CHAPTER 4

Advanced Correlation Scenarios

This chapter describes the specific alarms which use advanced correlation logic on top of the root cause analysis flow:

- Device Unreachable Alarm—Describes the device unreachable alarm, its correlation and provides various examples.
- IP Interface Failure Scenarios—Describes the ip interface status down alarm and its correlation. In addition, it describes the all ip interfaces down alarm, its correlation and provides several examples.
- Multi Route Correlation—Describes support for multi route scenarios and their correlation. In addition, it provides several examples.
- Generic Routing Encapsulation (GRE) Tunnel Down/Up—Provides an overview of GRE tunneling, describes the GRE tunnel alarm, and provides correlation examples.
- BGP Process Down Alarm—Describes the BGP process down alarm, and its correlation.
- MPLS Interface Removed Alarm—Describes the MPLS interface removed alarm, and its correlation.

Device Unreachable Alarm

Connectivity Test

Connectivity tests are used to verify connectivity between the VNEs and managed network elements. The connectivity is tested using each protocol the VNE uses to poll the device. The supported protocols for connectivity tests are SNMP, Telnet and ICMP.

A device unreachable alarm will be issued if one or more of the connectivity test fails, that is, the device does not respond on this protocol. The alarm will be cleared when all the protocol connectivity test are passed successfully.

Note The ICMP connectivity test is enabled in Cisco ANA Manage.

Device Fault Identification

When a network element stops responding to queries from the management system, one of two things has happened:

- Connectivity to that device is lost.
- The device itself crashes or restarts.

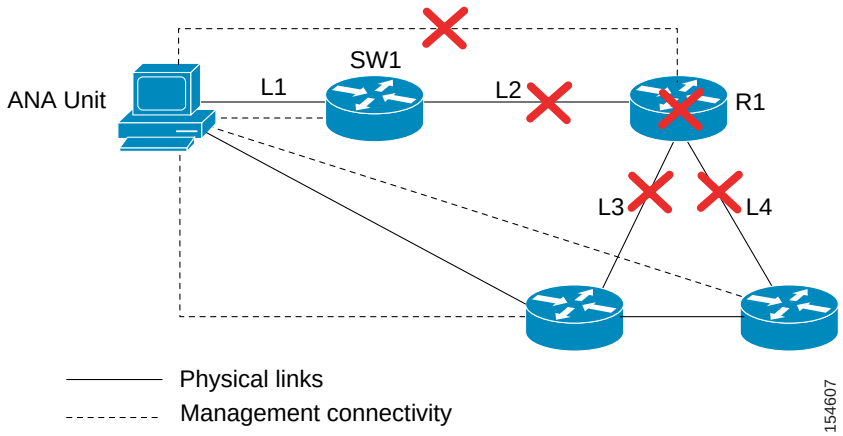
Cisco ANA implements an algorithm that uses additional data to heuristically resolve the ambiguity and declare the root cause correctly. Refer to the following examples:

- Device Unreachable Example 1
- Device Unreachable Example 2

Device Unreachable Example 1

In this example, the router (R1) goes down. As a result the links, L2, L3, and L4 go down in addition to the R1 session.

Figure 4-1 Device Unreachable Example 1



In this case the system will provide the following report:

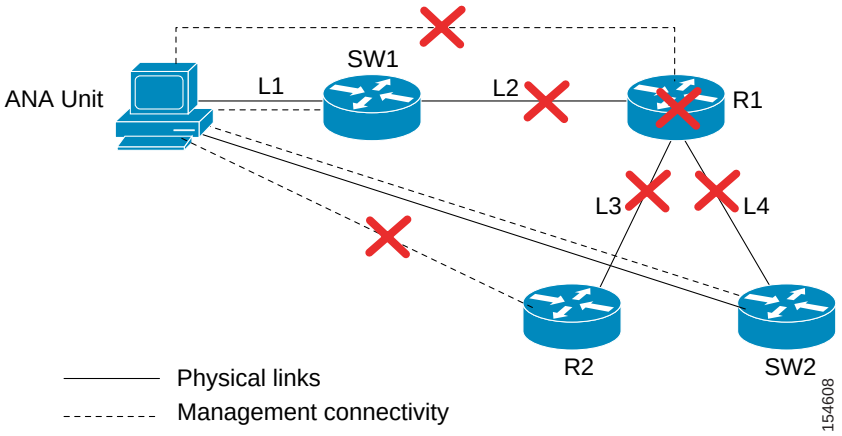
- Root cause—Device Unreachable (R1)
- Correlated events:
  - L2 down
  - L3 down
  - L4 down

Device Unreachable Example 2

In this example, the router (R1) goes down. As a result the links, L2, L3, and L4 go down as well as the R1 session. The router R2, accessed by the link L3 is also unreachable.

Note No link-down alarm is displayed for L3 as its state cannot be determined.

Figure 4-2 Device Unreachable Example 2



Note If the device has a single link and it is being managed through that link (in-band management), there is no way to determine if the device is unreachable due to a link down, or the link is down because the device is unreachable. In this case, Cisco ANA shows that the device is unreachable due to link down.

In this case the system will provide the following report:

- Root cause—Device Unreachable (R1)
- Correlated events:
  - L2 down
  - Device Unreachable (R2)
  - L4 down

IP Interface Failure Scenarios

This section includes:

IP Interface Status Down Alarm

Alarms related to subinterfaces, for example, line-down trap, line-down syslog, and so on, are reported on IP interfaces configured above the relevant subinterface. This means that in the system, subinterfaces are represented by the IP interfaces configured above them. All events sourcing from subinterfaces without a configured IP are reported on the underlying Layer 1.

