CHAPTER 6

Advanced Correlation Scenarios

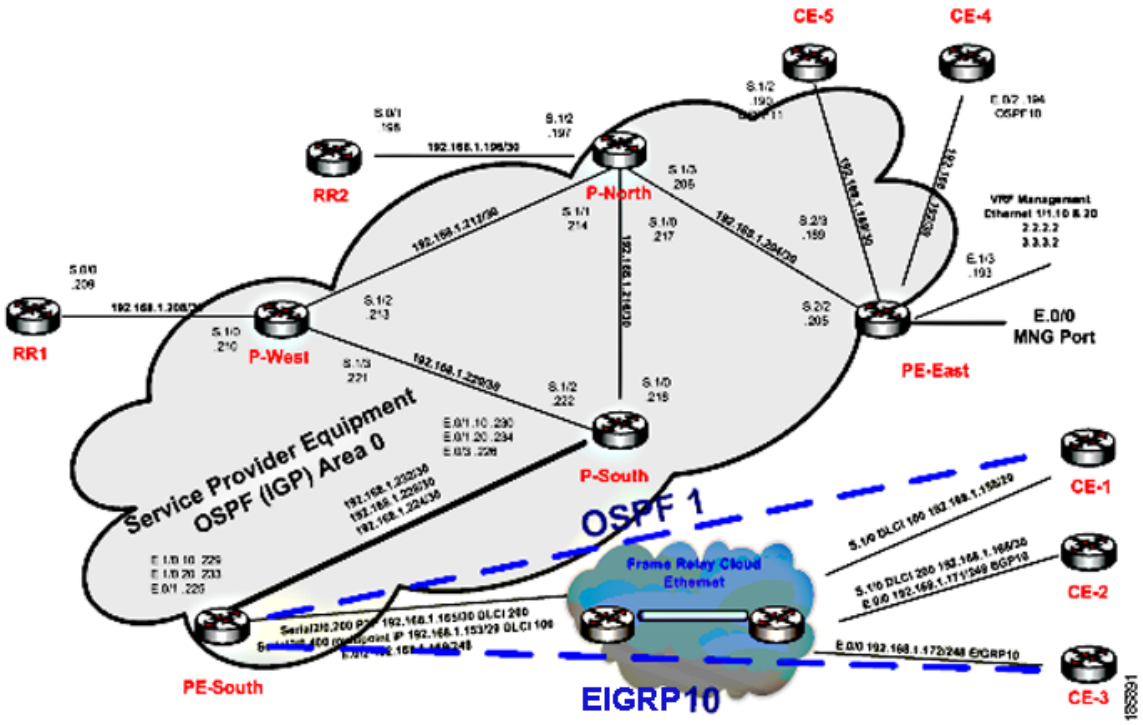
These topics describe the specific alarms which use advanced correlation logic on top of the root cause analysis flow:

- Lab Setup for the Scenarios in These Topics, page 6-2—Describes the lab setup for the scenarios described in these topics.
- Device Unreachable Correlation Scenarios, page 6-3—Describes the Device Unreachable alarm and its correlation and provides various examples.
- Multiroute Correlation Scenarios, page 6-12—Describes support for multiroute scenarios and their correlation. In addition, it provides several examples.
- BGP Neighbor Loss Correlation Scenarios, page 6-15—Describes the BGP alarms and their correlation.
- HSRP Scenarios, page 6-26—Describes the HSRP alarms and provides various examples.
- IP Interface Failure Scenarios, page 6-28—Describes the Interface Status Down alarm and its correlation. In addition, it describes the All IP Interfaces Down alarm and its correlation and provides several examples.
- GRE Tunnel Down/Up, page 6-35—Provides an overview of GRE tunneling, describes the GRE Tunnel alarm, and provides correlation examples.

Lab Setup for the Scenarios in These Topics

This section describe the lab's functionality and the applied technologies. The diagram illustrates the lab setup for the scenarios described in these topics.

Figure 6-1 Lab Setup



The lab simulates a network that is used by the service provider (SP). The core is based on MPLS technology and runs the OSPF routing protocol as Interior Gateway Protocol (IGP).

The P-network is topologically contiguous, whereas the C-network is delineated into a number of sites (contiguous parts of the customer network that are connected in some way other than through the VPN service). Note that a site does not need to be geographically contained.

The devices that link the customer sites to the P-network are called customer edge (CE) devices, whereas the service provider devices to which the CE routers connect are called provider edge (PE) devices. Where the provider manages an Ethernet access network, the CE devices will be connected to the PE devices, which are usually LAN switches with L3 capabilities.

The access network can be any L2 technology.

In this lab there are two L2 technologies in the access network:

- Ethernet
- Frame Relay

The access network in the lab is unmanaged (a cloud).

In most cases, the P-network is made up of more than just the PE routers. These other devices are called P-devices (or, if the P-network is implemented with Layer 3 technology, P-routers). Similarly, the additional Layer 3 devices at the customer sites that have no direct connectivity to the P-network are called C-routers. In this example, C-routers are not part of the lab setup and are not managed by Cisco ANA.

The CE devices are located at the customer site and can be managed by the SP. All other devices (PEs, Ps, and RRs) are located at the SP site. These devices are maintained by the SP.

An end-to-end MPLS VPN solution is, like any other VPN solution, divided into the central P-network to which a large number of customer sites (sites in the C-network) are attached. The customer sites are attached to the PE devices (PE routers) through CE devices (CE routers). Each PE router contains several virtual routing and forwarding tables (VRFs), at least one per VPN customer. These tables are used together with multiprotocol BGP to run between the PE routers to exchange customer routes and to propagate customer datagrams across the MPLS network. The PE routers perform the label imposition (ingress PE router) and removal (egress PE router). The central devices in the MPLS network (P routers) perform simple label switching.

There are BGP processes running on the PE devices, and each PE is a neighbor to both RR devices. This way, the lab has a backup if one RR is down.

All the devices are managed inband. The management access point is Ethernet 0/0 on PE-East. To enable access to the CE devices, a loop was created between two ports on PE-East.

Device Unreachable Correlation Scenarios

Device reachability is measured by management protocol connectivity. Connectivity tests are used to verify the connection between VNEs and the managed network elements. The connectivity is tested per each protocol a VNE uses to poll a device. Cisco ANA-supported protocols for connectivity tests are SNMP, Telnet and ICMP.

The following topics describe the three scenarios in which device reachability issues occur:

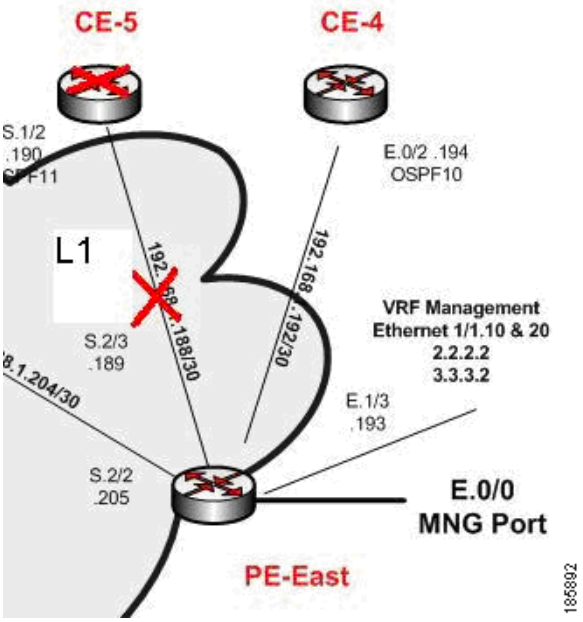
- Device Unreachable on Device Reload or Device Down Event, page 6-4
- Device Unreachable on Another Device Unreachable Event, page 6-7
- Device Unreachable on Link Down Event, page 6-10

For more information about device reachability, see Chapter 4, “Causality Correlation and Root Cause Analysis.”

Device Unreachable on Device Reload or Device Down Event

Figure 6-2 illustrates the lab setup for Device Unreachable on Device Down or Device Reload event.

Figure 6-2 Lab Setup for Device Unreachable on Device Down or Device Reload Event



Description of Fault Scenario in the Network

CE-5 goes down or is reloaded.

Related Faults

- The port S.1/2 of CE-5 operationally goes down (between CE-5 and PE-East).
- The port S.2/3 of PE-East operationally goes down (between PE-East and CE-5).
- CE-5 is unreachable from the management subnet.

Note Other related faults might occur due to the CE-5 down or reload. Syslogs and traps corresponding to network faults are also reported. Additional faults, other than for the connectivity issue of CE-5 and the Link Down with the PE-East device, might be reported but are not described in this section. This section relates specifically to Device Unreachable events.

Cisco ANA Failure Processing

Event Identification

The following service alarms are generated by the system:

- [Device Unreachable, CE-5] event. See Component Unreachable, page 16-11.

  The device unreachability event means that no other information can be collected from this device by the VNE.

- [Link Down on Unreachable, PE-East < > CE-5] event. See Link Down, page 16-22.

  The Link Down event is issued by the PE-East VNE (active) as a result of the link down negotiation process.

Possible Root Cause

1. Cisco ANA waits two minutes. For more information, see Correlation Process, page 4-3.
2. After two minutes, the following occurs:

- The [Device Unreachable, CE-5] event triggers the CE-5 VNE to initiate an IP-based flow to the management IP address:

  Flow Path: CE-5 > PE-East > management subnet

- The [Link Down on Unreachable, PE-East < > CE-5] event triggers the CE-5 VNE to initiate local correlation.

Root Cause Selection

For the event [Device Unreachable, CE-5]:

- Collected Events: [Link Down on Unreachable, PE-East < > CE-5].

  Note Collects other possible events, such as Interface Status Down events.

- Root Cause: There is no root cause (opens a new ticket in the gateway).

  Note The root cause selection process activates special filtering for the event [Device Unreachable, CE-5] for which the event [Link Down on Unreachable] cannot be selected as the root cause; therefore the event [Link Down on Unreachable, PE-East < > CE-5] will not be selected as the root cause.

For the event [Link Down on Unreachable, PE-East < > CE-5]:

- Collected Events: [Device Unreachable, CE-5].
- Root Cause: Correlates to [Device Unreachable, CE-5].

Figure 6-3 displays the events identified by the system in this scenario.

Figure 6-3 Device Unreachable on Device Down

ID	Short Description	Location	Time
59979	Device unreachable	ce-5-IOU-161	25/09/07 - 16:45:31
59978	Link down on unreachable	PE-East-IOU-161#0:Serial2/3<->ce-5-IOU-161#0:Serial1/2	25/09/07 - 16:45:24
59974	OSPF neighbor down syslog	PE-East-IOU-161 VRF vrfB IP:Serial2/3 : 169.254.161.223	25/09/07 - 16:44:48
59975	Interface status down	PE-East-IOU-161 VRF vrfB IP:Serial2/3	25/09/07 - 16:44:50
59973	Line down syslog	PE-East-IOU-161 VRF vrfB IP:Serial2/3	25/09/07 - 16:44:45

185893

Clearing Phase

When a down or reloaded device comes up again and starts responding to polling requests made by the corresponding VNE, the device is declared reachable, thus clearing the unreachable alarm. Other related alarms are cleared in turn after the corresponding VNEs verify that the malfunctions have recovered.

Variation

In a device reload scenario, the following additional events are identified by the system (in addition to the device down scenario):

- Reloading Device syslog.
- Cold Start trap.

For the event [Device Unreachable, CE-5]:

- Additional Collected Events: [Reloading Device syslog, CE-5].
- Root Cause: Correlates to [Reloading Device syslog, CE-5].

Figure 6-4 displays the events identified by the system in this scenario.

