CHAPTER 1

Fault Management Overview

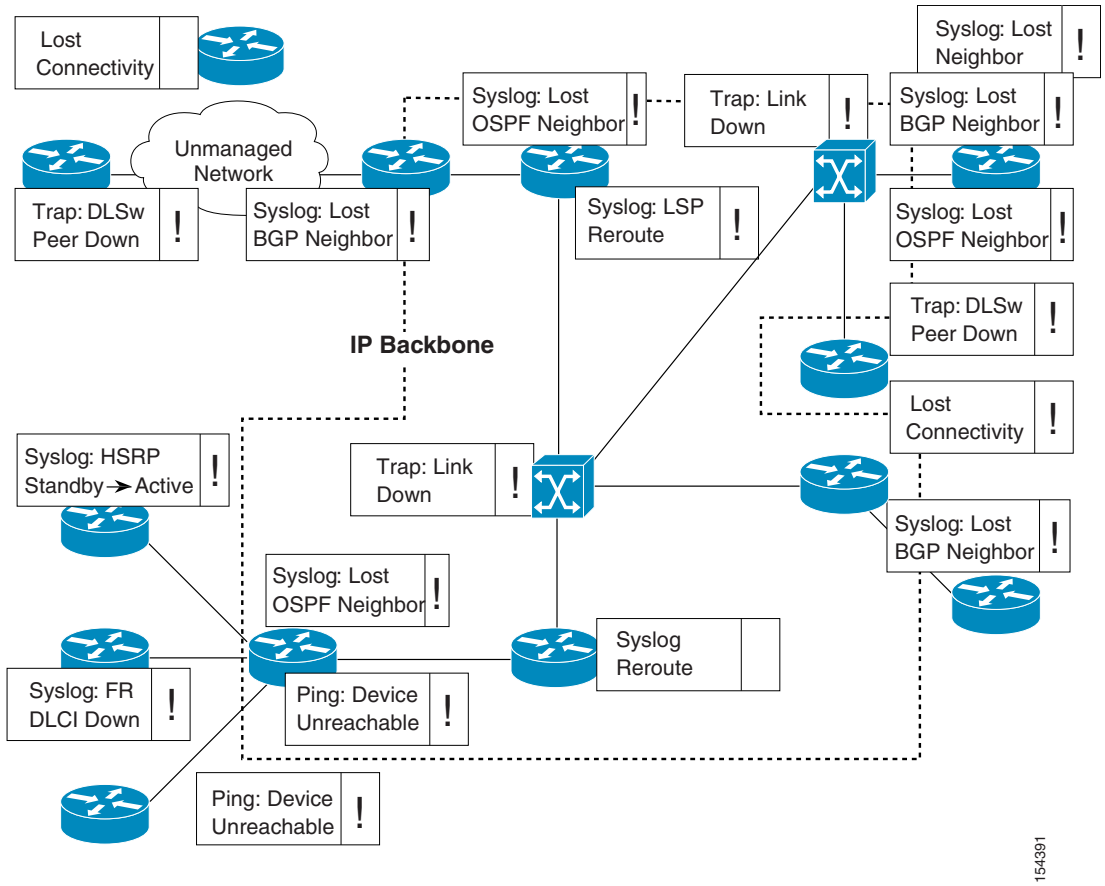
This chapter describes the challenge of managing an overabundance of events, and introduces some of the key concepts of Cisco ANA alarm management.

- Managing Events—Describes how to manage events effectively.
- Basic Concepts and Terms—Describes the basic concepts and terms used throughout this guide.
- Severity Propagation—Describes the concept of severity, and how severity is propagated.
- Event Processing Overview—Describes the process for identifying and processing raw events.

Managing Events

The challenge of dealing effectively with events and alarms is to know how to understand and efficiently process and organize bulks of raw events that may be generated as a result of single root cause events.

Figure 1-1 Event Flood



Meeting the event management challenge is done by correlating related events into a sequence that represents the alarm lifecycle, and using the network dependency model to determine the causal inter-relationship between alarms.

Cisco ANA can be used for analyzing and managing faults using fault detection, isolation and correlation. Once 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 and, if applicable, to perform service impact analysis.

