CHAPTER 5

Correlation Over Unmanaged Segments

This chapter describes how Cisco ANA performs correlation decisions over unmanaged segments, namely, clouds.

- Cloud VNE—Describes managing more than one network segment that interconnects with others, over another network segment which is not managed.
- Cloud Problem Alarm—Describes the cloud problem alarm, its correlation, and provides an example.

Cloud VNE

In some scenarios Cisco ANA is required to manage more than one network segment that interconnects with others over another network segment which is not managed. In such setups, faults on one device might be correlated to faults on another device that is located on the other side of the unmanaged segment of the network, or to unknown problems in the unmanaged segment itself.

A virtual cloud is used for representing unmanaged network segments. It represents the unmanaged segment of the network as a single device that the two managed segments of the network are connected to, and has that device simulate the workings of the unmanaged segment.

Virtual clouds support specific network setups. The types of unmanaged networks that are supported are:

- Frame Relay
- ATM
- Ethernet

Types of Unmanaged Networks Supported

This section describes the types of unmanaged networks that are supported when a VNE simulates an unmanaged segment of a network.

Note The unmanaged segments referred to in this section must be pure switches, no routing can be involved with the segment.

Table 5-1 Cloud Types Supported

Technology Type	Supported When...	Logical Inventory	Physical Inventory
ATM	An ATM cloud (representing unmanaged network segments) comprised of ATM switches is connected to routers (managed segments) with ATM interfaces. The ATM interface or sub-interface in the router is IP over an ATM VC encapsulation interface with a VC (VPI or VCI) or VP (VPI) configuration.	The IP interface connected to a routing entity or VRF component, for the ATM interface or sub-interface.	The ATM port connected to the VC encapsulation, for the ATM interface or sub-interface.
Frame Relay	A Frame Relay cloud (representing unmanaged network segments) comprised of Frame Relay switches is connected to routers (managed segments) with Frame Relay interfaces. The Frame Relay interface or sub-interface in the router is IP over a Frame Relay VC encapsulation interface with a DLCI configuration.	The IP interface connected to a routing entity or VRF component, for the Frame Relay interface or sub-interface.	The Frame Relay port connected to the VC encapsulation, for the Frame Relay interface or sub-interface.
Ethernet	A Ethernet LAN cloud (representing unmanaged network segments) comprised of Ethernet LAN switches is connected to routers (managed segments) with Ethernet interfaces. The ethernet interface or sub-interface in the router can be either native or VLAN interfaces.	The IP interface connected to a routing entity or bridges, for the ethernet interface or sub-interface.	The ethernet port connected to the VLAN encapsulation, for the ethernet interface or sub-interface.

Fault Correlation Across the Frame Relay or ATM or Ethernet Cloud

When a Layer 3 or Layer 2 event (for example, reachability problem, neighbor change, Frame Relay DLCI down, ATM PVC down) occurs, it triggers a flow along the physical and logical path modeled on the VNEs. This is done in order to correlate to the actual root cause of this fault. If the flow passes over a cloud along the path flow, it marks it as a potential root cause for the fault. If there is no other root cause found on the managed devices, then the cloud becomes the root cause. A ticket is then issued and the original event correlates to it.

Cloud Problem Alarm

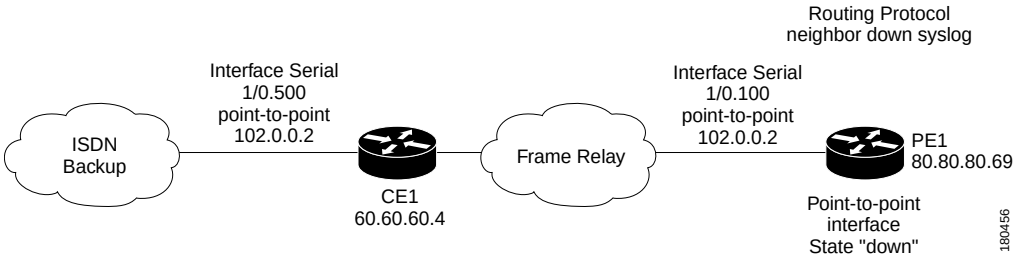
For some events, when there is no root cause found, a special cloud problem alarm is created. These events are then correlated to the alarm. The cloud problem alarm has a major severity, and is automatically cleared after a delay.

Note When required a correlation filter, filters the cloud problem. This enables or disables the ability of an alarm to create a cloud problem alarm, and to correlate to it. The default value is false for all alarms in the system, meaning that an alarm does not correlate to the cloud problem alarm by default. However, there are several alarms that override the default configuration and are set to true, as follows:
BGP neighbor down syslog
OSPF neighbor loss syslog
EIGRP router query to neighbors timeouted syslog
ipx 3 bad igrp sap syslog

Cloud Correlation Example

In this example, two devices that have OSPF configured are connected through a cloud. A malfunction occurs inside the unmanaged network that causes the OPSF neighbor down alarm to be generated. In this case the OSPF neighbor down alarm is correlated to the cloud problem.

Figure 5-1 Cloud Correlation Example



On the PE1 device, the OSPF neighbor down alarm was received, and no root cause was detected in any of the managed devices. A disconnected link inside the unmanaged network caused the OSPF neighbor down alarm. The following alarms are generated and correlated:

- Cloud problem on the cloud:
  - OSPF neighbor down on the PE1 is correlated to the cloud problem alarm.