Figure 6-4 Device Unreachable on Device Reload

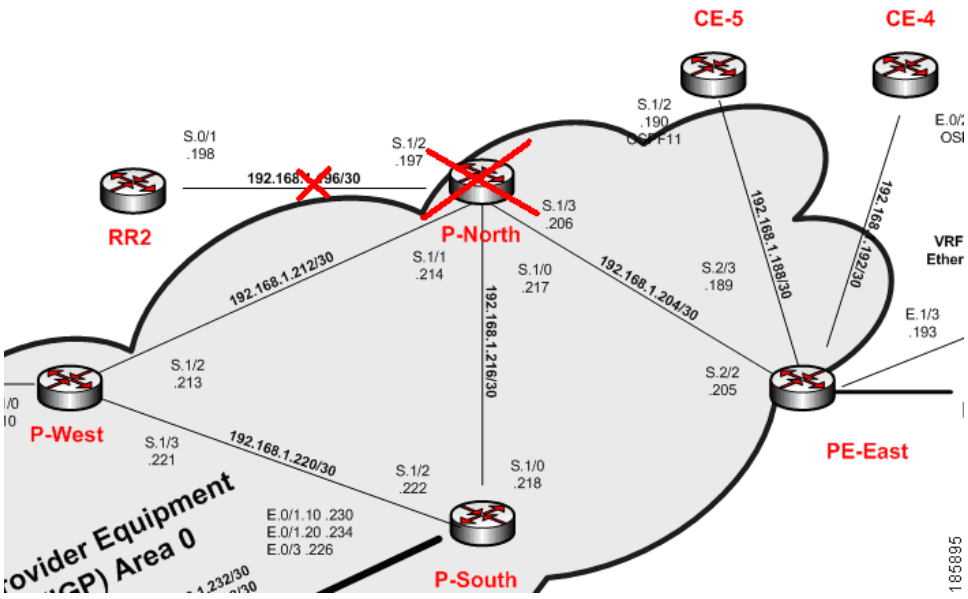
ID	Short Description	Location	Time
59989	Reloading device syslog	ce-5-IOU-161	25/09/07 - 17:17:16
59991	OSPF neighbor down syslog	PE-East-IOU-161 VRF vrfB IP:Serial2/3 : 169.254.161.223	25/09/07 - 17:17:34
59992	Interface status down	PE-East-IOU-161 VRF vrfB IP:Serial2/3	25/09/07 - 17:17:35
59993	Line down syslog	PE-East-IOU-161 VRF vrfB IP:Serial2/3	25/09/07 - 17:17:34
59994	Device unreachable	ce-5-IOU-161	25/09/07 - 17:17:56
59995	Link down on unreachable	PE-East-IOU-161#0:Serial2/3<->ce-5-IOU-161#0:Serial1/2	25/09/07 - 17:18:05

185894

Device Unreachable on Another Device Unreachable Event

Figure 6-5 illustrates the lab setup for Device Unreachable on another Device Unreachable event.

Figure 6-5 Lab Setup for Device Unreachable on Another Device Unreachable Event



Description of Fault Scenario in the Network

P-North device is reloaded.

Related Faults

- P-North is unreachable from the management subnet.
- The links of P-North operationally go down and as a result its surrounding devices go down.
- RR2, accessed by the link P-North, RR2 (also known as L3) is unreachable.

Cisco ANA Failure Processing

Note This scenario is similar to the one described in Device Unreachable on Device Reload or Device Down Event, page 6-4, except that in this scenario the L3 Link Down is *not* discovered because both connected devices (RR2 and P-North) are unreachable by Cisco ANA, and therefore the VNE is unable to detect the Link Down problem.

Event Identification

The following service alarms are generated by the system:

- [Device Unreachable, P-North] event. See Component Unreachable, page 16-11.

  The device unreachability event means that no other information can be collected from this device by the VNE.

- [Device Unreachable, RR2] event.

Possible Root Cause

1. Cisco ANA waits two minutes.
2. After two minutes, the following occurs:

- The [Device Unreachable, P-North] event triggers the P-North VNE to initiate an IP-based flow to the management IP:

  Flow Path: P-North > PE-East > management subnet

- The [Device Unreachable, RR2] event triggers the RR2 VNE to initiate an IP-based flow to the management IP.

  Flow Path: RR2 > P-North > PE-East > management subnet

Root Cause Selection

- For the event [Device Unreachable, P-North]:
  - Collected Events: [Reloading Device syslog, P-North].
  - Root Cause: Correlates to [Reloading Device syslog, P-North].
- For the event [Device Unreachable, RR2]:
  - Collected Events: [Device Unreachable, P-North] and [Reloading Device syslog, P-North].
  - Root Cause: Correlates to [Reloading Device syslog, P-North] (as this has a higher weight than the event [Device Unreachable, P-North]).

Figure 6-6 displays the events identified by the system in this scenario.

Figure 6-6 Device Unreachable on Other Device Unreachable

ID	Short Description	Location	Time
60327	Reloading device syslog	P-North-IOU-161	26/09/07 - 11:15:40
60334	LDP neighbor down	PE-East-IOU-161	26/09/07 - 11:15:51
60331	LDP neighbor down syslog	PE-East-IOU-161	26/09/07 - 11:15:40
60335	Interface status down	PE-East-IOU-161 IP:Serial2/2	26/09/07 - 11:15:58
60336	Line down syslog	PE-East-IOU-161 IP:Serial2/2	26/09/07 - 11:15:57
60337	BGP neighbor down syslog	PE-East-IOU-161 : 169.254.161.216	26/09/07 - 11:16:08
60338	BGP neighbour loss	PE-East-IOU-161	26/09/07 - 11:16:08
60339	BGP neighbor down syslog	PE-East-IOU-161 : 169.254.161.224	26/09/07 - 11:16:12
60340	Device unreachable	RR1-IOU-161	26/09/07 - 11:16:14
60341	Device unreachable	P-West-IOU-161	26/09/07 - 11:16:16
60347	Device unreachable	ce-1-IOU-161	26/09/07 - 11:16:34
60349	Device unreachable	RR2-IOU-161	26/09/07 - 11:16:38
60350	Device unreachable	PE-South-IOU-161	26/09/07 - 11:16:45
60351	Device unreachable	P-South-IOU-161	26/09/07 - 11:16:46
60352	Device unreachable	P-North-IOU-161	26/09/07 - 11:16:48
60348	Link down on unreachable	P-North-IOU-161#0:Serial1/3<->PE-East-IOU-161#0:Serial2/2	26/09/07 - 11:16:29
60354	LDP neighbor down	PE-East-IOU-161	26/09/07 - 11:17:24
60353	LDP neighbor down syslog	PE-East-IOU-161	26/09/07 - 11:17:14

185896

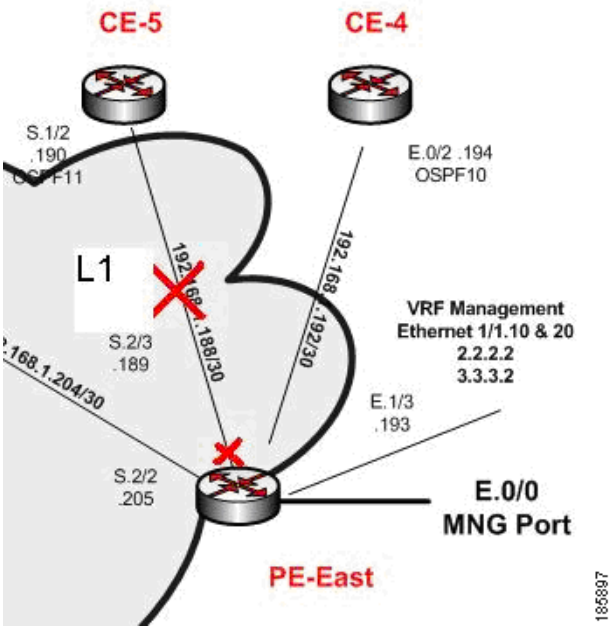
Clearing Phase

When a reloaded device comes up again (along with the L3 link that is vital for the RR2 management), the RR2 starts responding to polling requests from the RR2 VNE. The device is declared as reachable, thus clearing the Device Unreachable alarm.

Device Unreachable on Link Down Event

Figure 6-7 illustrates the lab setup for a Device Unreachable on a Link Down event.

Figure 6-7 Lab Setup for Device Unreachable on a Link Down Event



Description of Fault Scenario in the Network

The S.2/3 port of PE-East connected to the S.1/2 port of the CE-5 device (also called L1 link) is set to administrative status down. This effectively takes the L1 Link Down.

Related Faults

The CE-5 device is managed from this link with no backup. The L1 Link Down renders the CE-5 Device Unreachable from the management subnet.

Cisco ANA Failure Processing

Event Identification

The following service alarms are generated by the system:

- [Device Unreachable, CE-5] event. See Component Unreachable, page 16-11.

  The device unreachability event means that no other information can be collected from this device by the VNE.

- [Link Down Due to Admin Down, PE-East < > CE-5] event. See Link Down, page 16-22.

  The Link Down event is issued by the PE-East VNE (active) as a result of the Link Down negotiation process.

Noncorrelating Events

The noncorrelating event is:

[Link Down Due to Admin Down, PE-East < > CE-5]

This event opens a new ticket in the gateway.

The L1 Link Down event is configured to not correlate to other events at all. This is logical, because the edge VNEs identify the Link Down events as [Link Down Due to Admin Down] events. This implies that the VNEs know the root cause of the event already, based on the administrator's configurations. The [Link Down Due to Admin Down] events reach the northbound interface immediately after the links' new statuses are discovered by Cisco ANA and after the link down negotiation methods are completed.

Possible Root Cause

1. Cisco ANA waits two minutes.
2. After two minutes, the [Device Unreachable, CE-5] event triggers the CE-5 VNE to initiate an IP-based flow to the management IP:

   Flow Path: CE-5 > PE-East > management subnet

Root Cause Selection

For the event [Device Unreachable, CE-5]:

- Collected Events: [Link Down Due to Admin Down, PE-East < > CE-5].

Note Collects other possible events, for example, Interface Status Down events.

- Root Cause: Correlates to [Link Down Due to Admin Down, PE-East < > CE-5].

Figure 6-8 displays the events identified by the system in this scenario.

Figure 6-8 Device Unreachable on Link Down

ID	Short Description	Location	Time
59152	Link down due to admin down	PE-East-IOU-161#0:Ethernet0/3<->ce-5-IOU-161#0:Ethernet0/2	25/09/07 - 09:31:53
59158	OSPF neighbor down syslog	PE-East-IOU-161 VRF vrfB IP:Ethernet0/3 : 169.254.161.223	25/09/07 - 09:31:20
59159	Interface status down	OSPF neighbor down syslog 161 VRF vrfB IP:Ethernet0/3	25/09/07 - 09:31:22
59160	Link down syslog	PE-East-IOU-161 VRF vrfB IP:Ethernet0/3	25/09/07 - 09:31:22
59161	Line down syslog	PE-East-IOU-161 VRF vrfB IP:Ethernet0/3	25/09/07 - 09:31:22
59162	Device unreachable	ce-5-IOU-161	25/09/07 - 09:32:02

185898

Note In Figure 6-8 port E.0/3 should read S.2/3 and E.0/2 should read S.1/2.

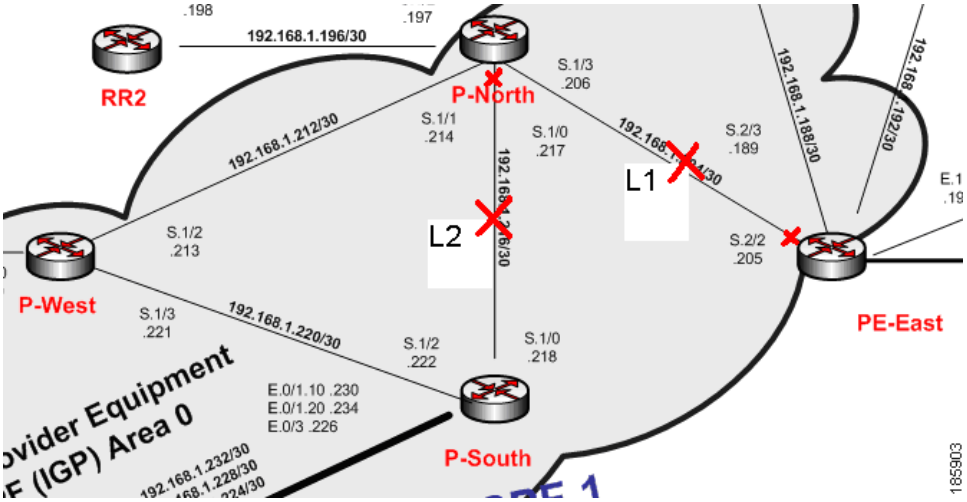
Clearing Phase

When the PE-East port S.2/3 (L1 link) comes up again, the CE-5 reachability from the management subnet comes back too. The CE-5 starts responding to polling requests from the CE-5 VNE. The device is declared reachable, thus clearing the Device Unreachable alarm. The L1 Link Down is cleared when the PE-East device indicates that the status of the connected port has changed to up again.

Multiroute Correlation Scenarios

Figure 6-9 displays the lab multiroute configuration setup between P-South, P-North and P-West devices. The Open Shortest Path First (OSPF) cost is the same along the path from P-South and P-North whether or not it goes via P-West; that is, P-South and P-North connect along two paths with equal cost.