Basic Concepts and Terms

Alarm

An alarm represents a scenario which involves a fault occurring in the network or management system. Alarms represent the complete fault lifecycle, from the time that the alarm is opened (when the fault is first detected) until it is closed and acknowledged. Examples of alarms include:

- Link down
- Device unreachable

- Card out
- An alarm is composed of a sequence of events, each representing a specific point in the alarm's lifecycle.

Event

An event is an indication of a distinct occurrence that occurred at a specific point in time. Events are derived from incoming traps and notifications, and from detected status changes. 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 reachable by the management station.
- User acknowledgement of an alarm.

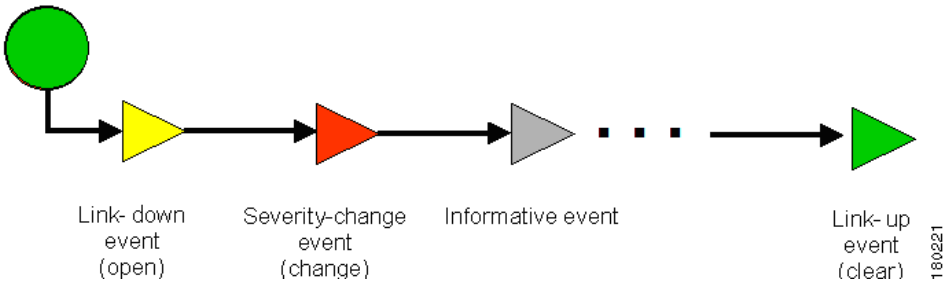
Events are written to the Cisco ANA database once and never change.

The collected events are displayed in Cisco ANA EventVision. Refer to the *Cisco Active Netowrk Abstraction EventVision User Guide* for more information.

Event Sequence

An event sequence is the set of related events which comprises a single alarm. For example, link down > ack > link up.

Figure 1-2 Event Sequence Example



Typically, a complete event sequence includes three mandatory events:

- Alarm open (in this example a link-down event).
- Alarm clear (in this example a link-up event).
- Alarm acknowledge.

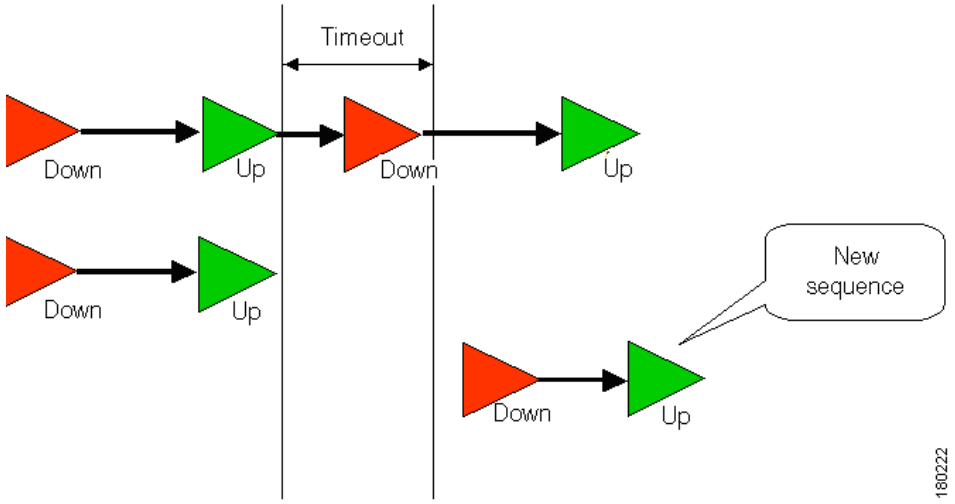
Optionally, there can be any number of alarm change events which can be triggered by new severity events, affected services update events, and so on.

Note The event types that will belong to each sequence can be configured in the system registry.
An event sequence can consist of a single event (for example, “device reset”).
The set of events that should participate in Cisco ANA alarm processing can be configured in the system registry.

Repeating Event Sequence

If a new opening event arrives within a configurable timeout after the clearing event of the same alarm, the alarm is updatable, and a repeating event sequence is created, that is, the event is attached to the existing sequence and updates its severity accordingly. If the new opening event occurs after the timeout, it opens a new alarm (new event sequence).

