Fault Management in Cisco ANA

Cisco ANA analyzes and manages faults through event collection, identification, and correlation. After identifying the event, Cisco ANA groups the events related to it, then uses the virtual network model to inspect the fault and perform correlation to find the root cause and create a ticket. The following topics describe key Cisco ANA fault management concepts:

- Event Management, page 3-1
- Correlation and Root Cause Analysis, page 3-4
- Ticket Management, page 3-11
- Event Flow Through Cisco ANA, page 3-19
- Northbound Integration Services, page 3-23
- Event Reporting, page 3-23
- Database Management, page 3-24

Event Management

An event is a distinct incident that occurs at a specific point in time. Examples of events include:

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

An event is a possible symptom of a fault, which is an error, failure, or exceptional condition in the network.
Events and Alarms

In Cisco ANA NetworkVision and Cisco ANA EventVision, an event is represented by a small icon in the form of a bell (see Figure 3-1).

**Figure 3-1 Example Events**

![Link down](186381) ![Link up](186382)

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 port-down and port-up. In this guide, an alarm is denoted by an oval (see Figure 3-2).

**Figure 3-2 Alarm Example**

![Link down](186380)

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 and state of the alarm. An alarm that ends with an event that has a severity of cleared is called a cleared alarm.

Event Discovery

Cisco ANA discovers events by:

- Receiving and analyzing notification events.
- Automatically polling devices and discovering changes that cause service alarms.

Events can pertain to network faults or network elements, including incoming network and generated event notifications:

- Incoming network event notifications—Cisco ANA captures the asynchronous SNMP traps and syslog notifications and sends them to the appropriate VNE for processing. Cisco ANA supports SNMP v1, v2, and v3 traps.
- Generated event notifications—After a VNE detects a network element state change, typically after polling it through Telnet or SNMP, the VNE generates an event message. Some event notifications, such as the VPN Leak event, can also be generated by the gateway.

After receiving an event notification or service alarm, Cisco ANA frequently expedites (immediately triggers) the polling of specific data from the device. The polling often yields additional generated event notifications or service alarms that are key to the subsequent correlation process. The list of traps and syslog notifications that cause polling expeditions is device specific, and varies from VNE to VNE. In addition to network faults, the gateway and units can generate system events that indicate Cisco ANA internal faults, such as disk full or unit unreachable.
Event Identification

The event manager parses the event notification message to get more information about the event and creates an internal event object to represent the underlying event. During event identification, Cisco ANA obtains 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 fault, such as Link Down.
- Event Subtype—The event subtype further clarifies the event type, such as Link Down Due to Admin Down.
- Event description strings—Includes the notification message content (for incoming event notifications) and a short description; this text is used to display the event to the operator.
- Event Severity—See Event Severity, page 3-4.

An event can have many additional correlation and metadata attributes that determine how Cisco ANA processes the event. These attributes are discussed in Chapter 4, “Correlation Scenarios,” and also the Cisco Active Network Abstraction 3.7.2 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 it has matching patterns and can be properly identified.

If the incoming event notification cannot be identified, Cisco ANA creates a nonactionable event-object type. Nonactionable events are not used in subsequent correlation activity. Instead, Cisco ANA preserves the trap OID and forwards it through the event notification service for both nonactionable and known event types.

Note

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.

Event identification is sometimes based on the internal event values. For example, the Line Down trap is mapped to event type and subtype as shown in Table 3-1. Traps are mapped to event type and subtype regardless of the SNMP version in use.

<table>
<thead>
<tr>
<th>Trap Internal Value</th>
<th>Event Type</th>
<th>Event Subtype</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status=down</td>
<td>Line Down trap</td>
<td>Line Down trap</td>
</tr>
<tr>
<td>Status=up</td>
<td>Line Down trap</td>
<td>Line Up trap</td>
</tr>
</tbody>
</table>

Event Dropping

The event type determines whether the event continues to be processed or is dropped. Events that are dropped are not stored in the Fault Database and do not participate in correlation. Dropping events is important because it prevents Cisco ANA from being overwhelmed by large numbers of insignificant event notifications.
Event Severity

Each event has an assigned severity. Events broadly fall into three broad severity categories, each with an associated Cisco ANA EventVision and Cisco ANA NetworkVision display color:

- **Flagging**—Indicates a fault: Critical (red), Major (orange), Minor (yellow), or Warning (sky blue).
- **Clearing**—Indicates a fault that is resolved: Cleared (green).
- **Informational**—Information only (dark blue).