Figure 6-9 Lab Multiroute Configuration Setup Between P-South, P-North and P-West



Description of Fault Scenario in the Network

In this example, the P-North, P-South link (also known as L2) goes down in a multiroute segment between P-South and P-North. After approximately one minute another link, L1 (PE-East, P-North), goes down too. Both links go down administratively, the first from the P-North device and the latter from the PE-East devices' ports.

Related Faults

Almost all the devices are unreachable from the management subnet. This section focuses on CE-1 unreachability (see Figure 6-1).

Note Syslogs and traps corresponding to network faults are also reported. Additional related faults might also be reported, but are not described in this section.

Cisco ANA Failure Processing

Event Identification

The following service alarms are generated by the system:

- [Device Unreachable, CE-1] event. See Component Unreachable, page 16-11.

  The device unreachability event means that no other information can be collected from this device by the VNE.

- [Link Down Due to Admin Down, P-North < > PE-East] event. See Link Down, page 16-22.

  The Link Down event is issued by the PE-East VNE (active) as a result of the link down negotiation process.

- [Link Down Due to Admin Down, P-North < > P-South] event.

  The Link Down event is issued by the P-North VNE as a result of the link down negotiation process.

Noncorrelating Events

- [Link Down Due to Admin Down, P-North < > PE-East] opens a new ticket in the gateway.
- [Link Down Due to Admin Down, P-North < > P-South] opens a new ticket in the gateway.

For more information, see Noncorrelating Events, page 6-11.

Possible Root Cause

1. Cisco ANA waits two minutes.
2. After two minutes, the [Device Unreachable, CE-1] event triggers the CE-1 VNE to initiate an IP-based flow to the management IP:

   Flow Path: CE-1 >Cloud > PE-South > P-South > P-North > PE-East > management subnet

   Flow Path: CE-1 >Cloud > PE-South > P-South > P-West > P-North > PE-East > management subnet

Root Cause Selection

For the event [Device unreachable, CE-1]:

- For the flow path: CE-1 > Cloud > PE-South > P-South > P-North > PE-East > management subnet:
  - Collected Events: [Link Down Due to Admin Down, P-North < > PE-East] and [Link Down Due to Admin Down, P-South > P-North].

    Note Collects other possible events, for example, Interface Status Down events.

  - Root Cause: Correlates to:
    [Link down due to admin down, P-SouthS.1/0 > P-North S.1/0 < > PE-East S.2/2] and
    [Link down due to admin down, P-NorthS.1/3 > PE-East S.2/2]
- For the Flow Path
  CE-1 > Cloud > PE-South > P-South > P-West > P-North > PE-East > management subnet:

  Root Cause: Correlates to [Link Down Due to Admin Down, P-North S.1/0 < > PE-East S.2/2]

Note The CE-1's VNE root cause selection method identifies the Device Unreachable event's root cause on the L1 Link Down event. According to the logic two flows that split and come up with two sets of possible root cause events, remove sets that are super sets of others (depending on whether both flows end at the same location). Sets that are not removed are united into one set containing all of the events. This implies that in this scenario, the set that includes both links is removed because it is a super set of the set that contains only the L1 link.

Note All devices that are unreachable correlate their unreachability events to the L1 link as expected.

Figure 6-10 displays the events identified by the system in this scenario (L1).

Figure 6-10 Multiroute Scenario—L1

ID	Short Description	Location	Time
61493	Link down due to admin down	P-North-IOU-161#0:Serial1/3<->PE-East-IOU-161#0:Serial2/2	30/09/07 - 13:07:07
61508	Interface status down	PE-East-IOU-161 IP:Serial2/2	30/09/07 - 13:06:36
61510	Link down syslog	PE-East-IOU-161 IP:Serial2/2	30/09/07 - 13:06:36
61511	Line down syslog	PE-East-IOU-161 IP:Serial2/2	30/09/07 - 13:06:37
61512	LDP neighbor down	PE-East-IOU-161	30/09/07 - 13:06:47
61509	LDP neighbor down syslog	PE-East-IOU-161	30/09/07 - 13:06:36
61513	BGP neighbor down syslog	PE-East-IOU-161 : 169.254.161.224	30/09/07 - 13:06:59
61514	BGP neighbour loss	PE-East-IOU-161	30/09/07 - 13:06:59
61515	BGP neighbor down syslog	PE-East-IOU-161 : 169.254.161.216	30/09/07 - 13:07:01
61516	Device unreachable	ce-3-IOU-161	30/09/07 - 13:07:07
61518	Device unreachable	ce-1-IOU-161	30/09/07 - 13:07:17
61519	Device unreachable	ce-2-IOU-161	30/09/07 - 13:07:20
61522	Device unreachable	PE-South-IOU-161	30/09/07 - 13:07:27
61523	Device unreachable	RR1-IOU-161	30/09/07 - 13:07:34
61524	Device unreachable	P-West-IOU-161	30/09/07 - 13:07:34
61526	Device unreachable	P-South-IOU-161	30/09/07 - 13:07:35
61525	Device unreachable	P-North-IOU-161	30/09/07 - 13:07:35
61527	Device unreachable	RR2-IOU-161	30/09/07 - 13:07:36
61530	LDP neighbor down	PE-East-IOU-161	30/09/07 - 13:08:14
61529	LDP neighbor down syslog	PE-East-IOU-161	30/09/07 - 13:08:03

185904

Figure 6-11 displays the events identified by the system in this scenario (L2).

Figure 6-11 Multiroute Scenario—L2

ID	Short Description	Location	Time
61491	Link down due to admin down	P-North-IOU-161#0:Serial1/0<->P-South-IOU-161#0:Serial1/0	30/09/07 - 13:05:31
61496	Interface status down	P-North-IOU-161 IP:Serial1/0	30/09/07 - 13:05:31
61495	OSPF neighbor down syslog	P-North-IOU-161 IP:Serial1/0 : 169.254.161.214	30/09/07 - 13:05:28
61499	Link down syslog	P-North-IOU-161 IP:Serial1/0	30/09/07 - 13:05:30
61500	Line down syslog	P-North-IOU-161 IP:Serial1/0	30/09/07 - 13:05:31
61501	OSPF neighbor down syslog	P-South-IOU-161 IP:Serial1/0 : 169.254.161.213	30/09/07 - 13:05:40
61502	Interface status down	P-South-IOU-161 IP:Serial1/0	30/09/07 - 13:05:40
61503	Line down syslog	P-South-IOU-161 IP:Serial1/0	30/09/07 - 13:05:40
61504	LDP neighbor down	P-North-IOU-161	30/09/07 - 13:05:41
61498	LDP neighbor down syslog	P-North-IOU-161	30/09/07 - 13:05:31
61507	LDP neighbor down	P-South-IOU-161	30/09/07 - 13:05:42
61497	LDP neighbor down syslog	P-South-IOU-161	30/09/07 - 13:05:30

185905

Clearing Phase

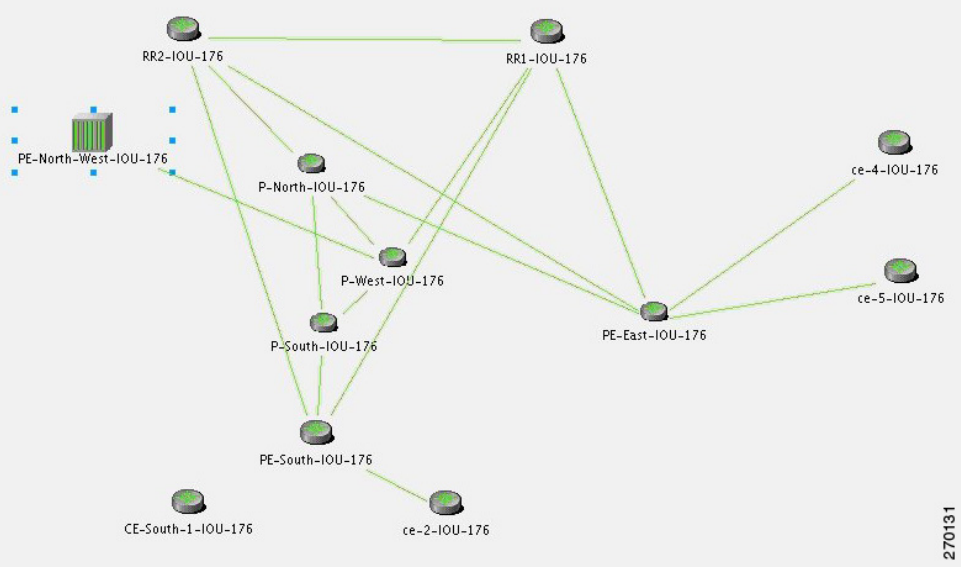
Enabling the L1 link makes the CE-1 device reachable from the management IP. This alone clears the Device Unreachable event of the CE-1 device. When the L1 link's new status is discovered by Cisco ANA, the PE-East device eventually initiates a Link Up event for this link. When the administrator enables the L2 link and Cisco ANA discovers this change, this Link Down event is cleared by its matching Link Up event.

BGP Neighbor Loss Correlation Scenarios

The VNE models the BGP connection between routers and actively monitors its state. BGP neighbor loss events are generated from both sides of the connection only in the case of a connectivity loss, and where the other side of the link is unmanaged.

The correlation engine identifies various faults that affect the BGP connection and reports them as the root cause for the BGP Neighbor Loss alarm; for example, Link Down, CPU Overutilized, and Link Data Loss.

Figure 6-12 Lab Setup for BGP Neighbor Loss Correlation Scenarios



Note In Figure 6-12 the link between P-West and PE-North-West is not real and merely emphasizes how PE-North-West is connected in the network.

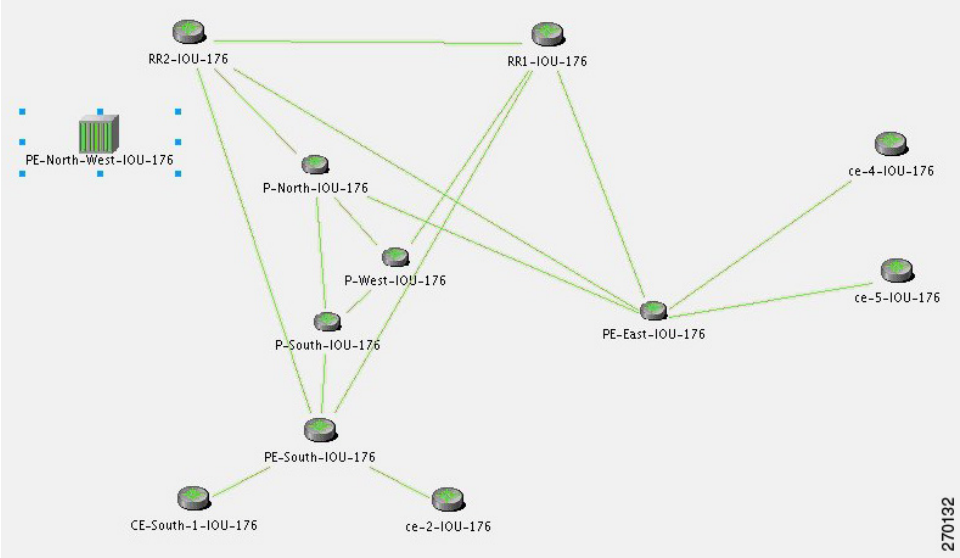
There are two main scenarios that might lead to a BGP neighbor loss event:

- BGP neighbor loss due to a Link Down (or an equivalent port down).
- BGP neighbor loss due to BGP Process Down or device down.

BGP Neighbor Loss Due to Port Down

Figure 6-13 displays the BGP neighbor loss due to port down scenario.

Figure 6-13 BGP Neighbor Loss Due to Physical Port Down (P-West > PE-North-West)



Description of Fault Scenario in the Network

In Figure 6-13 the BGP neighbor loss occurs due to a physical port down (in P-West that connects to PE-North-West). The relevant devices are PE-North-West, RR2, P-North and P-West.

Related Faults

- Port on P-West that is connected to the PE-North-West goes down.
- BGP neighbor, on RR2, to PE-North-West changes state from Established to Idle.

Note Syslogs and traps corresponding to network faults are also reported. Additional related faults might also be reported, but are not described in this section.

Cisco ANA Failure Processing

Event Identification

The following service alarms are generated by the system:

- [BGP Neighbor Loss, RR2] event. See BGP Neighbor Loss, page 16-5.

