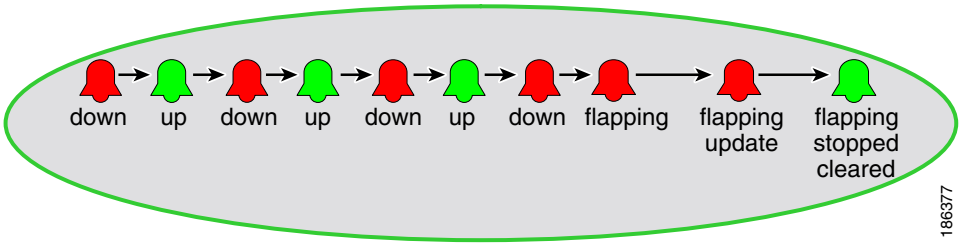
Flapping is the occurrence of a flood of consecutive event notifications (often severity toggling) related to the same alarm. This can happen when a fault is unstable and causes repeated event notifications, for instance, the use of a cable with a loosely-fitting, rattling connector. Cisco ANA recognizes this flapping phenomenon, and represents the new event notifications with a single generated event with a "flapping" subtype. The alarm is said to be flapping. When the fault stabilizes and the new event notification

frequency goes back to normal, the fault management logic terminates the alarm's flapping mode by generating a final event notification (either Flapping Stopped Cleared or Flapping Stopped Uncleared subtype), based on the state of the fault (the last received new event notification) at that time.

During flapping, the fault management logic will generate periodic event notifications with a Flapping Update subtype that also becomes part of the alarm's event sequence.

A flapping situation is illustrated in Figure 5-9:

Figure 5-9 Flapping Event



A sequence of events is identified as flagging if:

- All events share the same event type and are associated to the same source.
- The time interval between consecutive events is less than 1 minute (default value).
- There are more than five events (default value) with a severity different from Cleared.

The flapping detection code is configurable. The following parameters affect the behavior (default values in parentheses):

- flapping-threshold—The number of consecutive events that must be received at intervals shorter than the flapping interval, to be considered a flapping sequence (5).
- flapping-interval—The maximum time interval between consecutive event notifications that are part of a flapping sequence (1 minute).
- update-threshold—The number of events in an incoming flapping sequence that triggers the generation of a Flapping Update event notification (20).
- update-interval—If no Flapping Update event notification was sent during this time, one will be generated (about 3 minutes).
- clear-interval—The time that the alarm is not updated with new events, in order to exit the flapping mode (4 minutes).

Flapping detection is enabled for certain events and disabled for others.

Event Persistency

All events that are not dropped after the identification phase, and the relationship between these events, are stored in the system database. The content of the database can be reviewed using Cisco ANA EventVision.

Note Events are stored in the form of the Cisco ANA event object. The original notification structure of incoming event notifications (trap or syslog) is not maintained.

Archived Events

The stored events might be marked as *archived*. Archived events are persisted in the system database but can be presented to the operator only by using Cisco ANA EventVision.

An event is archived either because:

- The whole correlation hierarchy that it was part of was marked as archived (see Ticket Management Operations, page 5-9).
- The event was found not to relate to any other event, nor was it ticketable.

Tickets

An alarm represents a scenario which involves a fault in the network, the managed element or the management system. A *ticket* represents the complete hierarchy of correlated alarms representing a single specific fault scenario. Both Cisco ANA NetworkVision and Cisco ANA EventVision display tickets and allow drilling down to view the consequent alarm hierarchy.

From an operator's point of view, a fault is always represented by a complete ticket. Operations such as Acknowledge or Remove are always applied to the whole ticket.

A ticket points to the root cause alarm that is the top-most alarm in the correlation hierarchy. The attributes of the ticket (such as short description) are derived from the root cause alarm.

Ticketable Event

A *ticketable* event is an event that becomes a root cause for a new ticket in case it was not correlated to any other event.

An event is configured to be ticketable through the registry if the is-ticketable parameter for the event subtype is set to True.

Ticket Severity

Each ticket assumes the propagated severity of the alarm with the top-most severity, within all the alarms in the correlation hierarchy at any level.

A ticket is considered open as long as its severity is not cleared.

Ticket Management Operations

The following management operations might be applied to a ticket either manually or through the system (northbound) API:

- Acknowledge—Mark a ticket as acknowledged. It is used to distinguish between new faults and faults that are known or handled by the operation team.
- Remove—Set the ticket and all the events in the hierarchy as archived. An archived ticket is removed from the display in Cisco ANA NetworkVision.
- Clear—Set all uncleared alarms in the hierarchy to cleared severity.

