



# Drilling Down into an NE's Physical and Logical Inventories and Changing Basic NE Properties

---

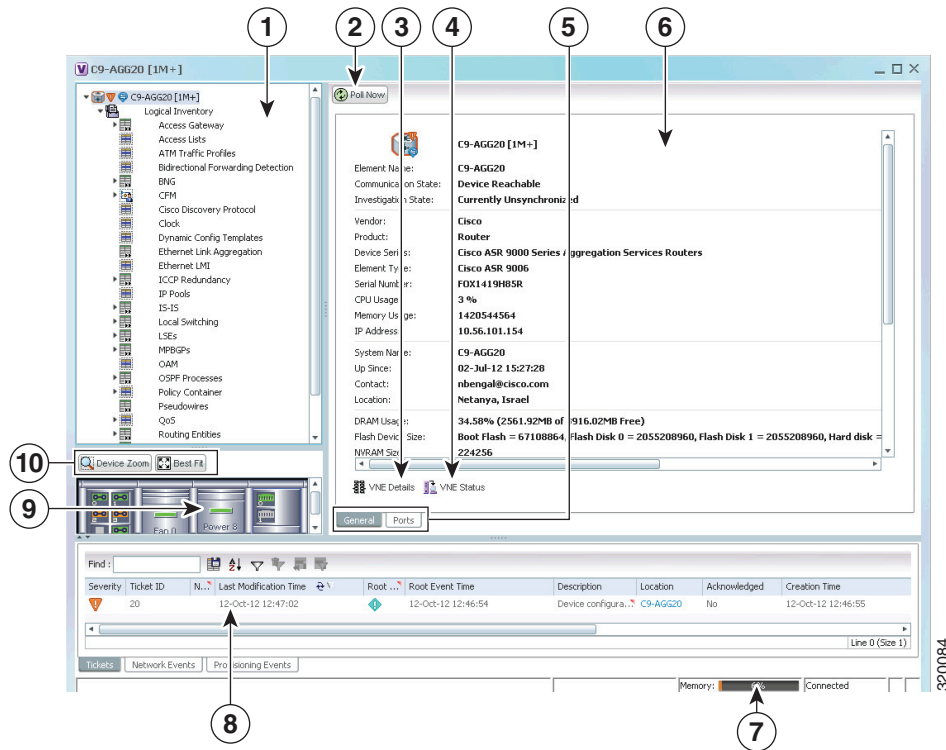
The following topics describe how to view a device's physical and logical inventory using the Vision client:

- [Drilling Down into the Properties of a Network Element, page 8-2](#)
- [Viewing Single- and Multi-Chassis Devices, Clusters, Satellites and Their Redundancy Settings, page 8-4](#)
- [Viewing Cards, Fans, and Power Supplies and Their Redundancy Settings, page 8-13](#)
- [Viewing Port Status and Properties and Checking Port Utilization, page 8-15](#)
- [Viewing the Logical Properties of a Device \(Traffic, Routing, Information, Tunnels, Data Link Aggregations, Processes\), page 8-21](#)
- [Viewing a Device's Operating System Details \(and K9 Security\), page 8-25](#)
- [Updating the Inventory \(Poll Now\), page 8-26](#)
- [Changing the NE Host Name, page 8-26](#)
- [Changing the SNMP Configuration and Managing SNMP Traps, page 8-27](#)
- [Changing Device Port Properties and Disabling Ports, page 8-29](#)
- [Changing Device Interface Properties and Disabling Interfaces, page 8-30](#)
- [Changing Server Settings for DNS, NTP, RADIUS, and TACACs, page 8-31](#)
- [Suppressing Service Alarms on Virtual Interfaces, page 8-32](#)

# Drilling Down into the Properties of a Network Element

From a map, double-click an NE to open its inventory window. [Figure 8-1](#) provides an example.