  Since the VNE that monitors each PE or RR holds records of the entire device's BGP information, the change in the BGP table is identified by the VNE and causes it to send this event.

Possible Root Cause

1. Cisco ANA waits two minutes. For more information, see Correlation Process, page 4-3.
2. After two minutes, the [BGP Neighbor Loss, RR2] event triggers the VNE to initiate an IP-based flow to the destination IP of its lost BGP neighbor (PE-North-West):

   Flow Path: RR2 > P-North > P-West > P-West port is connected to PE-North-West (which is unmanaged), and is in a down state.

Root Cause Selection

For the event [BGP Neighbor Loss, RR2]:

- Collected Events: [Port Down, P-West].
- Root Cause: Correlates to [Port Down, P-West].

Figure 6-14 displays the events identified by the system in this scenario.

Figure 6-14 BGP Neighbor Loss Due to Physical Port Down

ID	Short Description	Location	Time	Last Modification Time
51552	Port down	P-West-IOU-176#0:Serial...	12/6/07 - 18:11:59	12/6/07 - 18:11:59
51556	OSPF neighbor down syslog	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:56	12/6/07 - 18:11:56
51561	Interface status down	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:59	12/6/07 - 18:11:59
5155	Link down syslog	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:58	12/6/07 - 18:11:58
5156	Line down syslog	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:59	12/6/07 - 18:11:59
5156	Line down trap	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:59	12/6/07 - 18:11:59
51565	LDP neighbor down	P-West-IOU-176	12/6/07 - 18:12:10	12/6/07 - 18:12:10
5156	LDP neighbor down syslog	P-West-IOU-176	12/6/07 - 18:11:59	12/6/07 - 18:11:59
51566	BGP neighbor down syslog	RR2-IOU-176 : 169.254....	12/6/07 - 18:12:18	12/6/07 - 18:12:18
51567	BGP neighbour loss	RR2-IOU-176	12/6/07 - 18:12:19	12/6/07 - 18:12:19
51569	BGP neighbor down syslog	RR1-IOU-176 : 169.254....	12/6/07 - 18:12:25	12/6/07 - 18:12:25
51570	BGP neighbour loss	RR1-IOU-176	12/6/07 - 18:12:26	12/6/07 - 18:12:26

270133

Clearing Phase

When a Port Up event is detected by the system for the same port that was detected as the root cause for the BGP Neighbor Loss event, the alarm is cleared. The ticket is cleared (colored green) when all the alarms in the ticket have been cleared.

Figure 6-15 displays the up event that clears all the down events identified by the system.

Figure 6-15 BGP Neighbor Up Event that Clears All the Down Events

ID	Short Description	Location	Time	Last Modification Time
51552	Port up	P-West-IOU-176#0:Serial...	12/6/07 - 18:11:59	12/6/07 - 18:23:13
51556	OSPF neighbor up syslog	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:56	12/6/07 - 18:23:22
51561	Interface status up	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:59	12/6/07 - 18:23:13
5155	Link up syslog	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:58	12/6/07 - 18:23:12
5156	Line up syslog	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:59	12/6/07 - 18:23:12
5156	Line down trap	P-West-IOU-176 IP:Serial...	12/6/07 - 18:11:59	12/6/07 - 18:11:59
51565	LDP neighbor up	P-West-IOU-176	12/6/07 - 18:12:10	12/6/07 - 18:23:40
5156	LDP neighbor up syslog	P-West-IOU-176	12/6/07 - 18:11:59	12/6/07 - 18:23:28
51566	BGP neighbor up syslog	RR2-IOU-176 : 169.254....	12/6/07 - 18:12:18	12/6/07 - 18:23:38
51567	BGP neighbour found	RR2-IOU-176	12/6/07 - 18:12:19	12/6/07 - 18:23:39
51569	BGP neighbor up syslog	RR1-IOU-176 : 169.254....	12/6/07 - 18:12:25	12/6/07 - 18:23:44
51570	BGP neighbour found	RR1-IOU-176	12/6/07 - 18:12:26	12/6/07 - 18:23:45

270134

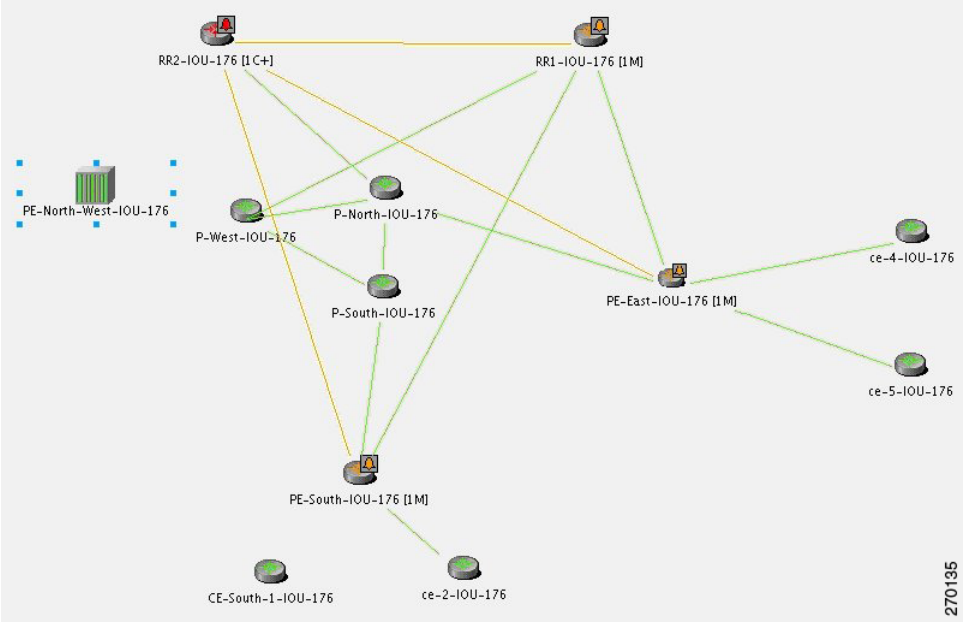
Variation

In a BGP process down scenario, the following additional events are identified by the system (in addition to the BGP Neighbor Loss event):

- [BGP Process Down]. See BGP Process Down, page 16-6.

In Figure 6-16 the BGP Process Down event causes several events (the BGP Neighbor Loss event cannot be seen). The relevant devices are RR2 (BGP Process Down, marked in red), and PE-North-West (marked as unmanaged).

Figure 6-16 BGP Process Down Causes Several Events



For the event [BGP Neighbor Loss, RR2]:

- Additional Collected Events: [BGP Process Down, RR2], [BGP Neighbor Loss, RR2].
- Root cause: Correlates to [BGP Process Down, RR2].

Figure 6-17 displays the events identified by the system in this scenario.

Figure 6-17 BGP Process Down Correlation

ID	Short Description	Location	Time	Last Modification Time	Reductic
51878	BGP process down	RR2-IOU-176	12/9/07 - 11:50:31	12/9/07 - 11:50:31	1
51879	BGP neighbor down syslog	RR2-IOU-176 : 169.254....	12/9/07 - 11:50:31	12/9/07 - 11:50:31	1
51881	BGP neighbor down syslog	RR2-IOU-176 : 169.254....	12/9/07 - 11:50:31	12/9/07 - 11:50:31	1
51880	BGP neighbor down syslog	RR1-IOU-176 : 169.254....	12/9/07 - 11:50:31	12/9/07 - 11:50:31	1
51883	BGP neighbor down syslog	PE-South-IOU-176 : 169....	12/9/07 - 11:50:31	12/9/07 - 11:50:31	1
51882	BGP neighbor down syslog	RR2-IOU-176 : 169.254....	12/9/07 - 11:50:31	12/9/07 - 11:50:31	1
51884	BGP neighbor down syslog	PE-East-IOU-176 : 169.2..	12/9/07 - 11:50:32	12/9/07 - 11:50:32	1
51885	BGP neighbor down syslog	RR2-IOU-176 : 169.254....	12/9/07 - 11:50:32	12/9/07 - 11:50:32	1
51887	BGP link down	PE-East-IOU-176<->RR..	12/9/07 - 11:50:32	12/9/07 - 11:50:32	1
51889	BGP link down	PE-South-IOU-176<->R..	12/9/07 - 11:50:32	12/9/07 - 11:50:32	1
51888	BGP link down	RR1-IOU-176<->RR2-I...	12/9/07 - 11:50:32	12/9/07 - 11:50:32	1
51886	BGP neighbour loss	RR2-IOU-176	12/9/07 - 11:50:32	12/9/07 - 11:50:32	1

270136

BGP Link Down Scenarios

Figure 6-18 illustrates the lab setup for the BGP Link Down scenarios described in this topic.

Figure 6-18 Lab Setup for BGP Link Down Scenarios

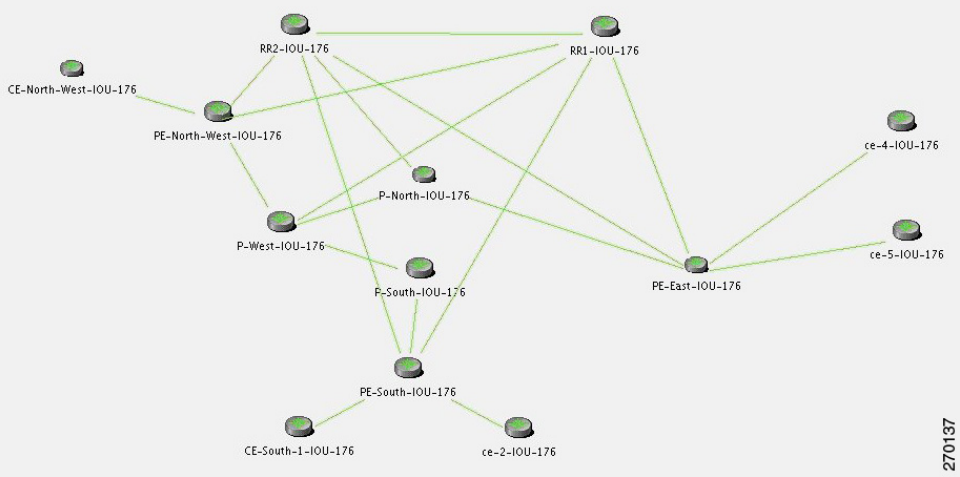
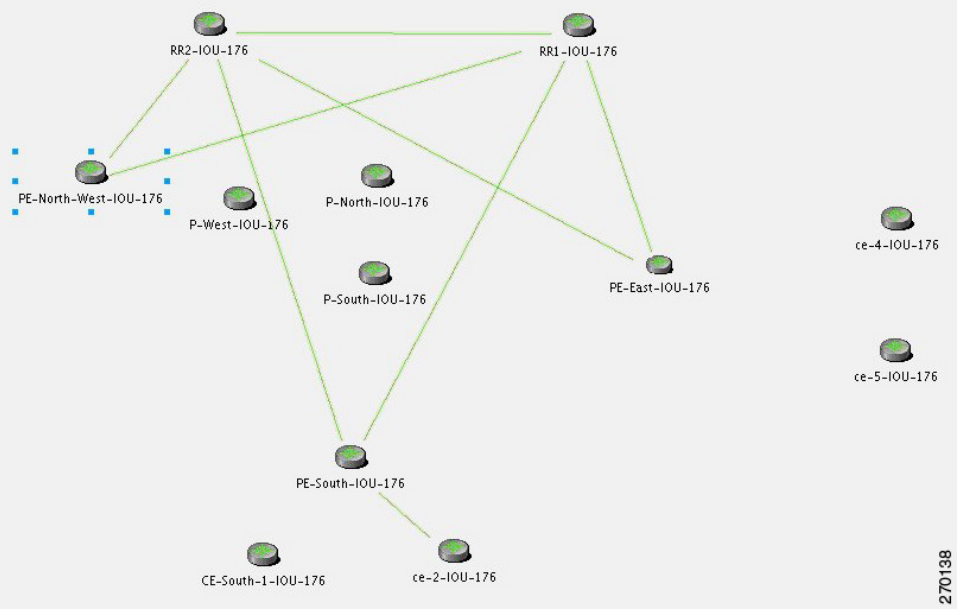


Figure 6-19 illustrates the lab setup for the scenarios with only the BGP links displayed.

Figure 6-19 Lab Setup for Scenarios With Only the BGP Links Displayed



The VNE models the BGP connection between routers and actively monitors its state. If the connectivity is lost and a link between the devices exists in the VNE, a BGP Link Down event is created. A BGP Link Down event is created only if both sides of the link are managed.