For example, a Link Down event might receive a critical severity, while its corresponding Link Up event receives 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 3-14), which do not change the severity of the sequence (the alarm).

Event Source Association

Event identification is followed by *source association*. Cisco ANA examines the event notification message to pinpoint the precise entity that is the location, or source, of the event. The association code identifies the precise event source, which corresponds to a VNE model object. The event is populated with the unique IMO identifier (the OID). For example, the source of an Ethernet flow point (EFP) Down event is the corresponding EFP model object. Correctly associating an event to its closest source is important for the subsequent correlation actions.

Source Association Fallback

In some cases, the event source is not in the internal VNE model when the event notification occurs. For example, after a new device module is installed, it takes 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 not find and retrieve the entity that is the correct source of the trap. A retry mechanism minimizes the occurrence of such a rare condition, but if it persists, the association logic falls 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. For more information about alarm source OIDs, see the *Cisco Active Network Abstraction 3.7.2 Reference Guide*.

Correlation and Root Cause Analysis

Causality correlation is the process of relating an event to an existing alarm in a causality relationship. The root of the resulting causality hierarchy is called the *root cause*, and the correlation process that determines the fault’s root cause is referred to as *root cause analysis* (RCA).

RCA is performed on historic snapshots of the VNE model and forwarding information. These snapshots, maintained for ten minutes, enable the correlation logic to traverse the VNE network model at a time in the past, before the occurrence of the fault being analyzed. This is critical for root cause analysis in the presence of network faults. The Cisco ANA correlation capability comes from the ability to learn the suspected fault impact by examining network snapshots before the fault occurred.
Network and Local Correlation

Cisco ANA supports both network and local correlation event RCAs:

- **Network correlation**—Network correlation associates events according to network logic. This logic correlates an event that occurred on a specific VNE component to an event that occurred on another component on the same VNE, or a component on a different VNE. The correlation is based on a flow that runs across the distributed network element model and their topology. Network correlation is most successful if the event holds forwarding information, such as the IP address of a Border Gateway Protocol (BGP) neighbor, or a Frame Relay virtual connection. A root cause is identified among the group of correlated alarms.

- **Local correlation**—Local correlation is used for events that occur on the same VNE. In this model, events are correlated according to event weight. Each parent event can have multiple child events, and each event can have a different weight. Local correlation is tried first with the event having the highest associated weight.

- **Local special correlation**—Local special correlation is used for events that occur on the same VNE, such as link down to card out, or link down to device unreachable.

After correlation and RCA, the event is considered an enriched event. For more information about correlation and root cause analysis, see Chapter 4, “Correlation Scenarios.”

Event Correlation and Alarms

Event correlation is the process of relating one event to other events. Cisco ANA distinguishes two event relationship types:

- **An event sequence.** 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 3-3). For more information, see New Event Associations, page 3-6.

- **An event sequence hierarchy (alarms), representing causality.** Causality correlation is the process of relating an event to an existing alarm in a causality relationship (see Figure 3-4).
Causality correlation creates a hierarchy, and the top-most cause is called the root cause. In Figure 3-5, 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. For more information about event correlation, see Chapter 4, “Correlation Scenarios.”

**New Event Associations**

Cisco ANA associates a new event to an existing event if the existing event:

- Has the same event type and source as the new event.
- Does not have a successor.
- Is not archived.

The event is associated to the alarm as long as the ticket is active.
Flapping Events

Flapping is a flood of consecutive event notifications (often severity toggling) related to the same alarm. Flapping can occur when a fault is unstable and causes repeated event notifications; for example, the use of a cable with a loosely-fitting connector. Cisco ANA recognizes flapping and represents the new event notifications with a single generated event with a flapping subtype. The alarm is said to be flapping. After the fault stabilizes and the new event notification frequency returns 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 generates 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 3-6.