An “ip interface status down” alarm is generated when the status of the IP interfaces (whether it is over an interface or a subinterface) changes from up to down or any other non-operational state. All events sourced from the subinterfaces correlate to this alarm. In addition an “All ip interfaces down” alarm is generated when all the IP interfaces above a physical port change state to down.

Table 4-1 IP Interface Status Down Alarm

Name	Description	Ticketable	Correlation allowed	Correlated to	Severity
Interface status down/up	Sent when an IP interface changes oper status to “down”	Yes	Yes	Link Down/Device unreachable/Configuration changed	Major

The alarm’s description includes the full name of the IP interface, for example Serial0.2 (including the identifier for the subinterface if it is a subinterface) and the source of the alarm source points to the IP interface (and not to Layer1).

All syslogs and traps indicating changes in subinterfaces (above which an IP is configured) correlate to the “ip interface status down” alarm (if this alarm was supposed to be issued). The source of these events is the IP interface. Syslogs and traps that indicate problems in Layer1 (that do not have a subinterface qualifier in their description) are sourced to Layer1.

Note In case a syslog or trap is received from a subinterface that does not have an IP configured above it, the source of the created alarm is the underlying Layer 1.

For example:

- Line-down trap (for subinterface).
- Line-down syslogs (for subinterface).

For events that occur on subinterfaces:

- When sending the information northbound, the system uses the full subinterface name in the interface name in the source field, as described in the ifDesc/ifName OID (for example Serial0/0.1 and not Serial0/0 DLCI 50).
- The source of the alarm is the IP interface configured above the subinterface.
- If there is no IP configured, the source is the underlying Layer 1.

In case the main interface goes down, all related subinterfaces’ traps and syslogs are correlated as child tickets to the main interface parent ticket.

The following technologies are supported:

- Frame Relay/HSSI
- ATM
- Ethernet, Fast Ethernet, Gigabit Ethernet
- POS
- CHOC

Correlation of Syslogs and Traps

When receiving a trap or syslog for the subinterface level, immediate polling of the status of the relevant IP interface occurs and a polled parent event (for example, ip interface status down) is created. The trap or syslog is correlated to this alarm.

Where there is a multipoint setup and only some circuits under an IP interface go down, and this does not cause the state of the IP interface to change to down, then no “ip interface status down” alarm is created. All the circuit down syslogs correlate by flow to the possible root cause, for example, Device unreachable on a customer edge (CE) device.

All IP Interfaces Down Alarm

- When all the IP interfaces configured above a physical interface change their state to down, the All ip interfaces down alarm is sent.
- When at least one of the IP interfaces changes its state to up, a clearing (active ip interfaces found) alarm is sent.
- The ip interface status down alarm for each of the failed IP interfaces is correlated to the All ip interfaces down alarm.

Note When an All ip interfaces down alarm is cleared by the active ip interfaces down alarm but there are still correlated ip interface status down alarms for some IP interfaces, the severity of the parent ticket is the highest severity among all the correlated alarms. For example, if there is an uncleared interface status down alarm, the severity of the ticket remains major, despite the fact that the Active ip interfaces found alarm has a cleared severity.

Table 4-2 All IP Interfaces Down

Name	Description	Ticketable	Correlation allowed	Correlated to	Severity
All ip interfaces down/Active ip interfaces found	Sent when all the IP interfaces configured above a physical port change their oper status to down	Yes	Yes	Link Down/Configuration Change	Major

The All ip interfaces down alarm is sourced to the Layer1 component. All alarms from “the other side”, for example, device unreachable correlate to the All ip interfaces down alarm.

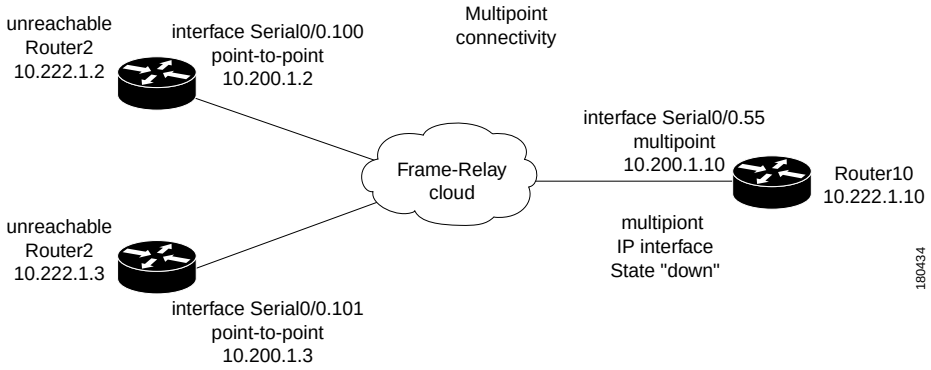
IP Interface Failure Examples

Note In all the examples that follow it is assumed that the problems that result in the unmanaged cloud, or the problems that occurred on the other side of the cloud (for example, an unreachable CE device from a provider edge (PE) device) cause the relevant IP interfaces’ state to change to down. This in turn causes the ip interface status down alarm to be sent.
If this is not the case, as in some Ethernet networks, and there is no change to the state of the IP interface, all the events on the subinterfaces that are capable of correlation flow will try to correlate to other possible root causes, including “cloud problem”.