A BGP link might be disconnected in the following scenarios:

- The BGP process on a certain device goes down, causing all the BGP links that were connected to that device to disconnect.
- Disconnection of a physical link (path) that causes one side of the logical BGP link to become unreachable.
- A device that becomes unreachable, due to reload or because it is shutting down. This causes all the links to the device to be lost, including the BGP links.

Description of Fault Scenario in the Network

Due to a physical link down, the BGP connection between PE-North-West and RR2 is lost.

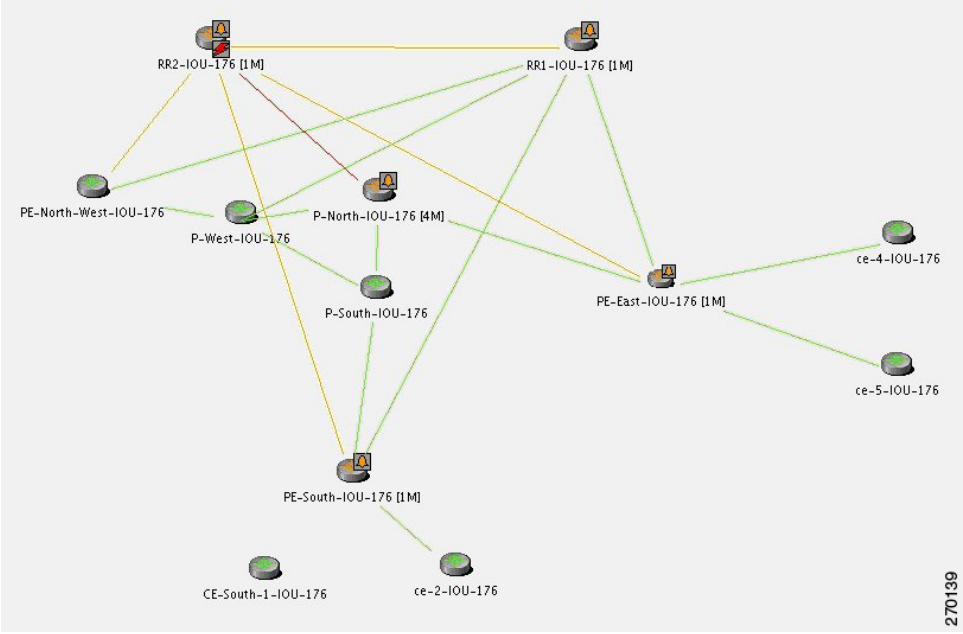
Related Faults

- Port that is connected to the P-North goes down.
- Port that is connected to the RR2 goes down.
- BGP link between RR2 and PE-North-West is disconnected.

Note Syslogs and traps corresponding to network faults are also reported. Additional related faults might also be reported, but are not described in this section.

Figure 6-20 reflects the BGP Link Down due to physical link down scenario. The relevant devices are RR2, P-north, P-West and PE-North-West.

Figure 6-20 BGP Link Down Due to Physical Link Down



Cisco ANA Failure Processing

Event Identification

The following service alarms are generated by the system:

- [BGP Link Down, RR2 < > PE-North-West] event. See BGP Link Down, page 16-4. This event might be revealed in one of two ways:
  - Changes in the BGP neighbor list in the device are found after polling
  - Syslogs suggest that something has changed in the device's BGP neighbors or process

  This causes an acceleration of the polling for the BGP neighbor data on the device.

Possible Root Cause

1. Cisco ANA waits two minutes. For more information, see Correlation Process, page 4-3.
2. After two minutes, the [BGP Link Down, RR2 < > PE-North-West] event triggers the RR2 VNE to initiate two IP-based flows one from its routing entity to the destination IP of its lost BGP neighbor: PE-North-West, and one from the destination IP address of its lost BGP neighbor back to the RR2:

   Flow Path: RR > P-North > PE-North-West

   Flow Path: RR > PE-North-West > P-North > RR2

Root Cause Selection

For the event [BGP Link Down, RR2 < > PE-North-West]:

- Collected Events: [Link Down, P-North < > RR2] and [BGP Link Down, RR2 < > PE-North-West].
- Root Cause: Correlates to [Link Down, P-North < > RR2].

Figure 6-21 displays the events identified by the system in this scenario.

Figure 6-21 BGP Link Down Correlation to the Root Cause of Physical Link Down

ID	Short Description	Location	Time	Last Modification Time
52140	Link down due to admin down	P-North-IOU-176#0:Seri...	12/9/07 - 14:23:52	12/9/07 - 14:23:52
52142	OSPF neighbor down syslog	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:20	12/9/07 - 14:23:20
52143	Interface status down	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:22	12/9/07 - 14:23:22
5214	Link down syslog	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:22	12/9/07 - 14:23:22
5214	Line down syslog	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:22	12/9/07 - 14:23:22
5214	Line down trap	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:22	12/9/07 - 14:23:22
52150	BGP neighbor down syslog	PE-South-IOU-176 : 169...	12/9/07 - 14:23:46	12/9/07 - 14:23:46
52166	BGP link down	PE-South-IOU-176<->R...	12/9/07 - 14:23:47	12/9/07 - 14:23:47
52151	BGP neighbor down syslog	RR1-IOU-176 : 169.254....	12/9/07 - 14:23:47	12/9/07 - 14:23:47
52152	BGP neighbor down syslog	PE-East-IOU-176 : 169.2...	12/9/07 - 14:23:47	12/9/07 - 14:23:47
52167	BGP link down	PE-East-IOU-176<->RR...	12/9/07 - 14:23:48	12/9/07 - 14:23:48
52168	BGP link down	RR1-IOU-176<->RR2-I...	12/9/07 - 14:23:49	12/9/07 - 14:23:49
52161	Device unreachable	RR2-IOU-176	12/9/07 - 14:23:50	12/9/07 - 14:23:50
52171	BGP link down	PE-North-West-IOU-176...	12/9/07 - 14:26:16	12/9/07 - 14:26:16

270140

Clearing Phase

A BGP Link Up event arrives when the root cause event is fixed so that the network is repaired. This clearing event is created after a clearing syslog arrives or after the next polling result reestablishes the BGP connection.

Figure 6-22 displays the up event that clears all the tickets identified by the system.

Figure 6-22 BGP Link Up Clears All the Tickets

ID	Short Description	Location	Time	Last Modification Time
52140	Link up	P-North-IOU-176#0:Seri...	12/9/07 - 14:23:52	12/9/07 - 14:35:46
52142	OSPF neighbor up syslog	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:20	12/9/07 - 14:35:55
52143	Interface status up	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:22	12/9/07 - 14:35:45
5214	Link up syslog	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:22	12/9/07 - 14:35:44
5214	Line up syslog	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:22	12/9/07 - 14:35:45
5214	Line down trap	P-North-IOU-176 IP:Seri...	12/9/07 - 14:23:22	12/9/07 - 14:23:22
52150	BGP neighbor up syslog	PE-South-IOU-176 : 169....	12/9/07 - 14:23:46	12/9/07 - 14:36:04
52166	BGP link up	PE-South-IOU-176<->R...	12/9/07 - 14:23:47	12/9/07 - 14:36:05
52151	BGP neighbor up syslog	RR1-IOU-176 : 169.254....	12/9/07 - 14:23:47	12/9/07 - 14:36:17
52152	BGP neighbor up syslog	PE-East-IOU-176 : 169.2...	12/9/07 - 14:23:47	12/9/07 - 14:36:00
52167	BGP link up	PE-East-IOU-176<->RR...	12/9/07 - 14:23:48	12/9/07 - 14:36:01
52168	BGP link up	RR1-IOU-176<->RR2-I...	12/9/07 - 14:23:49	12/9/07 - 14:36:18
52161	Device reachable	RR2-IOU-176	12/9/07 - 14:23:50	12/9/07 - 14:36:20
52171	BGP link up	PE-North-West-IOU-176...	12/9/07 - 14:26:16	12/9/07 - 14:41:16

270141

Variation

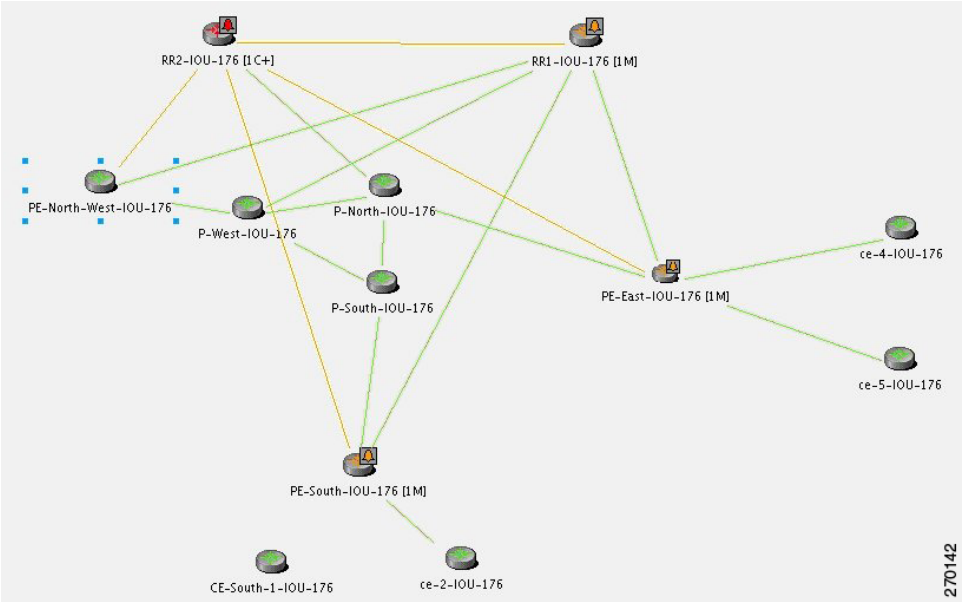
In a managed network, the following additional events might be identified by the system (in addition to the BGP Link Down event):

- BGP Process Down. See BGP Process Down, page 6-22.
- Device Unreachable. See Device Unreachable, page 6-23.

BGP Process Down

Figure 6-23 displays the scenario where a BGP Process Down event causes BGP Link Down events.

Figure 6-23 BGP Process Down Causes BGP Link Down Events



For the event [BGP Link Down, RR2 < > PE-North-West]:

- Additional Collected Events: [BGP Process Down, RR2]. See BGP Process Down, page 16-6.
- Root cause: Correlates to the event [BGP Process Down, RR2].

Figure 6-24 displays the events identified by the system in this scenario.

Figure 6-24 BGP Process Down Correlation

ID	Short Description	Location	Time	Last Modification Time
52896	BGP process down	RR2-IOU-176	12/10/07 - 18:01:41	12/10/07 - 18:01:41
52899	BGP neighbor down syslog	RR2-IOU-176 : 169.254....	12/10/07 - 18:01:41	12/10/07 - 18:01:41
52900	BGP neighbor down syslog	RR2-IOU-176 : 169.254....	12/10/07 - 18:01:41	12/10/07 - 18:01:41
53001	BGP neighbor down syslog	RR2-IOU-176 : 169.254....	12/10/07 - 18:01:41	12/10/07 - 18:01:41
53002	BGP neighbor down syslog	PE-East-IOU-176 : 169.2...	12/10/07 - 18:01:42	12/10/07 - 18:01:42
53003	BGP neighbor down syslog	RR2-IOU-176 : 169.254....	12/10/07 - 18:01:42	12/10/07 - 18:01:42
53004	BGP link down	PE-East-IOU-176<->RR...	12/10/07 - 18:01:42	12/10/07 - 18:01:42
53005	BGP link down	PE-South-IOU-176<->R...	12/10/07 - 18:01:42	12/10/07 - 18:01:42
53007	BGP link down	RR1-IOU-176<->RR2-I...	12/10/07 - 18:01:42	12/10/07 - 18:01:42
53031	BGP link down	PE-North-West-IOU-176...	12/10/07 - 18:01:42	12/10/07 - 18:01:42
53008	BGP neighbor down syslog	PE-South-IOU-176 : 169...	12/10/07 - 18:01:42	12/10/07 - 18:01:42
53006	BGP neighbor down syslog	RR1-IOU-176 : 169.254....	12/10/07 - 18:01:42	12/10/07 - 18:01:42

270143

Device Unreachable

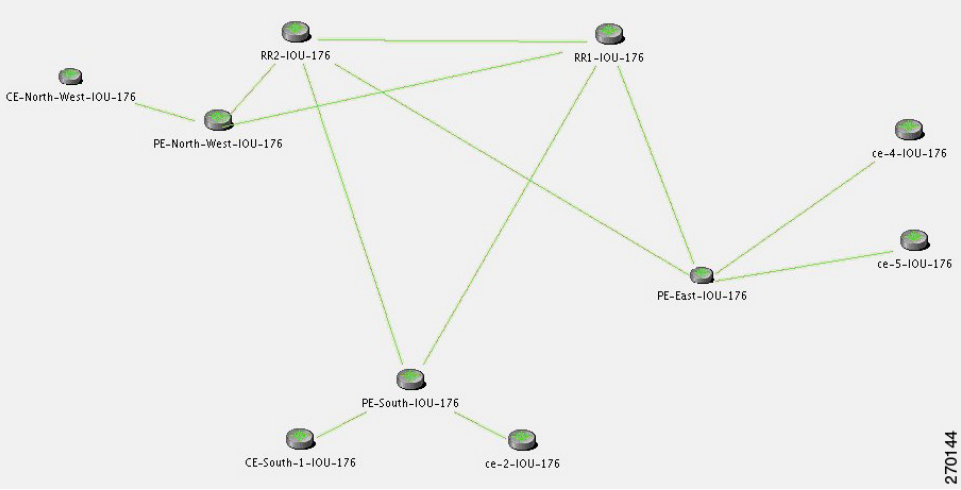
For the event [BGP Link Down, RR2 < > PE-North-West]:

- Additional Collected Events: [Device Unreachable, RR2].
- Root cause: Correlates to [Device Unreachable, RR2].