Remove and Clear operations might be done automatically by the system. The mechanism used for these automatic processes is described in the following topics:

- Ticket Auto-Remove, page 5-10
- Ticket Auto-Clear, page 5-10

Bookkeeping Events

Cisco ANA also generates so-called bookkeeping events. When a ticket is archived or acknowledged, a bookkeeping event is generated for all alarms that are correlated to the ticket.

Ticket Auto-Remove

Cisco ANA implements a process to remove tickets automatically. The process launches periodically and scans through all unarchived tickets. It will remove a ticket automatically if all of the following conditions are met:

- The Ticket is Cleared, or its type value is Info.
- The time that has passed from the clearing of the ticket is greater than the gw-correlation-timeout parameter.
- The auto-remove parameter for the subtype of the first event in the sequence of the root cause alarm is set to True.
- The time that has passed from the last update to the ticket is greater than auto-remove-timeout which is by default set to 88 minutes. Any change to correlation hierarchy or to the sequence of one of the alarms in the correlation hierarchy is considered as an update to the ticket.

The default value for the time interval to trigger the auto-remove process is one minute.

Note After the ticket is archived, the events in its correlation hierarchy are no longer presented in Cisco ANA NetworkVision.

Cisco ANA implements an additional automatic process to maintain the number of concurrent open (noncleared) tickets below a predefined threshold. If the number of open tickets found is above the threshold the oldest tickets will be removed and archived. This automatic process is part of the integrity test. For more information, see the *Cisco Active Network Abstraction 3.6.6 Administrator Guide*. The default threshold number is 5000.

Ticket Auto-Clear

There are situations when the root cause alarm is cleared but there are still noncleared alarms in the correlation tree (hierarchy) of the ticket.

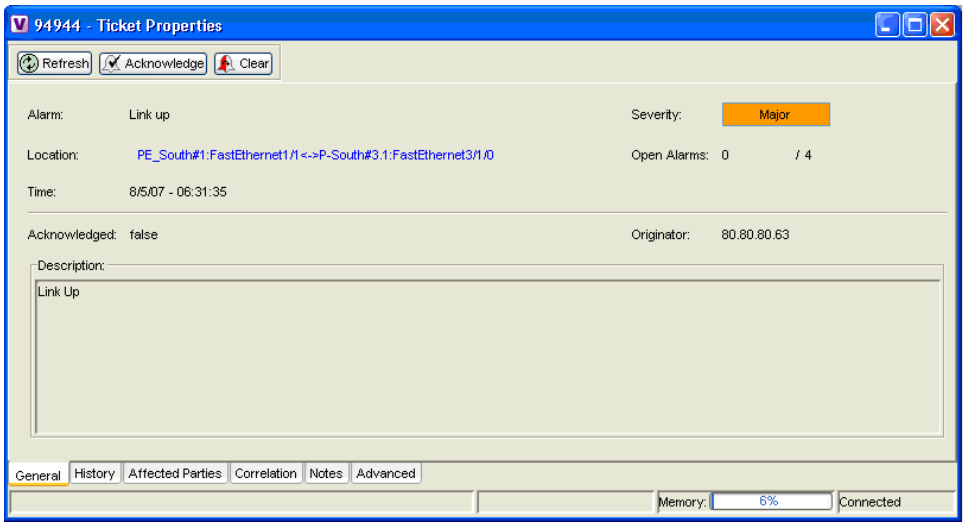
Noncleared alarms might exist in the correlation tree for one of the following reasons:

- The network event that caused the alarm creation has still not been fixed or the network event that caused the alarm creation was fixed, but the VNE has still not identified the change.
- The network event that caused the alarm creation was fixed. A clearing notification (trap or syslog) associated with this event was sent from the device but did not reach Cisco ANA, or was not identified correctly by Cisco ANA.

The situation described in the second scenario is undesirable; that is why Cisco ANA supports a feature called *auto-clearing* (the ticket is cleared automatically).

Figure 5-10 shows an example ticket of a Link Down alarm.