Interface Example 1

In this example there is multipoint connectivity between a PE and number of CEs through an unmanaged Frame Relay network. All the CEs (Router2 and Router3) have logical connectivity to the PE through a multipoint subinterface on the PE (Router10). The keep alive option is enabled for all circuits. A link is disconnected inside the unmanaged network that causes all the CEs to become unreachable.

Figure 4-3 Interface Example 1



The following failures are identified in the network:

- A device unreachable alarm is generated for each CE.
- An ip interface status down alarm is generated for the multipoint IP interface on the PE.

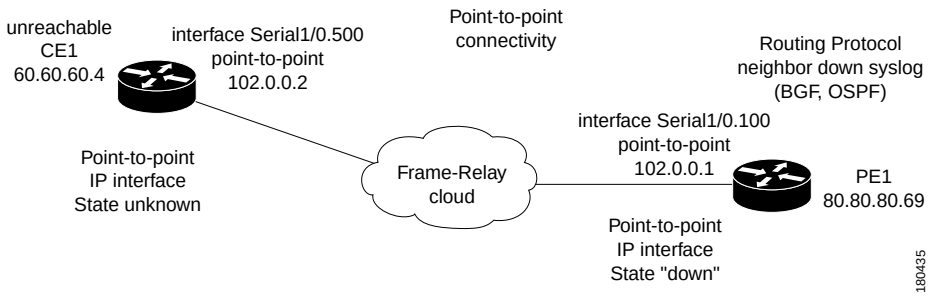
The following correlation information is provided:

- The root cause is IP subinterface down.
- All the device unreachable alarms are correlated to the ip interface status down alarm on the PE.

Interface Example 2

In this example there is point-to-point connectivity between a PE and a CE through an unmanaged Frame Relay network. CE1 became unreachable, and the status of the IP interface on the other side (on the PE1) changed state to down. The “keep alive” option is enabled. The interface is shut down between the unmanaged network and CE1.

Figure 4-4 Interface Example 2



The following failures are identified in the network:

- A device unreachable alarm is generated on the CE.

- An ip interface status down alarm is generated on the PE.

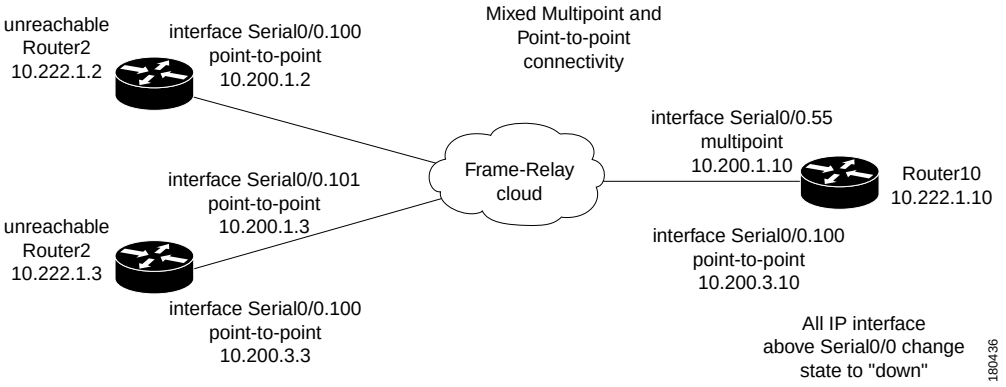
The following correlation information is provided:

- The root cause is device unreachable:
  - The ip interface status down alarm is correlated to the device unreachable alarm.
  - The syslogs and traps for the related subinterfaces are correlated to the ip interface status down alarm.

Interface Example 3

In this example there is a failure of multiple IP interfaces above the same physical port (mixed point-to-point and multipoint Frame Relay connectivity). CE1 (Router2) has a point-to-point connection to PE1 (Router10). CE1 and CE2 (Router3) have multipoint connections to PE1. The IP interfaces on PE1 that are connected to CE1, and CE2 are all configured above Serial0/0. The “keep alive” option is enabled. A link is disconnected inside the unmanaged network that has caused all the CEs to become unreachable.

Figure 4-5 Interface Example 3



The following failures are identified in the network:

- All the CEs become unreachable.
- An ip interface status down alarm is generated for each IP interface above Serial0/0 that has failed.

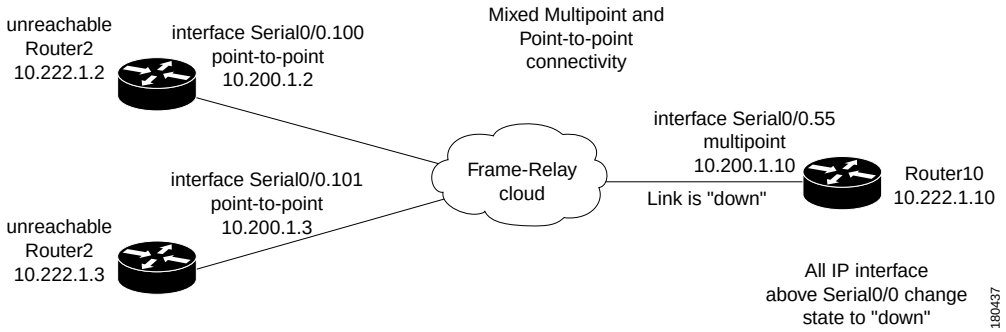
The following correlation information is provided:

- The root cause is All IP interfaces down on Serial0/0 port:
  - The ip interface status down alarms are correlated to the All IP interfaces down alarm.
  - The device unreachable alarms are correlated to the All IP interfaces down alarm.
  - The syslogs and traps for the related subinterfaces are correlated to the All IP interfaces down alarm.