In an unmanaged network core (as illustrated in Figure 6-25), the following additional events might be identified by the system (in addition to the BGP Link Down event):

- BGP Process Down. See BGP Process Down, page 6-22.
- Device Unreachable. See Device Unreachable, page 6-23.

Figure 6-25 Lab Setup With Unmanaged Network Core

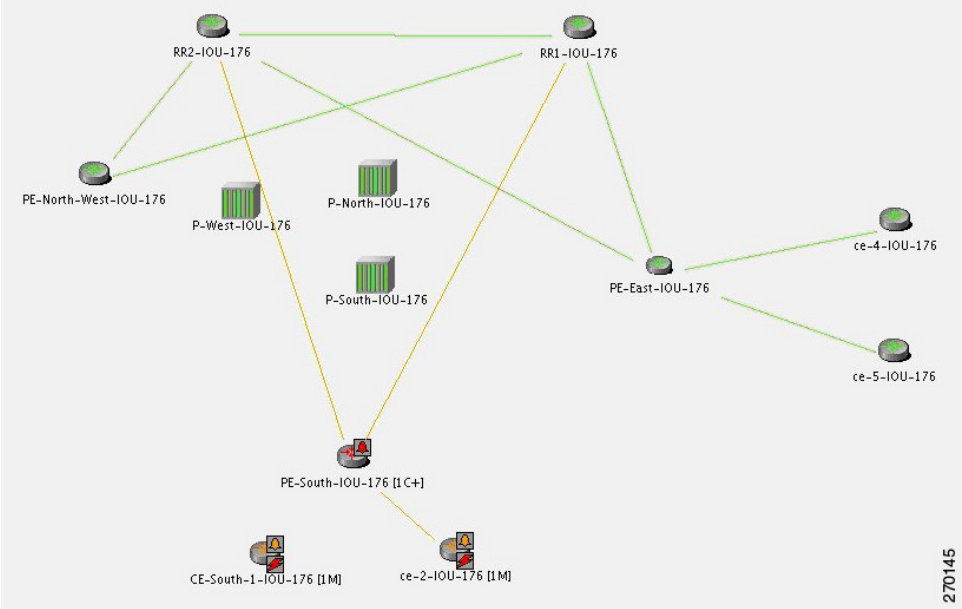


BGP Process Down

Note The BGP Process Down event occurs on the managed PE-South.

In Figure 6-26, BGP Process Down event on PE-South causes BGP Link Down events. The relevant devices are PE-South, RR1 and RR2.

Figure 6-26 BGP Process Down on PE-South Causes BGP Link Down Events



For the event [BGP Link Down, PE-South < > RR2] (see BGP Link Down, page 16-4):

- Additional Collected Events: [BGP Process Down, PE-South] and [BGP Link Down, PE-South < > RR1].
- Root cause: Correlates to [BGP Process Down, PE-South].

Figure 6-27 displays the events identified by the system in this scenario.

Figure 6-27 BGP Process Down Correlation

ID	Short Description	Location	Time
52738	BGP process down	PE-South-IOU-176	12/9/07 - 17:45:34
52739	BGP neighbor down syslog	PE-South-IOU-176 : 169.254.176.216	12/9/07 - 17:45:34
52742	BGP neighbor down syslog	PE-South-IOU-176 : 169.254.176.224	12/9/07 - 17:45:34
52743	BGP link down	PE-South-IOU-176<->RR2-IOU-176	12/9/07 - 17:45:35
52778	BGP link down vrf	PE-South-IOU-176<->ce-2-IOU-176	12/9/07 - 17:45:35
52757	BGP link down	PE-South-IOU-176<->RR1-IOU-176	12/9/07 - 17:45:36

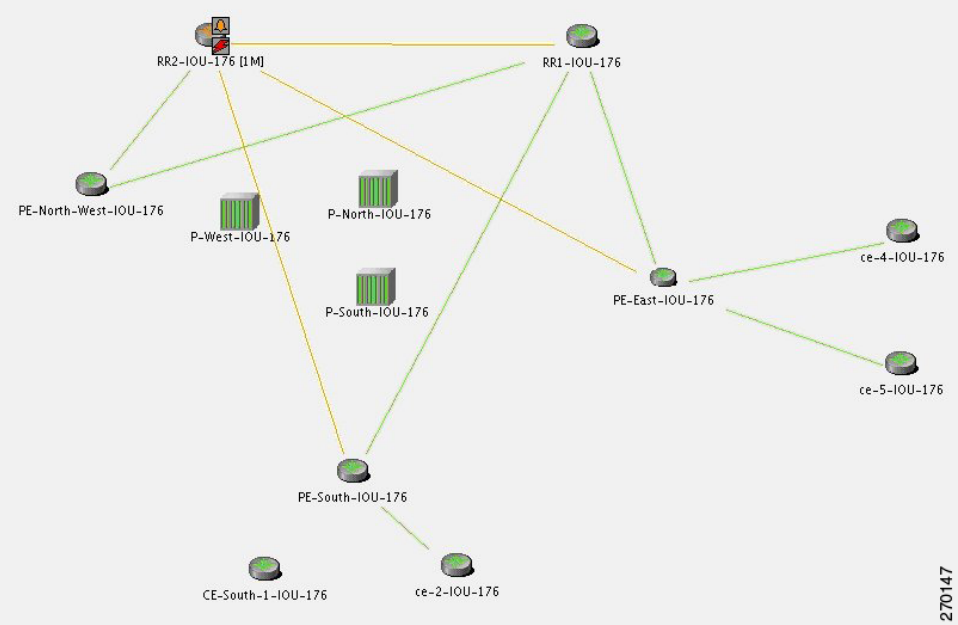
270146

Device Unreachable

For the Device Unreachable event, one or more PEs report on BGP connectivity loss to a neighbor that is unreachable.

In Figure 6-28, the Device Unreachable on an unmanaged core causes multiple BGP Link Down events. The relevant devices are RR2 (Device Unreachable), RR1, PE-East, PE-South.

Figure 6-28 Device Unreachable on Unmanaged Core Causes Multiple BGP Link Down Events



For the event [BGP Link Down, RR2 < > PE-South] (see BGP Link Down, page 16-4):

- Additional Collected Events: [Device Unreachable, RR2] and [BGP Link Down, RR2 < > RR1].
- Root cause: Correlates to [Device Unreachable, RR2].

Figure 6-29 displays the events identified by the system in this scenario.

Figure 6-29 Device Unreachable on Unmanaged Core Correlation

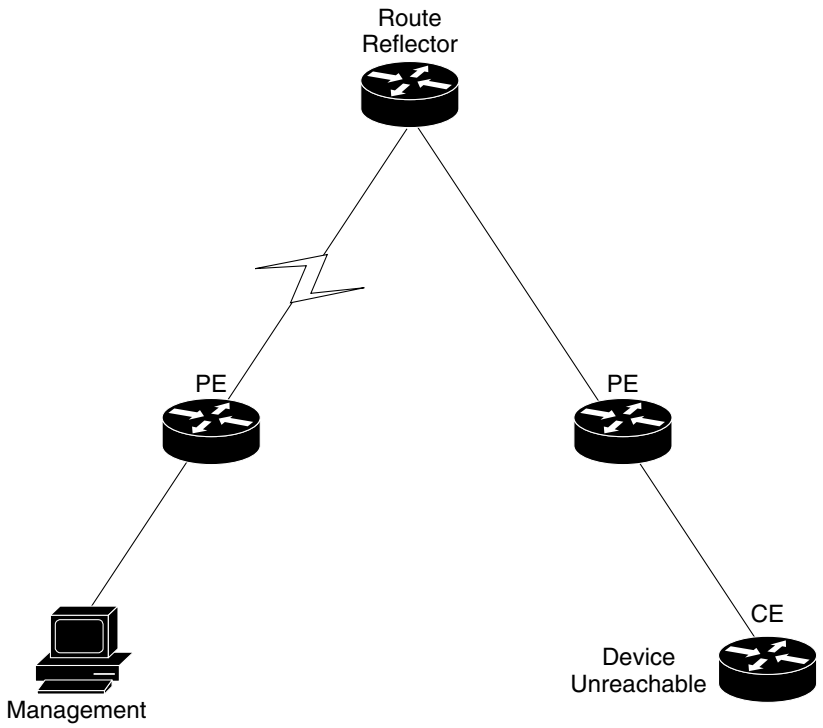
ID	Short Description	Location	Time	Last Modification Time
52573	Device unreachable	RR2-IOU-176	12/9/07 - 16:16:06	12/9/07 - 16:16:06
52567	BGP link down	PE-South-IOU-176<->R...	12/9/07 - 16:15:54	12/9/07 - 16:15:54
52569	BGP link down	PE-East-IOU-176<->RR...	12/9/07 - 16:15:54	12/9/07 - 16:15:54
52570	BGP link down	RR1-IOU-176<->RR2-I...	12/9/07 - 16:15:55	12/9/07 - 16:15:55

270148

For the event [Device Unreachable, RR2] (see Figure 6-30 and Component Unreachable, page 16-11):

- Additional Collected Events: [BGP Link Down, RR2 < > PE-South].
- Root cause: Correlates to [BGP Link Down, RR2 < > PE-South].

Figure 6-30 Device Unreachable on CE



HSRP Scenarios

These topics describe scenarios that can generate HSRP alarms:

- HSRP Alarms, page 6-26
- HSRP Example, page 6-27

HSRP Alarms

When an active Hot Standby Router Protocol (HSRP) group's status changes, a service alarm is generated and a syslog is sent.