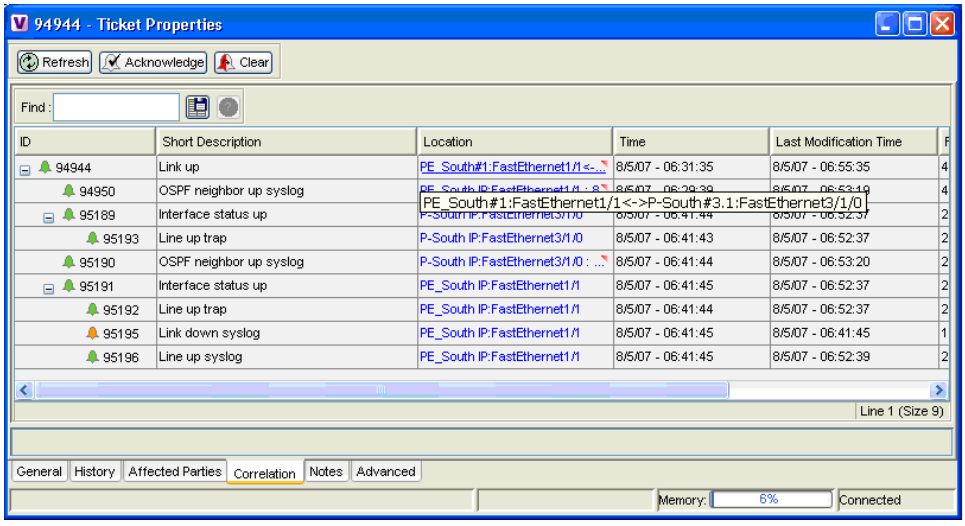
Figure 5-10 Ticket of a Link Down Alarm



In this example, the alarm has already been cleared (Link Up) while the severity of the ticket is still Major (Orange).

The reason for this situation is hidden in the correlation tree of the ticket (see Figure 5-11). The tree contains one Link Down syslog alarm that has not been cleared, because its clearing syslog event did not reach Cisco ANA.

Figure 5-11 Correlation Tree of the Link Down Ticket



The auto-clear mechanism handles such possibilities automatically. It is, of course, also possible to manually clear the ticket in Cisco ANA NetworkVision.

The auto-clear attribute is an attribute that is set per event, configured in Cisco ANA. It indicates whether or not this type of event can be auto-cleared by the auto-clear mechanism. This mechanism runs on the gateway every minute and iterates on all the tickets that are not archived. For any open ticket, the auto-clear mechanism checks if all its events are either cleared or have the auto-clear attribute set to True. In this case, the mechanism will auto-clear the ticket.

Note The auto-clear mechanism will not clear a ticket if the root cause event has not been cleared.

When an event is auto-cleared, the clearing event description displayed in Cisco ANA NetworkVision indicates this (for example, Auto Cleared - Link Down due to Admin Down).

In Cisco ANA, all syslogs and traps have the auto-clear attribute set to True, except the following:

- Syslogs and traps which are ticketable.
- A few important syslogs and traps that do not have a corresponding service alarm.

Note A device that suddenly loses power will not send a down event. It will send a coldstart trap when it subsequently recovers, and this trap will not auto-clear. There is no corresponding down event, and if the coldstart trap were auto-cleared, the important device-recovery notification would be lost.

Syslog and trap events like this must be cleared manually, using Cisco ANA NetworkVision.