Interface Example 4

In this example there is a link down. In a situation where a link down occurs, whether it involves a cloud or not, the link failure is considered to be the most probable root cause for any other failures. In this example, a link is disconnected between the unmanaged network and the PE.

Figure 4-6 Interface Example 4



The following failures are identified in the network:

- A link-down alarm is generated on Serial0/0.
- A device unreachable alarm is generated for each CE.
- An ip interface status down alarm is generated for each IP interface above Serial0/0.
- An All interfaces down alarm is generated on Serial0/0.

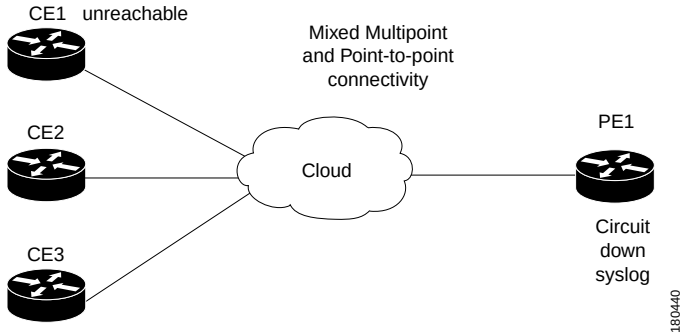
The following correlation information is provided:

- The device unreachable alarms are correlated to the link-down alarm
- The ip interface status down alarm is correlated to the link-down alarm
- The All interfaces down alarm is correlated to the link-down alarm
- All the traps and syslogs for the subinterfaces are correlated to the link-down alarm

Interface Example 5

In this example on the PE1 device that has multipoint connectivity, one of the circuits under the IP interface has gone down and the CE1 device which is connected to it has become unreachable. The status of the IP interface has not changed and other circuits are still operational.

Figure 4-7 General Interface Example



The following failures are identified in the network:

- A device unreachable alarm is generated on CE1.
- A Syslog alarm is generated notifying the user about a circuit down.

The following correlation information is provided:

- device unreachable on the CE:
  - The Syslog alarm is correlated by flow to the possible root cause, for example, a device unreachable alarm on CE1

ATM Examples

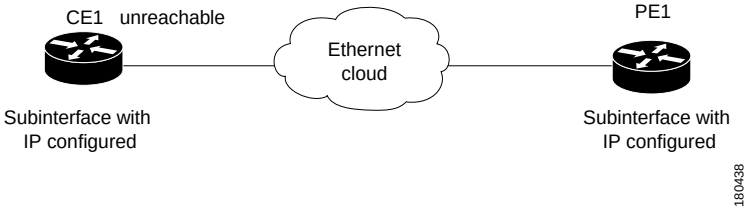
Similar examples involving ATM technology have the same result, assuming that a failure in an unmanaged network causes the status of the IP interface to change to down (ILMI is enabled).

Ethernet, Fast Ethernet, Giga Ethernet Examples

Interface Example 6

In this example there is an unreachable CE due to a failure in the unmanaged network.

Figure 4-8 Interface Example 6



The following failures are identified in the network:

- A device unreachable alarm is generated on the CE.
- A cloud problem alarm is generated.

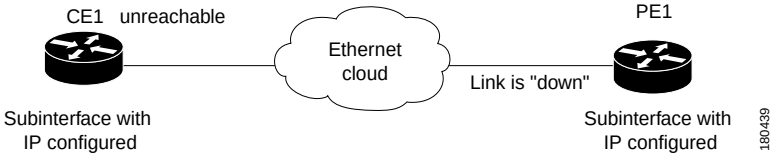
The following correlation information is provided:

- No alarms are generated on a PE for Layer1, Layer2 or for the IP layers.
- The device unreachable alarm is correlated to the cloud problem alarm.

Interface Example 7

In this example there is a link down on the PE that results in the CE becoming unreachable.

Figure 4-9 Interface Example 7



The following failures are identified in the network:

- A link-down alarm is generated on the PE.
- An ip interface status down alarm is generated on the PE.
- A device unreachable alarm is generated on the CE.

The following correlation information is provided:

- Link down on the PE:
  - The ip interface status down alarm on the PE is correlated to the link-down alarm.
  - The device unreachable alarm on the CE is correlated to the link-down alarm on the PE.
  - The traps and syslogs for the subinterface are correlated to the link down alarm on the PE

Interface Registry Parameters

ip interface status down Parameters

The following ip interface status down parameters can be controlled through the registry:

- is-correlation-allowed
- severity
- timeout
- time-stamp-delay
- weight
- is-ticketable

Note For more information about these parameters see Chapter 6, "Event and Alarm Configuration Parameters".

All ip interfaces down Parameters

The following All ip interfaces down parameters can be controlled through the registry:

- is-correlation-allowed
- is-ticketable
- severity
- activate-flow
- correlate
- timeout
- weight

Note For more information about these parameters, see Chapter 6, "Event and Alarm Configuration Parameters".