Figure 3-6 Flapping Event

A sequence of events is identified as flapping if:

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

Flapping detection is enabled for certain events and disabled for others. For information about customizing fault behavior, see the Cisco Active Network Abstraction 3.7.2 Customization User Guide.

Event Persistence

Correlated events that are not dropped after the identification phase are stored in the Cisco ANA Fault Database. The relationships between the events are also retained. 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.
Archive Events

The stored events might be marked as archived. Archived events are stored in the Fault Database (in an archive partition) and can be viewed by using Cisco ANA EventVision. An event is archived if either of the following is true:

- The ticket to which the event belongs is marked as archived, which means all its alarms and events are marked as archived (see Ticket Management Operations, page 3-14).
- Cisco ANA receives an event that does not correlate to any other event and is not ticketable. When this occurs, Cisco ANA immediately marks the event as archived.

Event Correlation Attributes

Table 3-2 describes the Cisco ANA event correlation attributes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correlation</td>
<td>Determines whether the event should be correlated and the root cause identified.</td>
</tr>
<tr>
<td>Activate Flow</td>
<td>Determines if the new event should initiate a network or a local correlation process.</td>
</tr>
<tr>
<td>Forwarding Information</td>
<td>Identifies event-specific flow information, for example the BGP neighbor IP address used in network correlation. Forwarding information includes:</td>
</tr>
<tr>
<td></td>
<td>- The component that started the correlation flow. This might be the VNE component that identified the event, for example, an IP interface component in an Interface Status Down event, or any other VNE component.</td>
</tr>
<tr>
<td></td>
<td>- Additional forwarding data used by the flow logic, including the flow direction and one of the following:</td>
</tr>
<tr>
<td></td>
<td>- The IP address used as the flow destination IP address.</td>
</tr>
<tr>
<td></td>
<td>- The virtual connection used as the flow entry point.</td>
</tr>
<tr>
<td></td>
<td>- The MPLS label used as the label entry point switched path (LSP).</td>
</tr>
<tr>
<td></td>
<td>- The destination VNE component.</td>
</tr>
<tr>
<td>Correlation Keys</td>
<td>Identifies one or more unique identifiers that are usually derived from the event type, source, and event message content parameters used in local and flow correlations.</td>
</tr>
<tr>
<td>Correlation Allowed</td>
<td>Identifies whether the event can be the possible cause for other events. If so, other alarms can be correlated to it. An event configured to allow correlation should also be ticketable.</td>
</tr>
<tr>
<td>Weight</td>
<td>The relative weight of an event as a cause candidate in relation to other causing events. A new event can only correlate to an event that has a higher weight. The heavier the event, the more likely it is to be chosen as the cause.</td>
</tr>
</tbody>
</table>
Correlation Process

Figure 3-7 illustrates the Cisco ANA correlation process.