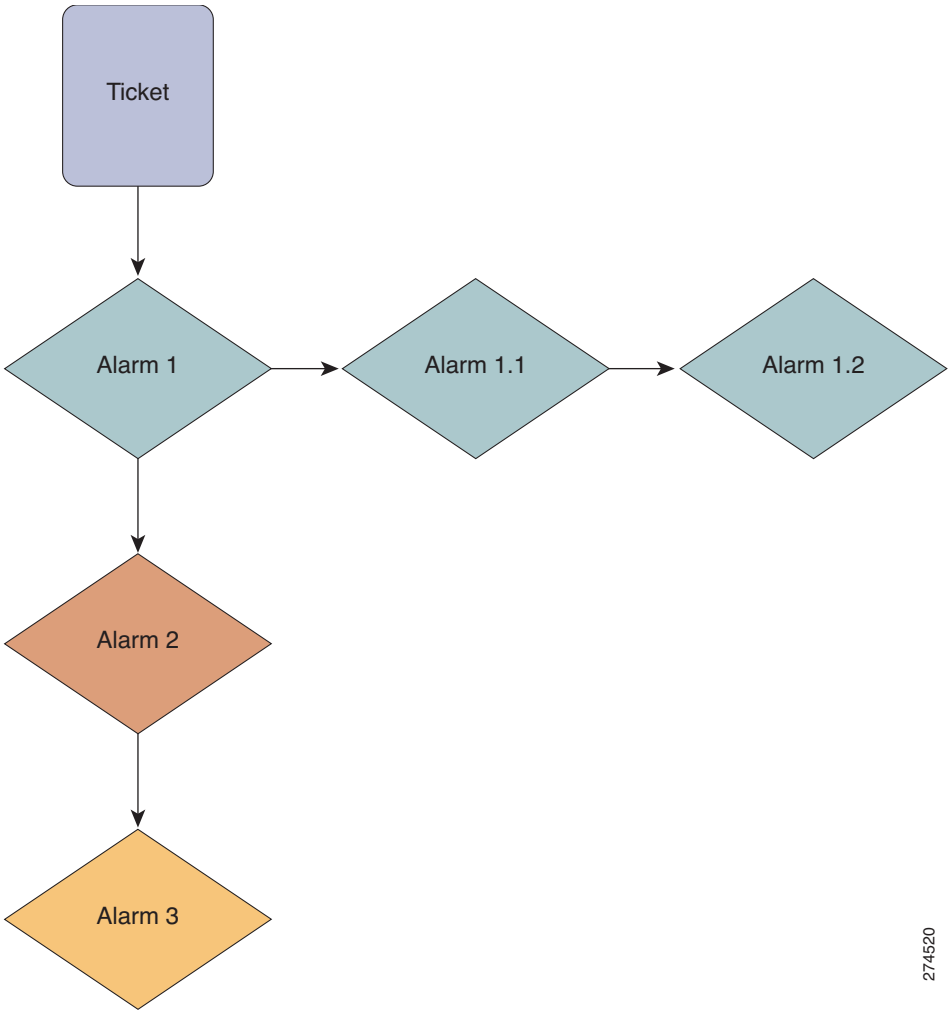
The process that checks periodically for open tickets is the same one used for auto-remove. Therefore, both operations share the same time interval, which is one minute by default.

Alarm Deduplication

By default, Cisco ANA is able to avoid creating duplicate tickets by identifying and appropriately linking duplicate alarms to existing alarms within previously generated tickets.

Figure 5-12 shows a generic example. Alarm 1 is the top-most, or root, alarm for the ticket. Alarms 2 and 3 are both part of the correlation tree, derived from Alarm 1. Two duplicate alarms, Alarm 1.1 and Alarm 1.2, have arrived and Cisco ANA has assigned them as successors to Alarm 1.

Figure 5-12 Duplicate Alarms in a Ticket Correlation Tree



Cisco ANA uses the predecessor/successor concept to handle incoming duplicates properly, without either discarding them or creating new tickets for them. In this example, Alarm 1 is the predecessor of Alarm 1.1, and Alarm 1.1 is the successor of Alarm 1. Similarly, Alarm 1.1 is the predecessor of Alarm 1.2, and Alarm 1.2 is the successor of Alarm 1.1.

Whenever an alarm arrives, Cisco ANA searches among its stored alarms for a possible predecessor. In our example, when Alarm 1.1 comes in, Cisco ANA quickly identifies Alarms 1, 2, and 3 as possible predecessors, then identifies the correct predecessor by matching it against the incoming alarm according to these rules:

1. The predecessor and successor both come from the same OID.
2. The predecessor and successor have the same alarm types.
3. The predecessor has not been archived. As explained in Ticket Auto-Clear, page 5-10, tickets with their auto-clear attribute set to True and a cleared alarm associated with the root cause are archived automatically. If any alarm within the ticket has auto-clear attribute set to False, the ticket is not archived. It can receive duplicate alarms until the user clears it manually.
4. The predecessor is not an indeterminate, info, or cleared alarm.
5. The predecessor's correlation timeout period has not elapsed.
6. The predecessor currently has no successor.