Multi Route Correlation

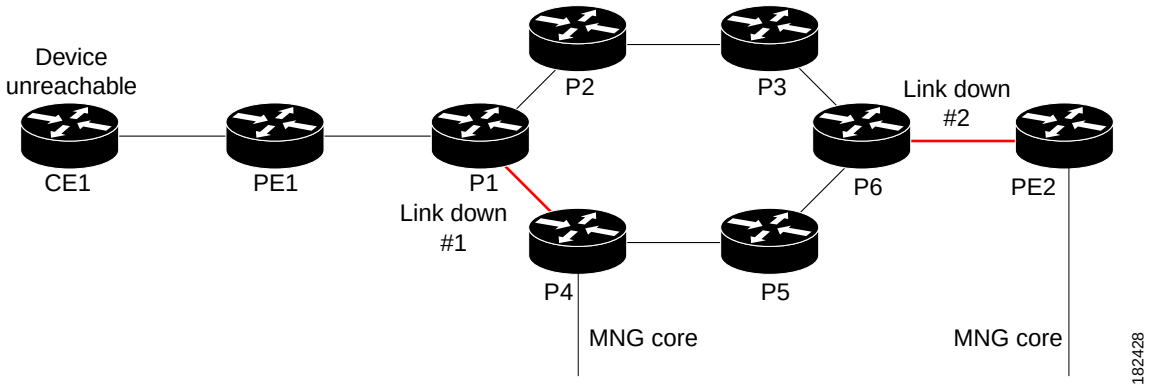
The correlation mechanism supports multi route scenarios, thereby eliminating false correlation, and guaranteeing that the correct root cause alarm is reported.

The correlation mechanism ensures that if multi-route segments exist then all the alarms found on a certain path (after eliminating invalid paths) are collected into an alarm set. These alarm sets are input into a multi route filtering algorithm which eliminates irrelevant alarms from these sets, and outputs the potentially root cause alarms. The root-cause alarm is determined from this group.

Multi Route Correlation Example 1

In this example, a link went down in the multi route segment between P1 and P4, and another link went down in the single route segment between P6 and PE2. As a result, CE1 lost connectivity to its management port, and became unreachable.

Figure 4-10 Multi Route Correlation Example 1



In this case the system will provide the following report:

- Root cause—Device Unreachable. *Link Down #2* is identified as the root-cause for Device Unreachable (CE1).

Note *Link Down #1* is not the root-cause of the alarm because after it occurs there is still an alternative route from CE1 to its management port.

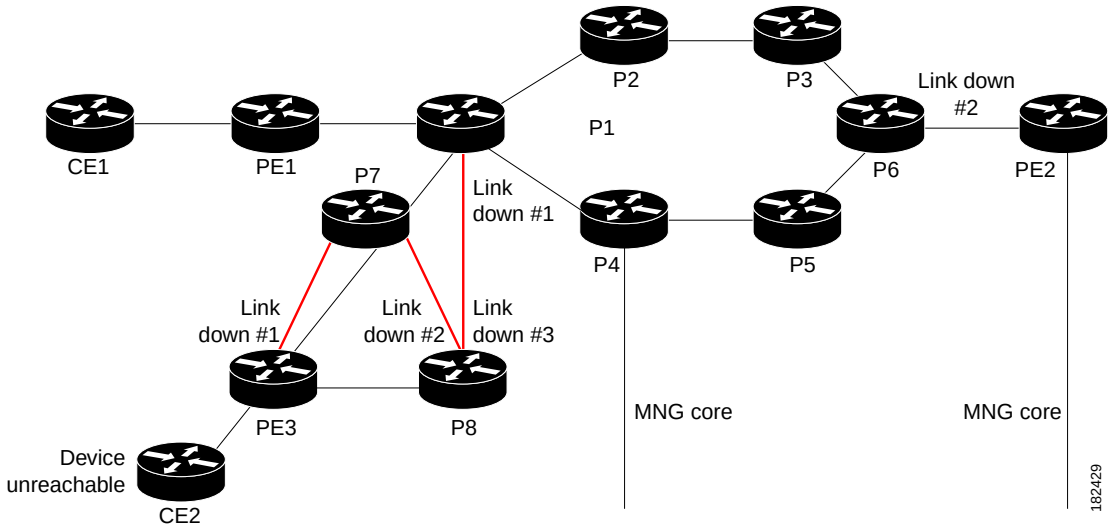
Multi Route Correlation Example 2

In this example, there are traffic engineering routes (RSVP) from router CE2, so that CE2 can reach P1 through only three possible paths, namely:

- CE2->PE3->P7->P8->P1
- CE2->PE3->P8->P1
- CE2->PE3->P7->P1

Several links went down, and as a result, router CE2 became unreachable.