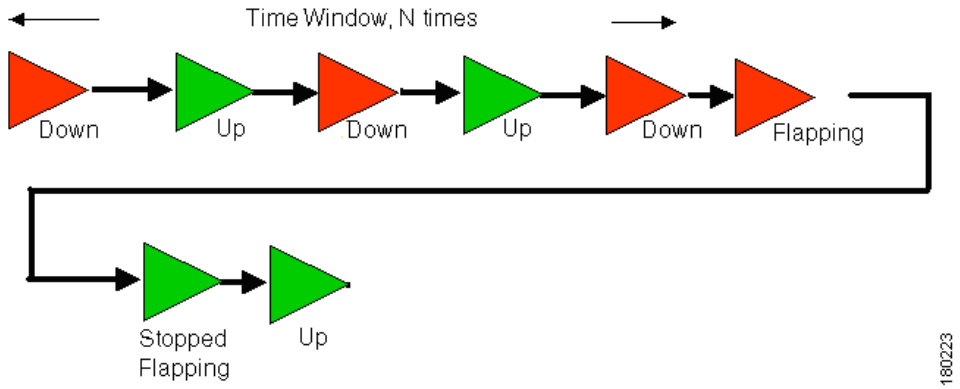
Figure 1-3 Repeating Event Sequence



Flapping Events

If a series of events that are considered to be of a same sequence occur in the network in a certain configurable time window a certain (configurable) amount of times, the virtual network element (VNE) may (upon configuration) reduce further the number of events, and will issue a single event which will be of type “event flapping”. Only when the alarm stabilizes and the event frequency is reduced, will another update to the event sequence be issued as “event stopped flapping”. Another update will be issued with the most up-to-date event state.

Figure 1-4 Flapping Event

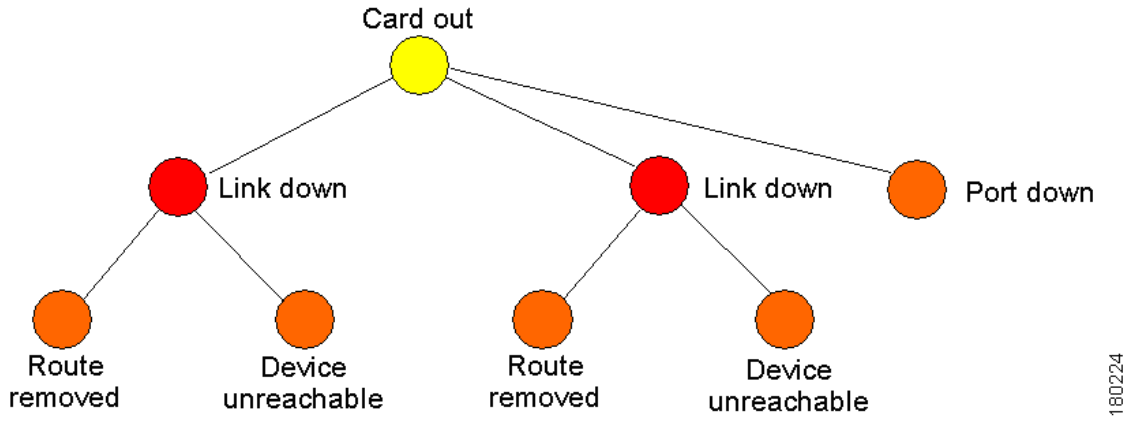


Correlation By Root Cause

Root cause correlation is determined between alarms or event sequences. It represents a causal relationship between an alarm and the consequent alarms that occurred because of it.

For example, a card-out alarm can be the root cause of several link-down alarms, which in turn can be the root cause of multiple route-lost and device unreachable alarms, and so on. A consequent alarm can serve as the root cause of other consequent alarms.

Figure 1-5 Root Cause Correlation Hierarchy Example



Ticket

A ticket represents the complete alarm correlation tree of a specific fault scenario. It can be also identified by the topmost or “root of all roots” alarm. 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, the managed entity is always a complete ticket. Operations such as Acknowledge, Force-clear or Remove are always applied to the whole ticket. The ticket also assumes an overall, propagated severity.