Table 6-1 HSRP Service Alarms

Alarm	Ticketable?	Correlation allowed?	Correlated to	Severity
Primary HSRP interface is not active/Primary HSRP interface is active (see HSRP Group Status Changed, page 16-16)	Yes	No	Can be correlated to several other alarms, for example, link down	Major
Secondary HSRP interface is active/Secondary HSRP interface is not active (see HSRP Group Status Changed, page 16-16)	Yes	No	Can be correlated to several other alarms, for example, Link Down	Major

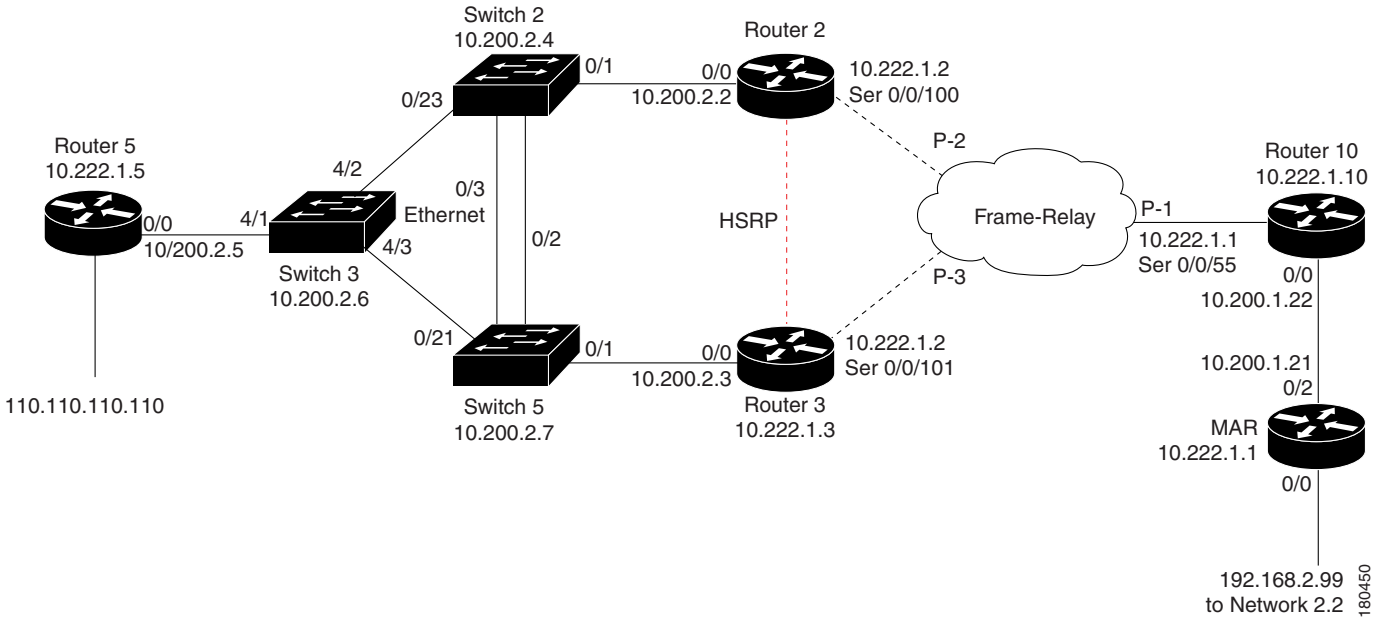
Note HSRP group information can be viewed in the Inventory window of Cisco ANA NetworkVision.

HSRP Example

In Figure 6-31, the link between Router 2 and Switch 2 is shut down, causing the HSRP standby group on Router 3 to become active, and a Link Down service alarm is generated. The primary HSRP group on Router 2 is not active anymore. A service alarm is generated and correlated to the Link Down alarm. Router 2 also sends a syslog which is correlated to the Link Down alarm.

The secondary HSRP group configured on Router 3 now changes from standby to active. This network event triggers an IP-based active flow with the destination being the virtual IP address configured in the HSRP group. When the flow reaches its destination, a service alarm is generated and correlated to the Link Down alarm. Router 3 also sends a syslog that is correlated to the Link Down alarm.

Figure 6-31 Example



In this case, the system provides the following report:

- Root cause: [Link Down, Router 2 < > Switch 2]
- Correlated events:
  - [Primary HSRP Interface is Not Active, Router 2]

    ```
    %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Speak (source:
    Router 2)
    ```

  - [Secondary HSRP Interface is Active, Router 3]

    ```
    %STANDBY-6-STATECHANGE: Ethernet0/0 Group 1 state Standby -> Active (source:
    Router 3)
    ```

IP Interface Failure Scenarios

These topics describe sample scenarios that can generate IP interface failures:

Interface Status Down Alarm

Alarms related to subinterfaces (for example, a Line Down trap or syslog) 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 interface are reported on the underlying Layer 1.

An Interface Status Down alarm is generated when the status of the IP interfaces (whether over an interface or a subinterface) changes from up to down or any other nonoperational state (see Table 6-3). All events sourced from the subinterfaces correlate to this alarm. In addition, an All IP Interfaces Status Down alarm is generated when all the IP interfaces above a physical port change state to down. For more information, see Interface Status, page 16-17.

Table 6-2 Interface Status Down Alarm

Name	Description	Ticketable	Correlation allowed	Correlated to	Severity
Interface status down/up	Sent when an IP interface changes operational status to down/up	Yes	Yes	Link down/Device unreachable	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 Layer 1).

All syslogs and traps indicating changes in subinterfaces (above which an IP is configured) correlate to the Interface Status Down alarm. 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 If a syslog or trap is received from a subinterface that does not have an IP interface 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.

If 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
- Channelized Optical Carrier (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 (such as 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 Interface Status Down alarm is created. All the circuit down syslogs correlate by flow to the possible root cause, such as 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 Interface Found) alarm is sent.
- The Interface Status Down alarm for each of the failed IP interfaces is correlated to the All IP Interfaces Down alarm.

Note If an All IP Interfaces Down alarm is cleared by the Active IP Interfaces Found alarm, but there are still correlated 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 Interface Found alarm has a cleared severity.

For more information, see Table 6-3 and All IP Interfaces Down, page 16-3.

Table 6-3 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 operational status to down	Yes	Yes	Link Down	Major

The All IP Interfaces Down alarm is sourced to the Layer 1 component. All alarms from the other side (such as Device Unreachable) correlate to the All IP Interfaces Down alarm.

IP Interface Failure Examples

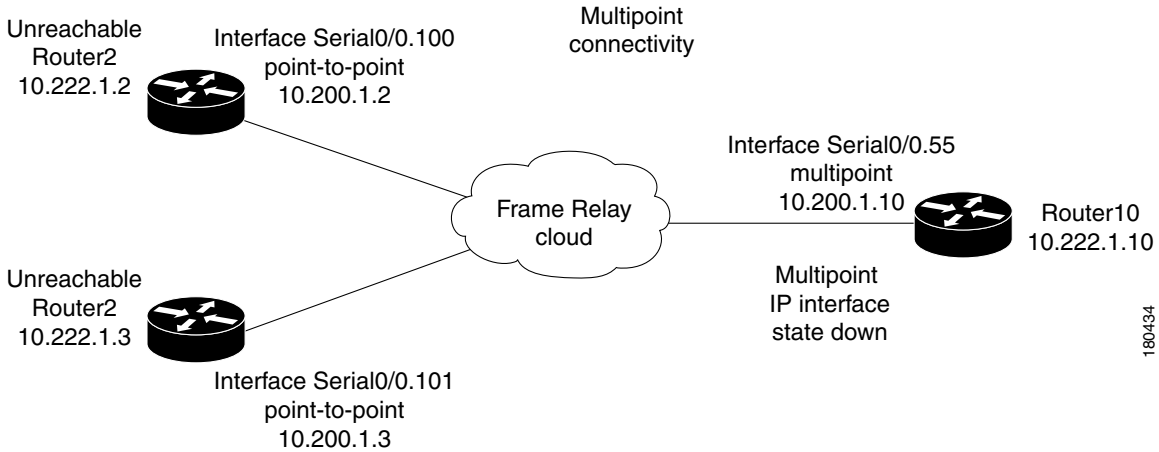
Note In all the examples that follow, it is assumed that the problems that result in the unmanaged cloud, or the problems that occurred on the other side of the cloud (such as an unreachable CE device from a provider edge (PE) device) cause the relevant IP interfaces' state to change to down. This in turn causes the 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 Figure 6-32 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 keepalive option is enabled for all circuits. A link is disconnected inside the unmanaged network, causing all the CEs to become unreachable.

Figure 6-32 Interface Example 1



The following failures are identified in the network:

- A Device Unreachable alarm is generated for each CE.
- An Interface Status Down alarm is generated for the multipoint IP interface on the PE.

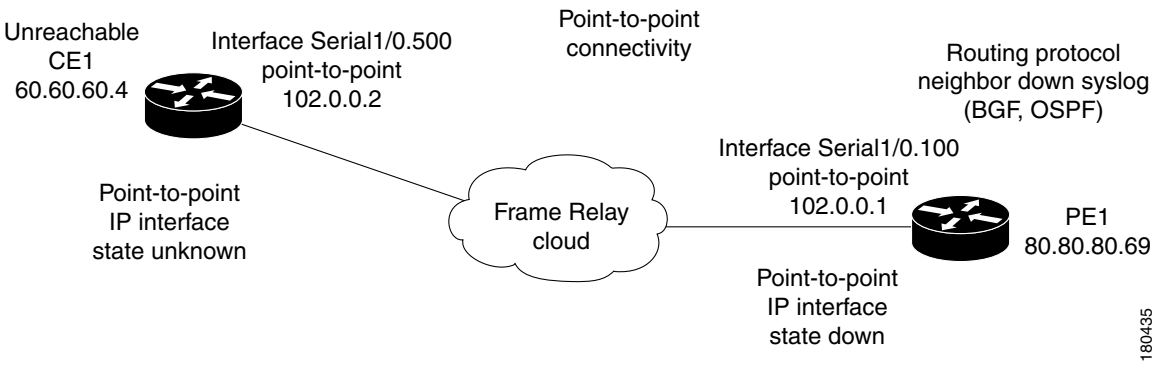
The following correlation information is provided:

- The root cause is Interface Status Down.
- All the Device Unreachable alarms are correlated to the Interface Status Down alarm on the PE.

Interface Example 2

In Figure 6-33 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 keepalive option is enabled. The interface is shut down between the unmanaged network and CE1.

Figure 6-33 Interface Example 2



The following failures are identified in the network:

- A Device Unreachable alarm is generated on the CE.
- An Interface Status Down alarm is generated on the PE.

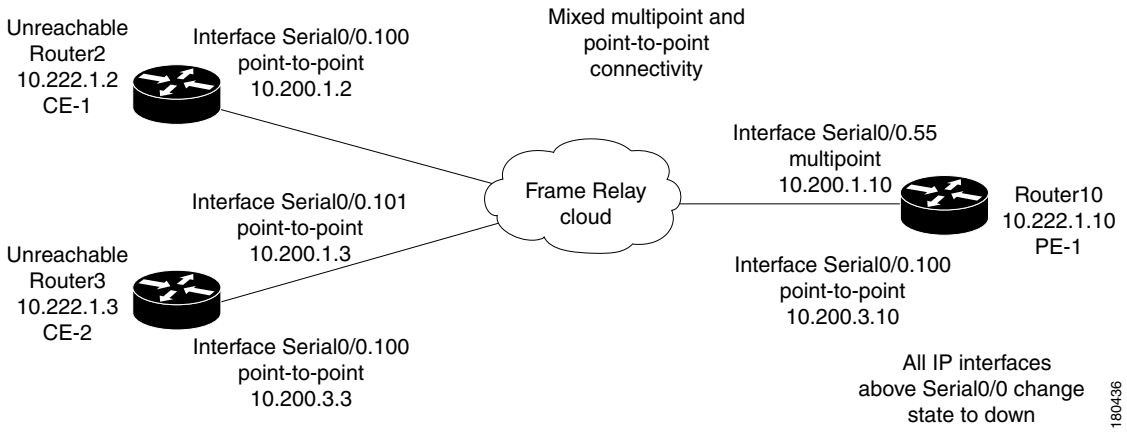
The following correlation information is provided:

- The root cause is Device Unreachable:
  - The Interface Status Down alarm is correlated to the Device Unreachable alarm.
  - The syslogs and traps for the related subinterfaces are correlated to the Interface Status Down alarm.

Interface Example 3

In Figure 6-34 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 keepalive option is enabled. A link is disconnected inside the unmanaged network that has caused all the CEs to become unreachable.

Figure 6-34 Interface Example 3



The following failures are identified in the network:

- All the CEs become unreachable.
- An Interface Status Down alarm is generated for each IP interface above Serial0/0 that has failed.

The following correlation information is provided:

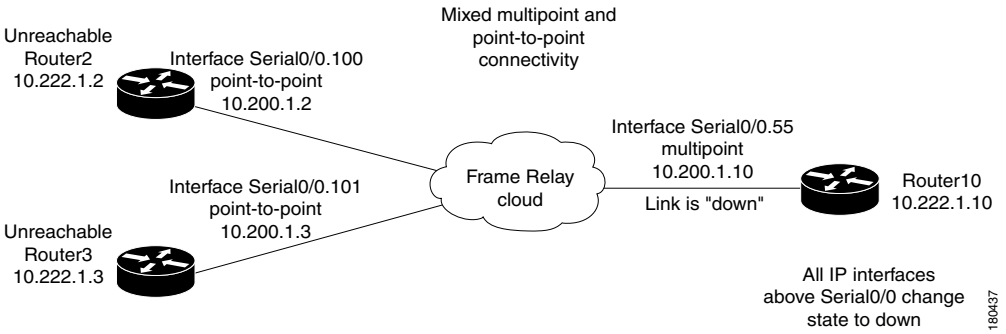
- The root cause is All IP Interfaces Down on Serial0/0 port:
  - The Interface Status Down alarms are correlated to the All IP Interfaces Down alarm.
  - The Device Unreachable alarms are correlated to the All IP Interfaces Down alarm.
  - The syslogs and traps for the related subinterfaces are correlated to the All IP Interfaces Down alarm.