Figure 4-11 Multi Route Correlation Example 2



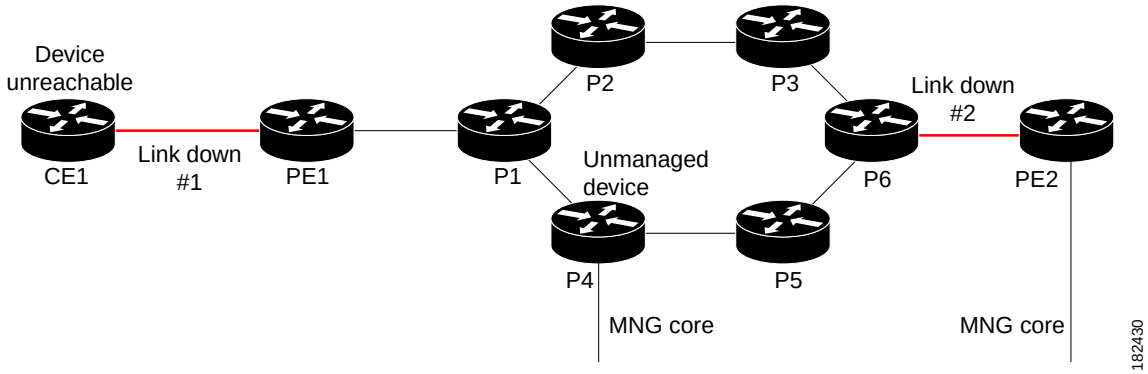
In this case the system will provide the following report:

- Root cause—Device Unreachable. *Link Down #1*, *Link Down #2* or *Link Down #3* is identified as the root cause for Device Unreachable (CE2), depending on which one occurred closest in time to the Device Unreachable event.

Multi Route Correlation Example 3

In this example, two paths exists from CE1 to PE2. Several links went down and as a result router CE1 became unreachable. In addition, router P4 is an unmanaged device.

Figure 4-12 Multi Route Correlation Example 3



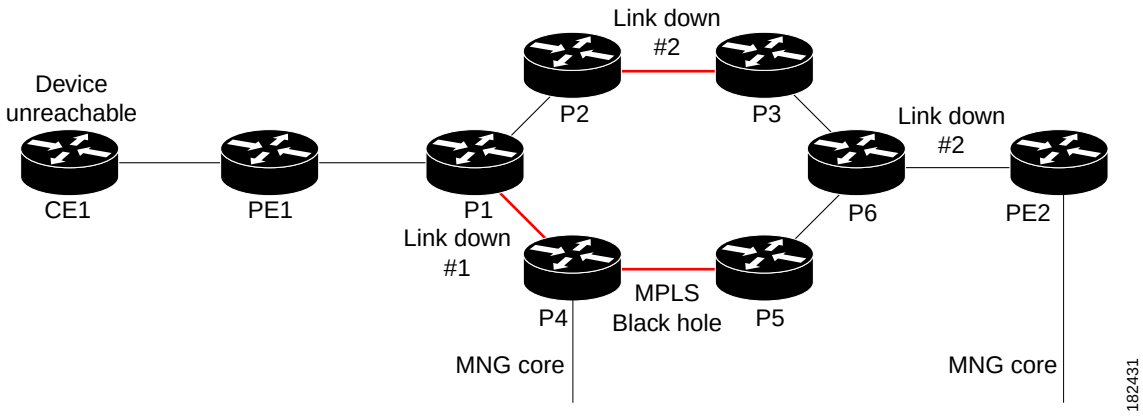
In this case the system will provide the following report:

- Root cause—Device Unreachable. *Link Down #1* or *Link Down #2* is identified as the root cause for Device Unreachable (CE1), depending on which one occurred closest in time to the Device Unreachable event.

Multi Route Correlation Example 4

In this example, two paths exists from CE1 to PE2. Several links went down, and there is a MPLS black hole in the multi route segment. As a result router CE1 became unreachable.

Figure 4-13 Multi Route Correlation Example 4



In this case the system will provide the following report:

- Root cause—Device Unreachable. *Link Down #2* is identified as the root cause for Device Unreachable (CE1).

Generic Routing Encapsulation (GRE) Tunnel Down/Up

Generic Routing Encapsulation (GRE) is a tunneling protocol that encapsulates a variety of network layer packets inside IP tunneling packets, creating a virtual point-to-point link to devices at remote points over an IP network. It is used on the Internet to secure virtual private networks (VPNs). GRE encapsulates the entire original packet with a standard IP header and GRE header before the IPsec process. GRE can carry multicast and broadcast traffic, making it possible to configure a routing protocol for virtual GRE tunnels. The routing protocol detects loss of connectivity and reroutes packets to the backup GRE tunnel, thus providing high resiliency.

GRE is stateless, which means that the tunnel endpoints do not monitor the state or availability of other tunnel endpoints. This feature helps service providers support IP tunnels for clients, who don't know the service provider's internal tunneling architecture. It gives clients the flexibility of reconfiguring their IP architectures without worrying about connectivity.

GRE Tunnel Down/Up Alarm

When a GRE tunnel link exists, if the status of the IP interface of the GRE tunnel edge changes to down, a GRE Tunnel Down alarm is created. The IP Interface Down alarms of both sides of the link will correlate to the GRE Tunnel Down alarm. The GRE Tunnel Down alarm will initiate an IP based flow toward the GRE destination. If an alarm is found during the flow, it will correlate to it.

Note The GRE Tunnel Alarm Down is supported only on GRE tunnels that are configured with keepalive. When keepalive is configured on the GRE tunnel edge, if a failure occurs in the GRE tunnel link, both IP interfaces of the GRE tunnel will be in Down state. If keepalive is not configured on the GRE tunnel edge, since the alarm is generated arbitrarily from one of the tunnel devices when the IP Interface changes to the Down state, the GRE Tunnel Down alarm might not be generated.

When a failure occurs, the GRE tunnel link is marked orange. When the IP interface comes back up, a fixing alarm is sent, and the link is marked green. The GRE Tunnel Down alarm is cleared by a corresponding GRE Tunnel Up alarm. It will also be cleared when the GRE link is discovered again.