Figure 3-7  Correlation Process in Cisco ANA
The correlation process starts after a VNE receives a new event notification (see Event Identification, page 3-3). The correlation steps, shown in Figure 3-7, include:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Event identification is the first step. After the trap is identified and not dropped by the VNE, its attributes are identified.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the VNE is in maintenance state, the VNE does not expedite events but does respond to flows.</td>
</tr>
<tr>
<td>B</td>
<td>Cisco ANA examines and parses the event notification message to identify the event location entity or source. For more information on event source association, see Event Source Association, page 3-4.</td>
</tr>
<tr>
<td>C</td>
<td>Cisco ANA examines the new event for flapping. If the event is part of a flapping sequence, it is suppressed as described in Flapping Events, page 3-7.</td>
</tr>
<tr>
<td>D</td>
<td>Cisco ANA examines the new event. If the event is configured for correlation, it is subject to correlation. Most flapping events are subject to correlation; clearing events are not. If the event was configured to expedite polling, the specific polling command is generated as well, which might result in additional generated events. If the event is not configured for correlation, Cisco ANA tries to relate the event to an event sequence. See Step J to Step M for additional details.</td>
</tr>
<tr>
<td>E</td>
<td>The correlation process is suspended for two minutes to give other related events a chance to be detected. No further processing is performed on the event while it is suspended. As a result, updates to the Fault Database and Cisco ANA NetworkVision for this event are delayed by two minutes.</td>
</tr>
<tr>
<td>F</td>
<td>After the two-minute suspension, other events are examined as possible causes. Two different processes can be followed: local correlation (Step G) or network correlation (Step H), depending on the event configuration.</td>
</tr>
<tr>
<td>G</td>
<td>Local correlation finds and examines other events related to the same (local) NE from which the new event originated; no network flow is initiated. Local correlation is well suited for the following scenarios:</td>
</tr>
<tr>
<td></td>
<td>• A new event (such as a Module Out event) is in the device scope.</td>
</tr>
<tr>
<td></td>
<td>• The new event has a corresponding generated event message in Cisco ANA. It is desirable for the event to correlate to its generated event message. For example, a Link Down syslog event tries to correlate to a local Link Down or Port Down generated event message.</td>
</tr>
<tr>
<td></td>
<td>• The new event does not contain information that can be used to perform correlation beyond the scope of the local device. Such information is used to initiate the correlation flow.</td>
</tr>
<tr>
<td></td>
<td>Most trap and syslog events use the local correlation process. The correlation logic looks for causing events in the VNE that:</td>
</tr>
<tr>
<td></td>
<td>• Are configured to allow correlation.</td>
</tr>
<tr>
<td></td>
<td>• Arrived within the 7 minutes before the event or the 2 minutes after the event.</td>
</tr>
<tr>
<td></td>
<td>• Have a correlation key that matches at least one of the correlation keys of the new event.</td>
</tr>
</tbody>
</table>
Ticket Management

Ticket management refers to the process of managing the ticket life cycle, including:

- Creating tickets
- Associating events and alarms to tickets
- Acknowledging tickets
- Archiving tickets
Ticket creation is distributed among the units. When a ticket needs to be created, it is created in the unit that generated it by the Fault Agent running in that unit. Events and alarms are associated with tickets by polling the Fault Database and associating enriched events with the tickets and alarms.

Ticket management includes both automatic and manual operations involved in managing the ticket and alarm life cycle. Automatic operations include associating an event with a ticket and alarm, updating the aggregated ticket state (such as severity and event counter), and automatic archiving. Manual operations include acknowledging a ticket, clearing a ticket, and other operations. The automatic operations are orchestrated by the ticket agent in the gateway.

For information about automatic operations, see Automatic Operations, page 3-13. For information about manual operations, see Ticket Management Operations, page 3-14.

**Tickets**

An alarm represents a scenario that involves a fault in the network, a managed element, or the management system. A ticket represents an attention-worthy root alarm whose type is marked as ticketable. A ticket has the same type as the root alarm it represents, and it has a status, which represents the entire correlation tree.

A ticketable event is an event that becomes a root cause for a new ticket if the new ticket is not correlated to any other event. Events are configured to be ticketable or not ticketable. For more information, see Ticket-Related Configuration Options, page 3-14.

Tickets include the following elements and properties:

- 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 when its severity is not cleared.
- Both Cisco ANA NetworkVision and Cisco ANA EventVision display tickets and allow users to drill 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.

**User Roles and Tickets**

The following conditions apply when users work with tickets in Cisco ANA NetworkVision:

- If an element that is outside of a user’s scope is the root cause of a ticket that affects an element in the user’s scope, the user can view the ticket in Cisco ANA NetworkVision, but cannot:
  - View inventory by clicking the Location hyperlink.
  - Acknowledge, clear, remove, or clear and remove the ticket.
- Users can acknowledge, clear, remove, clear and remove, or add notes for a ticket only if they have OperatorPlus or higher permission for the element that holds the root alarm for that ticket.
The following options are available depending on the ticket source location and user scopes:

- If the source of the ticket or contained sources is not in the user’s scope, they cannot view the ticket in the ticket table, view ticket properties, filter tickets, or perform actions on the ticket. Actions include acknowledging, clearing, removing, and clearing and removing tickets.
- If the ticket contains a source that is in the user’s scope, but the source is not the root cause, the user can view the ticket in the ticket table and view ticket properties, but cannot perform actions on the ticket.
- If the source of the ticket is in the user’s scope, the user can view the ticket in the ticket table, view ticket properties, filter tickets, and perform actions on the ticket.