Interface Example 4

In Figure 6-35 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 keepalive option is enabled.

A link is disconnected inside the unmanaged network that has caused all the CEs to become unreachable. 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 6-35 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 Interface Status Down alarm is generated for each IP interface above Serial0/0.
- An All IP Interfaces Down alarm is generated on Serial0/0.

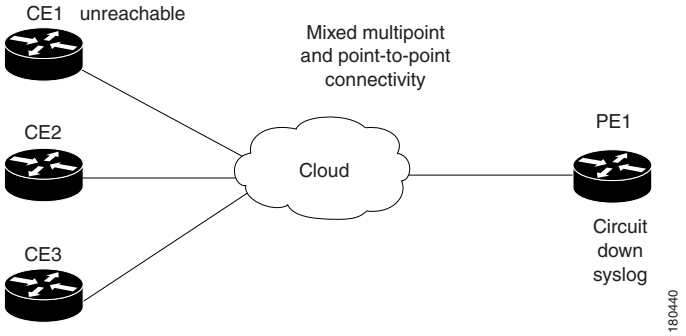
The following correlation information is provided:

- The Device Unreachable alarms are correlated to the Link Down alarm
- The Interface Status Down alarm is correlated to the Link Down alarm
- The All IP 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 Figure 6-36 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 6-36 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 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, Gigabit Ethernet Examples

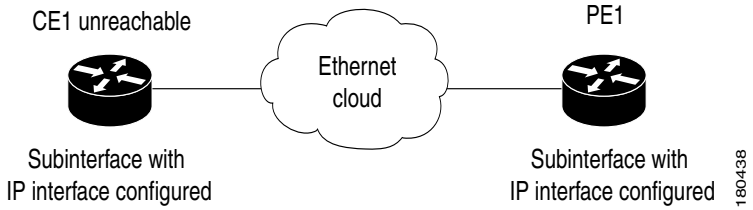
This section includes the following examples:

- There is an unreachable CE due to a failure in the unmanaged network.
- There is a Link Down on the PE that results in the CE becoming unreachable.

Interface Example 6

In Figure 6-37 there is an unreachable CE due to a failure in the unmanaged network.

Figure 6-37 Interface Example 6



The following failures are identified in the network:

- A Device Unreachable alarm is generated on the CE. For more information, see Component Unreachable, page 16-11.
- A Cloud Problem alarm is generated. For more information, see Cloud Problem, page 16-10.

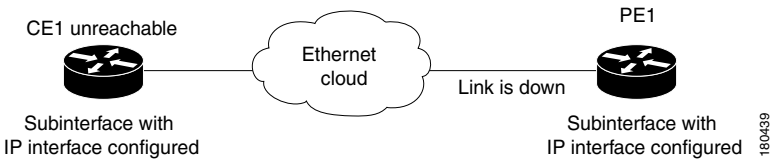
The following correlation information is provided:

- No alarms are generated on a PE for Layer1, Layer2 or the IP layers.
- The Device Unreachable alarm is correlated to the Cloud Problem alarm.

Interface Example 7

In Figure 6-38 there is a Link Down on the PE that results in the CE becoming unreachable.

Figure 6-38 Interface Example 7



The following failures are identified in the network:

- A Link Down alarm is generated on the PE. For more information, see Link Down, page 16-22.
- An Interface Status Down alarm is generated on the PE. For more information, see Interface Status, page 16-17.
- A Device Unreachable alarm is generated on the CE. For more information, see Component Unreachable, page 16-11.

The following correlation information is provided:

- Link Down on the PE:
  - The 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

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 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, meaning 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 do not 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 Status 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. For more information, see GRE Tunnel Down, page 16-15.

Note The GRE tunnel down alarm 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, because 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.

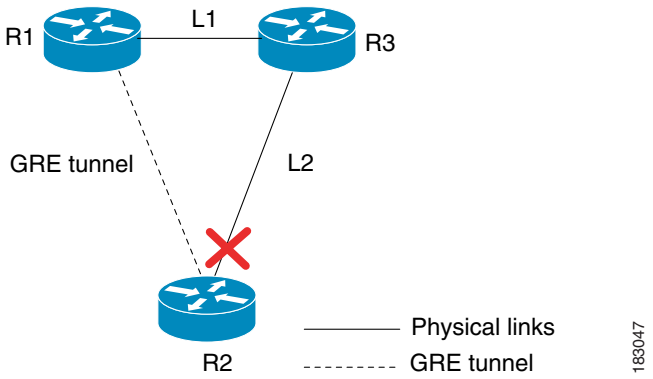
GRE Tunnel Down Correlation Example 1

Figure 6-39 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 6-39 GRE Tunnel Down Example 1 (Single GRE Tunnel)



When the 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 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] (see Link Down, page 16-22)
- Correlated events:

  [GRE Tunnel Down, Router1:tunnel < > Router 2:tunnel]

  - [Interface Status Down, Router 1:tunnel]
  - [Interface Status 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 ticket, as illustrated in Figure 6-40.

Figure 6-40 GRE Tunnel Down Example 2 (Multiple GRE Tunnels)

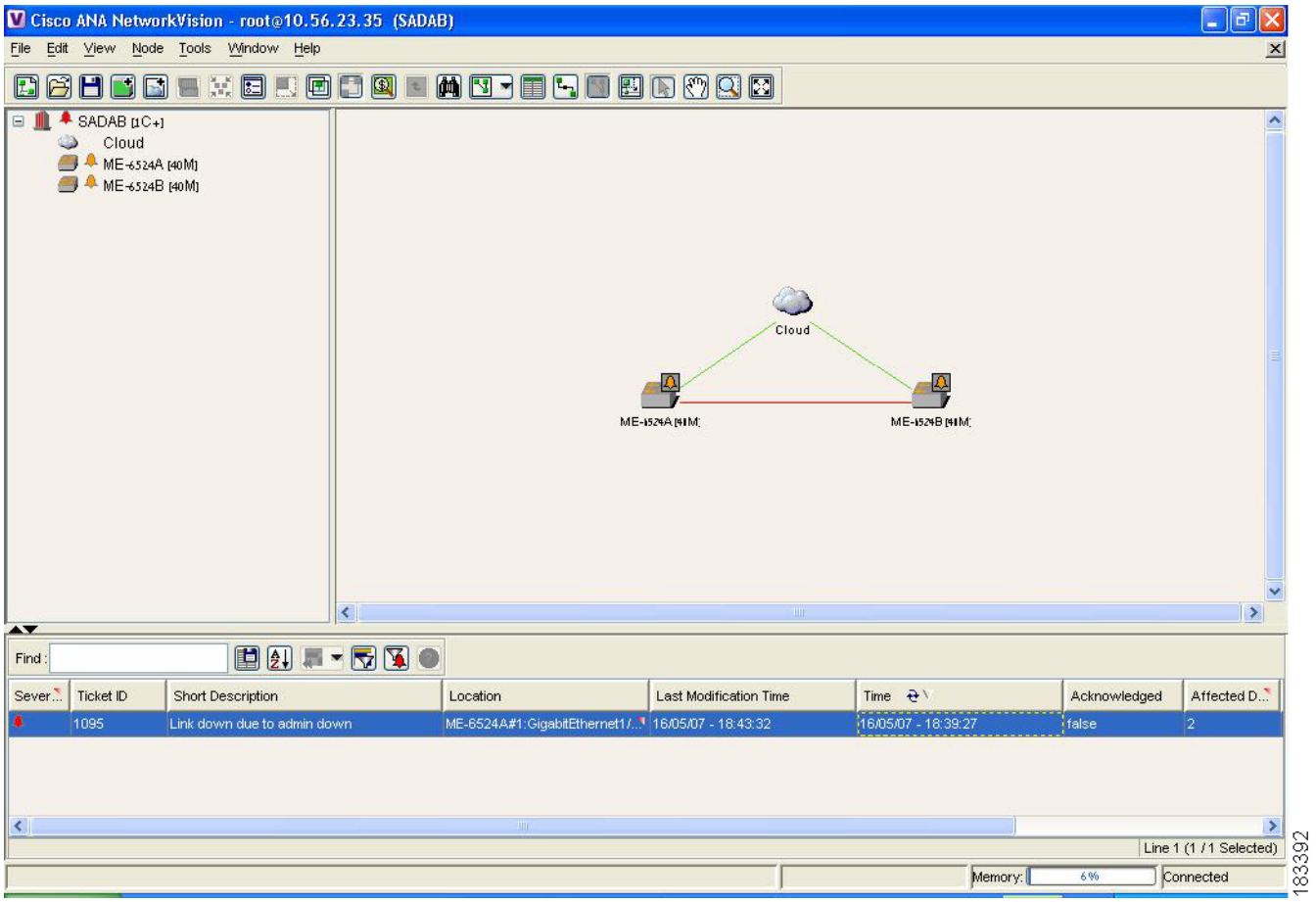
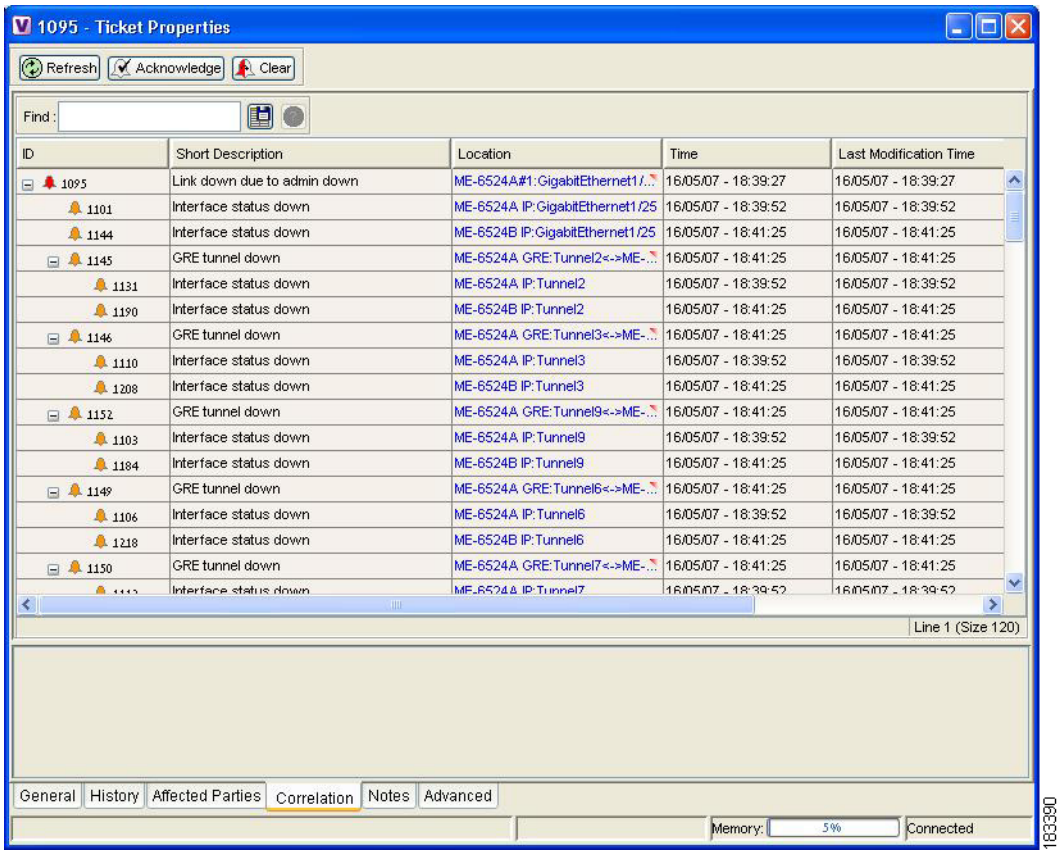


Figure 6-41 shows the Correlation tab of the Ticket Properties dialog box that displays all the alarms that are correlated to the ticket, including the correlation for each GRE tunnel and its interface status.

Figure 6-41 Alarms Correlation to GRE Tunnel Down Ticket



As illustrated, the system provides the following report:

- Root cause—Link Down Due to Admin Down (see Link Down, page 16-22)
- 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]

  and so on.