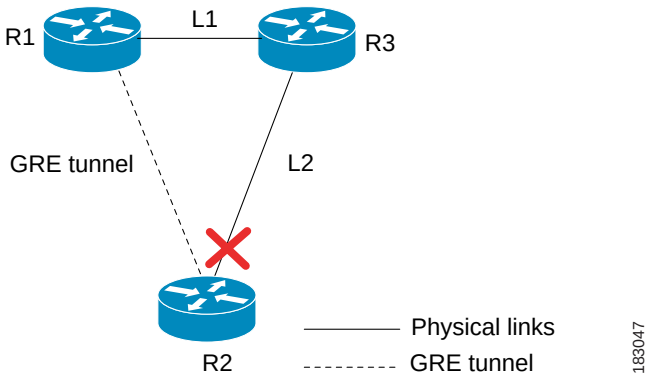
GRE Tunnel Down Correlation Example 1

The following provides an example of a GRE Tunnel Down correlation for a single GRE tunnel.

In this example:

- Router 1 (R1) is connected to Router 3 (R3) through a physical link L1.
- Router 3 is connected to Router 2 through a physical link L2.
- Router 1 is connected to Router 2 through a GRE tunnel.

Figure 4-14 GRE Tunnel Down Example 1 (Single GRE Tunnel)



When a Link Down occurs on L2, a Link Down alarm appears. A GRE Tunnel Down alarm is issued as the IP interfaces of the tunnel edge devices go down. The IP Interface Status Down alarms will correlate to the GRE Tunnel Down alarm. The GRE tunnel down will correlate to the Link Down alarm.

The system provides the following report:

- Root cause—Link down: L2 Router 2 <-> Router 3
- Correlated events:

  GRE tunnel down Router1:tunnel <-> Router 2:tunnel

  – IP interface down Router 1:tunnel
  – IP interface down Router 2:tunnel

GRE Tunnel Down Correlation Example 2

This example provides a real world scenario, whereby multiple GRE tunnels cross through a physical link. When this link is shut down by an administrator, many alarms are generated. All the alarms are correlated to the root cause ticket "Link down due to admin down", as illustrated in Figure 4-15.

Figure 4-15 GRE Tunnel Down Example 2 (Multiple GRE Tunnels)