For more information about the available Cisco ANA user ticket actions, see the *Cisco Active Network Abstraction 3.7.2 User Guide*.

**Automatic Operations**

In ticket management, automatic operations include finding the ticket to which an event belongs, finding the alarm to which the event belongs, and updating both. Alarms define a sequence of events in a ticket. After the ticket is found, the alarm is immediately updated. Each event originating in the network is associated with a ticket. Only events marked attention worthy, or ticketable, are visible to Cisco ANA NetworkVision. All alarms and tickets can be viewed in Cisco ANA EventVision.

**Associating Events, Tickets, and Alarms**

The main Cisco ANA ticket management component queries the Fault Database and retrieves events that can be connected to the ticket. Events that can be connected to a ticket are those events whose ticket ID is not known yet, but the ticket ID of the preceding event is known. The component continually executes this query to retrieve events that are not yet connected to a ticket or alarm. The following actions are taken for each event that is selected by the query:

1. The alarm whose source and name match those of the event (within the ticket) is updated for severity, state, and counter.
2. The ticket is updated for severity, last modification time, and counter.
3. The event is associated with the alarm and the ticket.

No events are lost in this process. As long as events are kept with their correlation information and the preceding event ID, they are associated with a ticket.

**Clearing Tickets**

Every minute, Cisco ANA reviews all the tickets and looks for tickets to clear. Cisco ANA clears a ticket if all of its events either are cleared or are configured for automatic clearing. In addition, Cisco ANA checks for tickets to archive. The archive timeout of a ticket is determined by the archive timeout setting of the root cause event.
Auto-Archiving Tickets

Auto-archiving is a ticket management component that periodically checks for tickets that are candidates for archiving. Archiving moves the ticket to an archive partition in the Fault Database. A ticket is a candidate for archiving if:

- All of its events are clear or auto-clear.
- The configured length of time has elapsed after the last event joined it.

Auto-archiving interacts only with the Fault Database. Archiving a ticket marks its events and alarms as archived. They are not permanently deleted from the Fault Database. Events are kept in the Fault Database for 14 days.

Ticket Management Operations

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

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

Remove and Clear operations might be done automatically. For more information, see the following topics:

- **Ticket Auto-Remove**, page 3-15
- **Ticket Auto-Clear**, page 3-15

For more information about integrating with northbound applications, see the *Cisco Active Network Abstraction Integration Developer Guide*.

Bookkeeping Events

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

Ticket-Related Configuration Options

You can configure the following ticket management options:

- Whether or not the alarm is to be treated as attention-worthy. If yes, it is treated as a ticket. If not, it is treated as an alarm and is not promoted to a ticket.
- The amount of time that must elapse from the time the ticket is cleared until it can be archived.
- Automatic clearing of alarms if they are not cleared by the network.

For more information about customizing fault behavior, see the *Cisco Active Network Abstraction 3.7.2 Customization User Guide*.
Ticket Auto-Remove

Cisco ANA uses the auto-remove process to remove tickets automatically. Auto-remove launches periodically and scans all unarchived tickets. It removes a ticket automatically if all of the following conditions are met:

- The ticket is cleared, or its type is Info.
- The time that has passed from the clearing of the ticket is greater than that configured for correlation.
- The subtype of the first event in the sequence of the root cause alarm is configured for automatic removal.
- The time that has passed from the last update to the ticket is greater than the time for automatically removing the ticket. 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 are removed and archived.

For more information about customizing fault behavior, see the Cisco Active Network Abstraction 3.7.2 Customization User Guide.

Ticket Auto-Clear

Situation can occur in which the root cause alarm is cleared, but alarms that are not cleared remain in the ticket correlation tree. Noncleared alarms might exist in the correlation tree for one of the following reasons:

- The network event that caused the alarm creation is not fixed, or the network event that caused the alarm creation was fixed, but the VNE has not identified the change.
- The network event that caused the alarm creation is 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. If this occurs, Cisco ANA enables you to configure automatic clearing of alarms to clear alarms when scenarios like this occur.