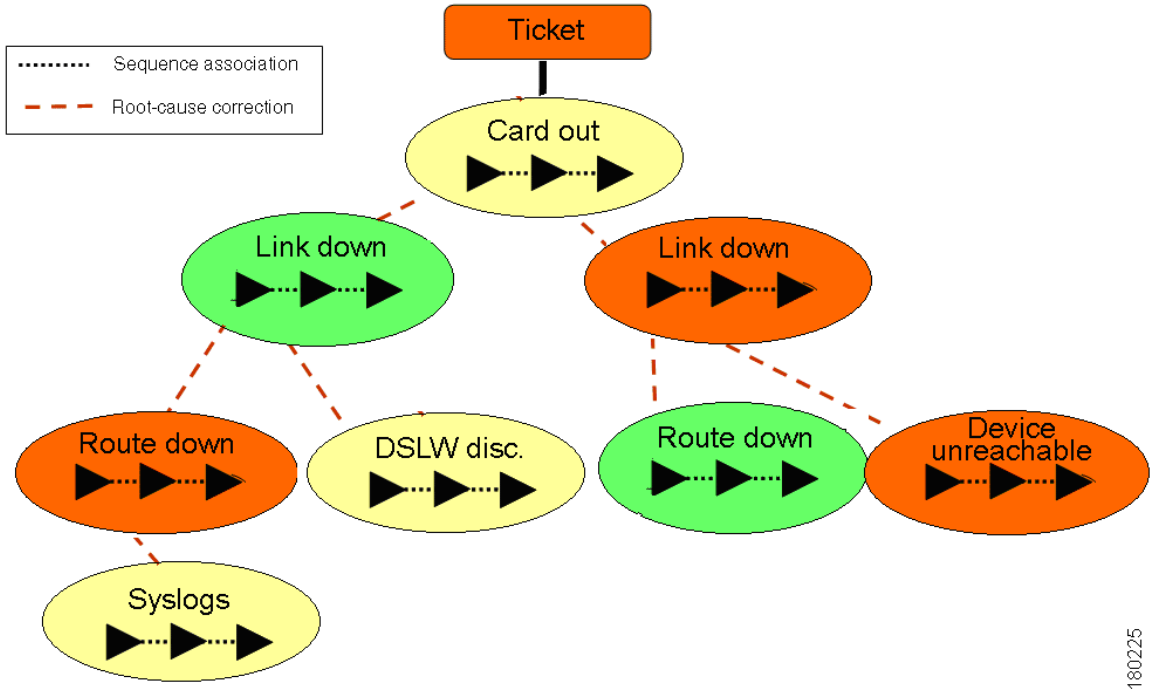
Sequence Association and Root Cause Analysis

There are two different types of relationships in Cisco ANA alarm management:

- Sequence Association—The association between events, which creates the event sequences and alarms.
- Root Cause Analysis—The association between alarms (event sequences) which represents the root cause relationship.

The following figure shows how both types of relationship are implemented in the ticket hierarchy:

Figure 1-6 Sequence Association vs. Root Cause Analysis



In the above figure, the alarms are correlated into a hierarchy according to root cause. Within each alarm is its respective event sequence representing the lifecycle of the alarm.

Severity Propagation

Each event has an assigned severity (user-configurable). For example, a link-up event may be assigned critical severity, while its corresponding link-up event will have normal severity.

The propagated severity of the alarm (the whole event sequence) is always determined by the last event in the sequence. In the above example, when the link-down alarm is open it will have critical severity; when it clears it moves to normal severity. An exception to this rule is the informational event (severity level of info) such as user acknowledge event, which does not change the propagated severity of the sequence (the alarm).

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

Note Each alarm does not assume the propagated severity of the correlated alarms beneath it. Each alarm assumes its severity only from its internal event sequence, as described above, while the ticket assumes the highest severity among all the alarms in the correlation tree.

Event Processing Overview

Cisco ANA provides a customizable framework for identifying and processing raw events. The raw events are collected into the Event Manager, forwarded to their respective VNE, and then processed as follows:

Step 1 The event data is parsed to determine its source, type, and alarm-handling behavior.

Step 2 If the event type is configured to try and correlate, the VNE attempts to find a compliant cause alarm. This is done in the VNE fabric.

Step 3 The event fields are looked up and completed.

Step 4 The event is sent to the Cisco ANA gateway, where:

- The event is written to the event database.
- If the event belongs to an alarm, it is attached to its respective event sequence and correlated to the respective root-cause alarm within the ticket, or a new sequence and new ticket is opened.
- If the event is marked as ticketable, and it did not correlate to any other alarm, a new ticket will be opened where the alarm that triggered the ticket will be the root cause of any alarms in the correlation tree.