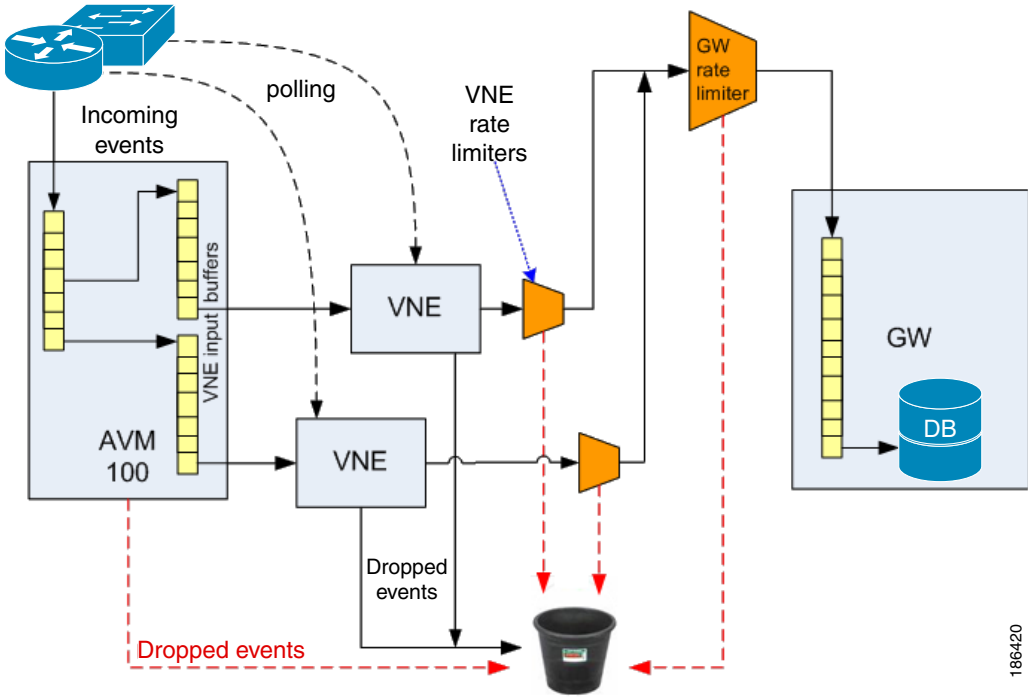
If all these conditions are met, then the incoming alarm is assigned to that predecessor, as shown in the example. The predecessor alarm also sets its successor to the new alarm. Later duplicates (like Alarm 1.2) become successors to the new alarm under the same processing rules.

Database Size Maintenance

To prevent overflow in the database, Cisco ANA implements an automatic process that deletes old data. There is a configurable setting of the period of time—the event history size attribute—for which events should be maintained. The oldest time for which events should be maintained is the current time minus the event history size. Any event before this time will be deleted. The automatic process is part of the integrity test (see the *Cisco Active Network Abstraction 3.6.6 Administrator Guide*) and is activated periodically.

Event Flow Through Cisco ANA

Figure 5-13 Event Flow Through Cisco ANA



Incoming event notifications (traps, syslogs) are received by an internal event listener process, also known as an AVM 100. The event listener stores the notifications in a VNE input buffer that corresponds to the Network Element from where the event notification came. The event notifications are then sent to the VNE at a fixed rate.

When a VNE input buffer in AVM 100 fills up, further events from this NE are dropped. This capability protects Cisco ANA from event storms or DOS attacks.

As discussed earlier, the VNE parses, identifies and processes the received notifications, drops flapping and other unimportant events, expedites certain polling operations, attempts to correlate (see Chapter 4, "Causality Correlation and Root Cause Analysis"), and sends the incoming and generated events to the gateway.

Event rate limiters prioritize the behavior of Cisco ANA during major outages and under heavy peak and flooding conditions. Each VNE has its own outgoing rate limiter; another rate limiter acts on the aggregate flow of events from all the VNEs coming into the gateway. See Figure 5-13.

The event rate limiters are configured for multiple commit and burst rates and durations per event type, based on priority and overall aggregate rates. Events that exceed the burst rates are dropped, and a special generated event is sent to the gateway, to inform the operator of this situation.

The gateway stores the events it receives in the database, performs final alarm association and ticket management, and notifies the northbound interface and Cisco ANA clients of the event.

Every minute, the gateway reviews all the tickets and looks for tickets to clear. The gateway clears a ticket if all its events are either cleared or have the auto-clear attribute. In addition, the gateway checks for tickets to archive (auto-remove). The archive timeout of a ticket is determined by the archive timeout attribute of the root cause event.

The actual event rates and optimal configurations of the flow processing path are highly dependent on the network topology and deployed networking technologies and configurations, the number of network elements under management, the frequency of fault incidents, and many other factors. Exhaustive testing is required before changing default values.