Figure 3-8 shows an example ticket of a Link Down alarm. In this example, the alarm is Critical. Ticket information includes the ticket ID, description, which indicates the device is reachable, location, whether the ticket is acknowledged, severity, time, and number of open alarms. Additional ticket information can be obtained from the tabs at the bottom.
The ticket correlation tree (see Figure 3-9) displays additional ticket information. In this example, the Layer 2 tunnel and LDP neighbor are up. The problem is isolated to the p2 to p3 link.
Cisco ANA can be configured to clear alarms automatically, or they can be manually cleared in Cisco ANA NetworkVision. Automatic clearing can be configured for each Cisco ANA event type. Auto-clear runs every minute and goes through all tickets that are not archived. For each open ticket, auto-clear determines if all of its events are cleared or are configured for automatic clearing. If either of these criteria are true, auto-clear automatically clears the ticket.

**Note**

Auto-clear does not clear a ticket if the root cause event is not cleared.

Events cleared automatically are displayed in the Cisco ANA NetworkVision clearing event description, for example, Auto Cleared - Link Down due to Admin Down. In Cisco ANA, all syslogs and traps are configured to clear automatically, except:

- Syslogs and traps that are ticketable.
- A few important syslogs and traps that do not have a corresponding service alarm. For example, a device that suddenly loses power does not send a Down event. Instead, it sends a cold start trap when it subsequently recovers, and this trap is not cleared automatically because no corresponding Down event exists, if the cold start trap were automatically cleared, the device-recovery notification would be lost.

Syslog and trap events not cleared automatically must be cleared manually in Cisco ANA NetworkVision.

The process that checks periodically for open tickets also automatically removes tickets. Both operations share the same time interval, which is one minute by default.

### Duplicate Alarm Processing

By default, Cisco ANA avoids duplicate tickets by identifying and appropriately linking duplicate alarms to existing alarms within previously generated tickets. **Figure 3-10** shows an 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, arrive, and Cisco ANA assigns them as successors to Alarm 1.
Cisco ANA uses the predecessor/successor relationship to properly handle incoming duplicates without either discarding them or creating new tickets. 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.

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

- The predecessor and successor both come from the same OID.
- The predecessor and successor have the same alarm type.
- The predecessor is not archived. As explained in Ticket Auto-Clear, page 3-15, tickets that are configured for automatic clearing and a cleared alarm associated with the root cause are archived automatically. If any alarm within the ticket is not configured for automatic clearing, the ticket is not archived. Instead, it can receive duplicate alarms until the operator clears it manually.

If all of these conditions are met, the incoming alarm is assigned to that predecessor, as shown in the Figure 3-10 example. The predecessor alarm also sets its successor to the new alarm. Later duplicates (such as Alarm 1.2) become successors to the new alarm under the same processing rules.

![Figure 3-10 Duplicate Alarms in a Ticket Correlation Tree](image-url)
Event Flow Through Cisco ANA

Figure 3-11 illustrates the logical flow of events through Cisco ANA. (The actual network communication is subject to the transport configuration between the gateway server and units.)

**Figure 3-11   Logical Event Flow Through Cisco ANA**

Events flow through Cisco ANA as follows:

1. Devices forward notifications to a Cisco ANA unit, where it is received by the Cisco ANA Event Collector (AEC), which runs on AVM 100. The AEC parses incoming events to identify basic event information.

2. The AEC stores each incoming raw event in the Event Archive.

3. The AEC distributes each incoming raw event to the corresponding VNE.

4. The VNE:
   - Defines the application type to use for the event type.
   - Extracts additional information from the raw event.
   - Passes the event to the Fault Agent, which runs on AVM 25.
   - Correlates associated events.

Note: Cisco ANA uses the CISCO-EPN-MIB-NOTIFICATION-MIB trap format to encapsulate the original trap. It does not use SNMP proxy function.
– Performs root cause analysis (RCA) on the event.
– Sends updated correlation and RCA information to the Fault Agent.