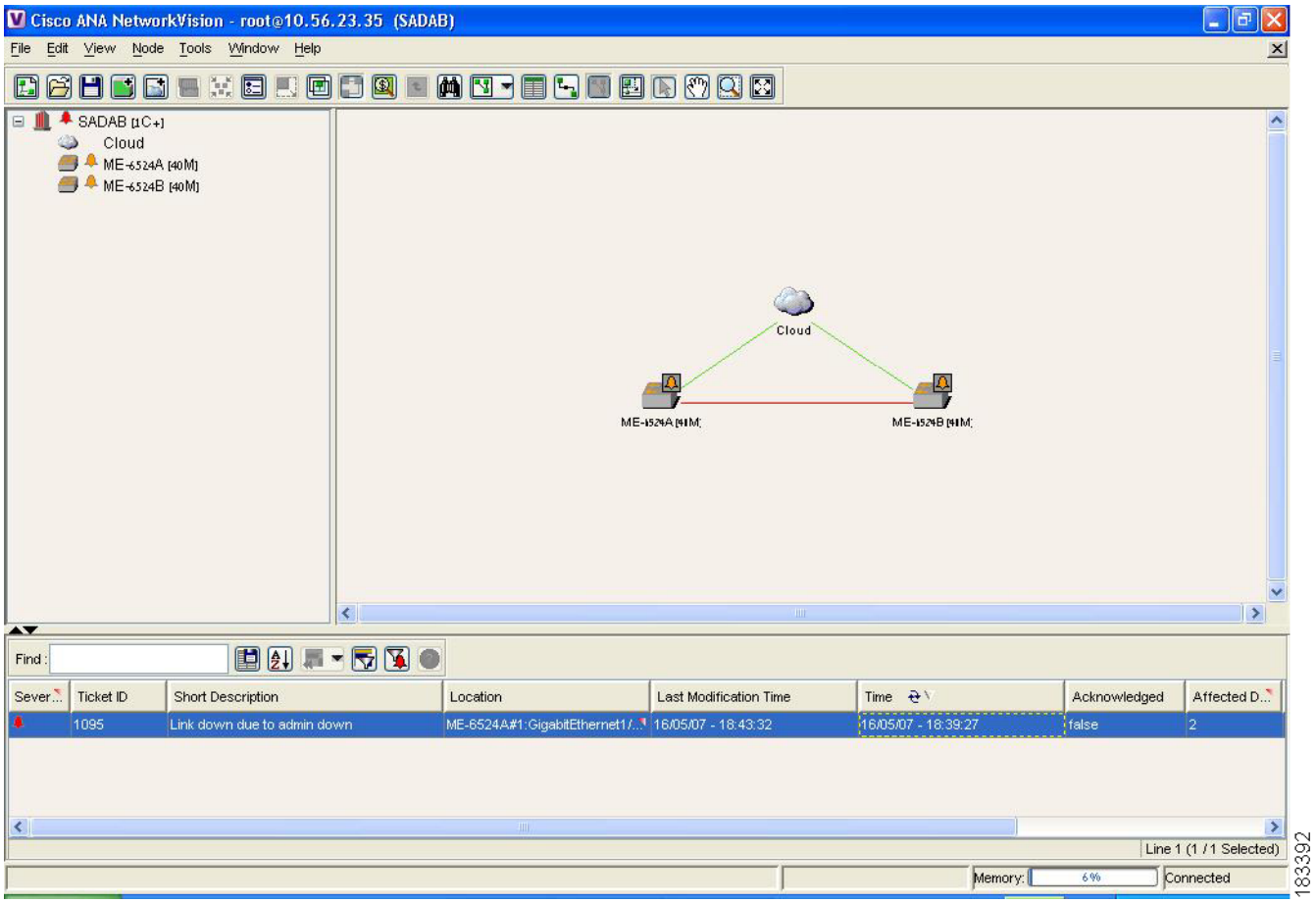
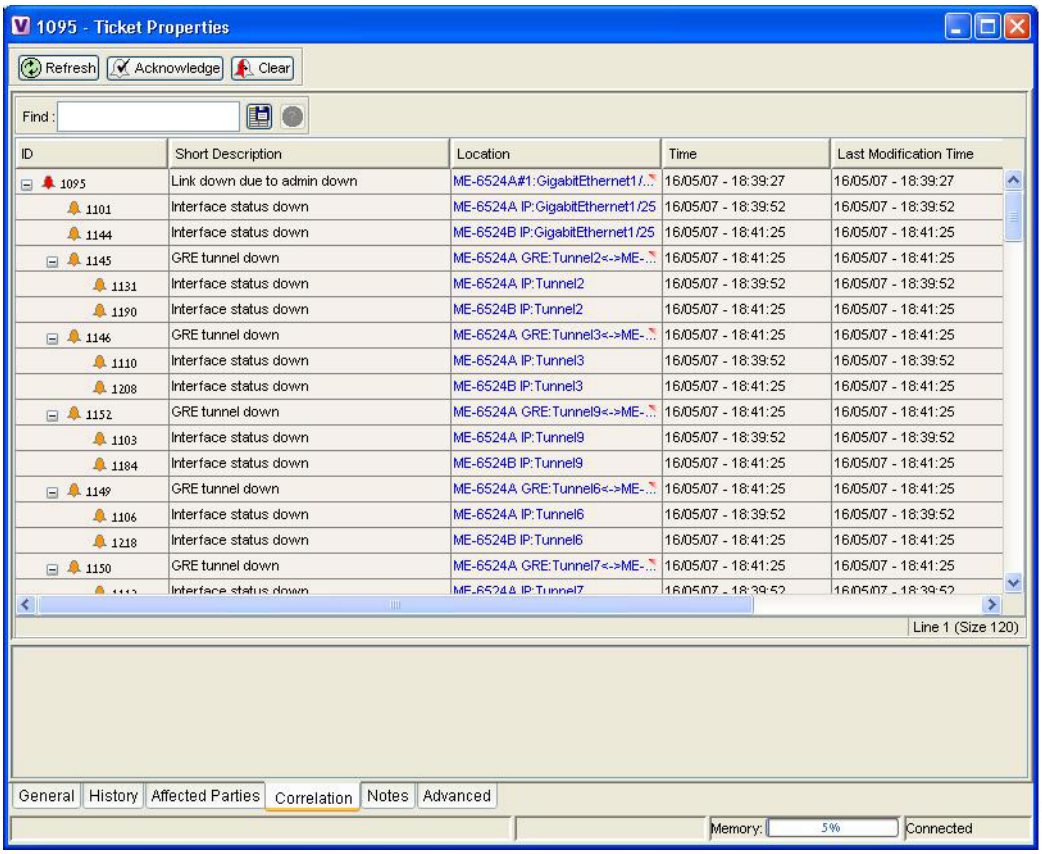


Figure 4-16 shows the Correlation tab of the Ticket Properties dialog box, which displays all the alarms that are correlated to the ticket, including the correlation for each GRE tunnel and its interface status.

Figure 4-16 Alarms Correlation to GRE Tunnel Down Ticket



As illustrated, the system provides the following report:

- Root cause—Link down due to admin down
- Correlated events:

  GRE tunnel down ME-6524AGRE:Tunnel2 <-> ME-6524B GRE:Tunnel2

  – Interface status down ME-6524A IP:Tunnel2

  – Interface status down ME-6524B IP:Tunnel2

  GRE tunnel down ME-6524AGRE:Tunnel3 <-> ME-6524B GRE:Tunnel3

  – Interface status down ME-6524A IP:Tunnel3

  – Interface status down ME-6524B IP:Tunnel3

  etc.

BGP Process Down Alarm

The BGP process down alarm is issued when the BGP process is shut down on a device. If a BGP process is shutdown on a device, the BGP neighbor down events will correlate to it as well as all the device unreachable alarms from the CE devices that lost connectivity to the VRF due to the BGP process down on the route reflector. The syslogs that the device issues expedite the status check of the BGP process and BGP neighbors.

MPLS Interface Removed Alarm

The MPLS interface removed alarm is issued when a MPLS IP interface is removed and there is no MPLS TE tunnel on the same interface. In addition, this may lead to two black holes on either side and MPLS black hole found alarms may be issued. The black holes will send a flood message to the PEs and check for any broken LSPs, and broken LSP discovered alarms may be issued. The MPLS black hole found and broken LSP discovered alarms are correlated to the MPLS interface removed alarm. The syslogs that the device issues expedite the status check of the label switching table and MPLS status.