5. The Fault Agent:
– Sends events to the Fault Database.
– Creates tickets, as appropriate.

6. Cisco ANA forwards all event notifications for actionable events and tickets to the gateway.

7. The gateway forwards the information shown in Figure 3-11 to external OSS applications, using either BQL or SNMP.

8. Event information is available on demand to users in standard or user-defined formats in the GUI clients.

9. Events older than three months are removed from the Event Archive and the Fault Database.

The actual flow processing path event rates and optimal configurations depend on many factors, including:

- Network topology
- Deployed networking technologies and configurations
- Number of network elements under management
- Frequency of fault incidents

Thorough testing is required before you change the default values. For more information about AEC and the different supported configurations, see the Cisco Active Network Abstraction 3.7.2 Administrator Guide.

Event Reduction

Cisco ANA event reduction plays a key role in providing operators with a set of correlated, actionable tickets. The AEC collects many events from the network and managed devices. Some are actionable while others are not. After saving all events to the Event Archive, Cisco ANA drops events that are nonactionable.

The remaining actionable events are identified, then examined to determine whether they represent a sequence of related events or alarms. For example, events arriving from the same device within a short period of time might be grouped and identified as an alarm because it is likely that they are related to each other.
After events are grouped, Cisco ANA looks for the root cause. If more than one event is a root cause candidate, the event with the highest weight or the closest in time is selected. If the root cause event is ticketable, a ticket is issued, and the corresponding alarms are associated with the ticket. Event reduction ensures important events are brought into focus, while nonactionable events are filtered out to avoid distracting attention away from the important events. Figure 3-12 illustrates the event reduction process.

**Figure 3-12 Event Reduction**

![Event Reduction Diagram]

**Events, the AEC, and VNEs**

Cisco ANA polls devices to discover changes in its network model and generates internal events. External events (traps, syslogs) are treated as fault indicators, which Cisco ANA confirms through expedited polling.

The AEC uses a high speed collector to obtain and receive traps and syslogs from network elements and distributes each event to the VNE representing the device that sent it. For each received trap or syslog, the AEC creates a raw (unparsed) event. The AEC also stores each event from a managed element by sending the event to the Event Archive.

The AEC then sends the event to a shared buffer for forwarding to the appropriate VNE. If a high number of notifications arrive simultaneously, exceeding the per-VNE limit, the overflow notifications are directed to a burst buffer. The burst buffer operates on a first-come, first-served basis. If the burst buffer is full, any additional new events are dropped, and a system event is generated to inform the operator of the situation.

If required, the following can be configured:

- Shared buffer size
- Burst buffer size
- Queue size
- Amount of time that elapses between each event that is sent

Upon receipt of the event, the VNE identifies the event type and drops the nonactionable events. Events that are dropped at this stage are not stored in the fault archive, and do not participate in correlation. Dropping events at this stage prevents Cisco ANA from being overwhelmed by large numbers of insignificant event notifications.

Pruning events older than three months in the Event Archive is handled by the Cisco ANA integrity process. For more information, see Database Management, page 3-24.
Event Manager

After an event notification reaches the VNE, it is processed by the event manager. The event manager handles all network events, regardless of their detection method, such as polling, syslogs, traps, or threshold crossing alerts (TCAs). The event manager parses and persists the events as follows:

- Event parsing applications extract information from the raw event, such as its source, the problem it represents, and its perceived severity.
- The VNE saves the event to the Fault Database. As soon as the event is persisted, it can be viewed in Cisco ANA EventVision.

VNE and Fault Agent

The VNE sends a message to the Fault Agent with information about the correlation result, which is updated in the event record. After the update message arrives, the Fault Agent determines if a new ticket is needed and if yes, creates the ticket.

After the VNE completes the correlation for a flapping event or completes the handling for a clearing event, it sends an update to the Fault Agent with the following information:

- Event ID—The updated event identifier.
- Causing event ID—The event cause identifier, if relevant.
- Causing event source OID—The event cause source OID.
- Causing event name—The event cause name.
- ConnectTo ID—The identifier of the preceding event. The preceding event can be the event cause, if it is found, or the preceding event in the alarm sequence.

This information is updated in the Fault Database event record. The concept of a preceding event boosts the association of the event with an alarm or ticket. If the event does not have a ConnectTo ID, the Fault Agent creates a ticket if the event is defined as attention worthy.

Fault Agent

The Fault Agent runs in each Cisco ANA unit and is responsible for:

-Persisting events.
- Updating correlation information for enriched events.
- Creating new tickets, as required.

The Fault Agent is available as soon as its hosting AVM is up. The Fault Agent is designed to recover quickly if failover occurs in a high availability environment.

The Fault Database receives events in the following modes:

- Batch mode—Events are inserted into the database in batches of configurable size. The configuration is dynamic and can be changed. For more information about customizing fault behavior, see the Cisco Active Network Abstraction 3.7.2 Customization User Guide.
- Poll mode—Polling is used so that events wait no longer than a configured amount of time if events arrive at a rate that does not fill the buffer.

As soon as an event is persisted, it can be viewed in Cisco ANA EventVision.
Event Archive and Fault Database

All incoming event notifications are archived in Event Archive. Events, alarms, and tickets that are not dropped after the identification phase are stored in the Fault Database. Cisco ANA stores all event types, even if the event is not recognized, and the archive includes the relationship between events and subsequent alarms and tickets. Events are stored as Cisco ANA event objects. The original incoming event notification structure (trap or syslog) is not maintained.

Fault Database content can be viewed using Cisco ANA EventVision. Statistics, such as the number of events persisted per second, number of created tickets, and other event data can be viewed using the Cisco ANA Report Manager, which can be launched from Cisco ANA Manage, Cisco ANA NetworkVision, and Cisco ANA EventVision.

Stored events might be marked as archived. Archived events are kept in the Fault Database and can be viewed in Cisco ANA EventVision. An event is archived when:

- The entire correlation hierarchy to which the event belongs is marked as archived (see Ticket Management Operations, page 3-14).
- The event did not relate to any other event or is not ticketable.

Northbound Integration Services

Cisco ANA supports notification services to both external OSS applications and northbound clients. Notification services are available for all event notifications for actionable and nonactionable events, as well as tickets and ticket updates. NBI services are available for SNMP and BQL. Notifications are available in EPM-NOTIFICATION-MIB format only. See the Cisco Active Network Abstraction Integration Developer Guide for more information about the Cisco EPM-NOTIFICATION-MIB and its format, and for configuring notification services.

Event Reporting

The Cisco ANA Report Manager, available in Cisco ANA Manage, Cisco ANA NetworkVision, and Cisco ANA EventVision, enables you to produce and customize reports about events, traps, tickets, and sylogs. Standard Cisco ANA event reports show:

- Number of sylogs, tickets, and traps in the alarm database and the AEC
- Daily average and peak number of sylogs and traps
- Daily event count
- Devices with the most events by severity or type
- Devices with the most sylogs or traps
- Most common daily events
- Most common sylogs
- Syslog count
- Syslog count by device

The reports allow you to specify the time period and devices to be included, and provide output in a variety of output formats, such as XML, XLS, HTML, and PDF.
For information on the types of fault management reports available and how to create them, see the Cisco Active Network Abstraction 3.7.2 User Guide.

Database Management

Cisco ANA provides the following processes for managing the database:

- Integrity and pruning process
- Database size maintenance

The integrity and pruning process is a scheduled Cisco ANA process responsible for:

- Guaranteeing the integrity of the alarm database by fixing any detected integrity violations. Integrity violations include correlation loops, missing root cause events, clearing events with no flagging event, and so on.
- Pruning old events and alarm and ticket records from the database.
- Pruning old raw event records from the Event Archive.

You can control the length of time events, alarms, and tickets are kept before they are pruned from the database. For more information about customizing fault behavior, see the Cisco Active Network Abstraction 3.7.2 Administrator Guide.

To prevent database overflow, Cisco ANA automatically deletes old data. You can configure the period of time that the events are maintained, which is the current time minus the event history size. Any event before this time is deleted. For more information about customizing fault behavior, see the Cisco Active Network Abstraction 3.7.2 Administrator Guide.