**Figure 8-1** Inventory Window

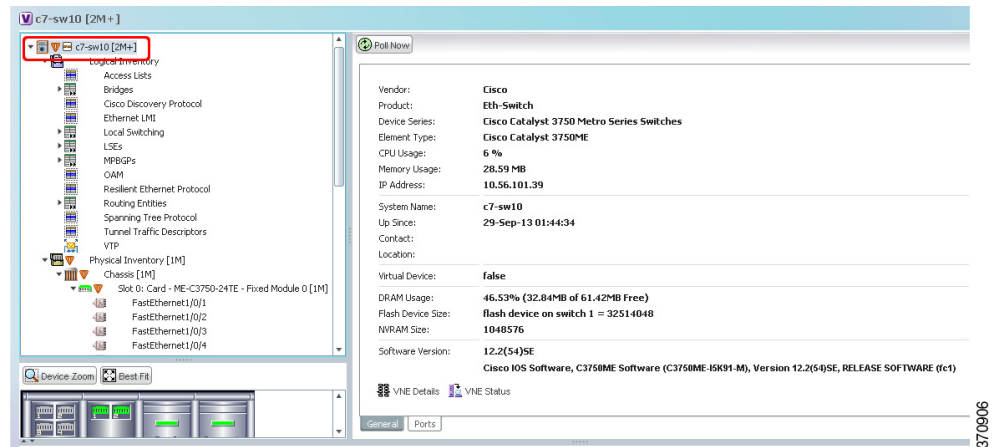


1	Physical and logical inventory—Physical Inventory includes the device components such as chassis, satellite, cards, and subslots. Configuration and status information is continuously updated. Logical inventory includes access lists, ATM traffic profiles, routing entities, and other logical entities.
2	Poll Now button—Initiates a poll of the selected NE.
3	VNE Details button (VNEs are internal components, one VNE per device)—Provides information about whether the VNE is operating correctly, what polling values are set, and so forth.
4	VNE Status button—Lists the protocols the device is using (it can also provide troubleshooting information).
5	Property tabs (General properties and Ports properties in this example)—The Ports tab provides a quick list of all device ports. The tabs displayed depend on what is selected. General tab can also display context-sensitive tabs and buttons.
6	Properties area—Provides inventory details. For a closer view of the Properties panel, see <a href="#">Figure 8-2 on page 8-3</a> . The NE icon may also display: <ul style="list-style-type: none"> <li>• Colors indicating a ticket and the ticket severity. See <a href="#">Severity Icons and Colors for Events, Tickets, and NEs, page A-15</a> for an explanation of the colors.</li> <li>• Badges that represent technologies such as a Protected LSP or an STP root. See <a href="#">Network Element Technology-Related Badges, page A-24</a> for a list of badges.</li> </ul>
7	Vision client status bar.

8	Ticket and events pane—Displays tickets associated with the selected NE (from the last 6 hours) and associated Network and Provisioning events. See e <a href="#">Ways You Can View Tickets and Events, page 11-1</a> .
9	Device view—Generic representation of the chassis, slots, modules, subslots and ports. All occupied slots are rendered in the device view pane. Problems are indicated with colors. See <a href="#">Figure 8-3 on page 8-4</a> .
10	Device view tools for zooming and best fit.

[Figure 8-2](#) shows the basic properties window for an NE. To display the basic properties, open the inventory window and select the NE at the very top of the navigation area.

**Figure 8-2** NE Basic Properties Window

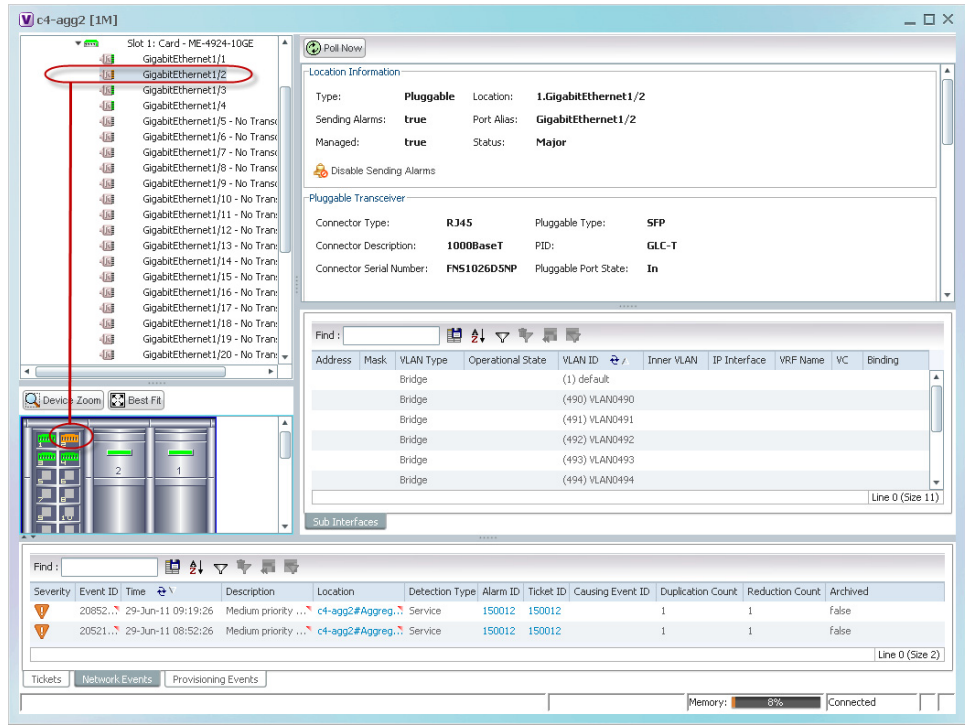


The following table provides information about the fields that are not self-explanatory.

Field	Description
Communication State	Ability of the Prime Network device model to reach the network element and other components in Prime Network.
Investigation State	Level of network element discovery that has been performed or is being performed by the Prime Network device model.
Up Since	Date and time the element was last reset.
Sending Alarms	Whether or not the element is configured for sending alarms (True or False)

[Figure 8-3](#) provides an example of the device view pane for a Cisco device. The circled slot in the device view pane corresponds to the circled slot in the physical inventory navigation pane.

Figure 8-3 Device View Pane



Tip

You can display or hide the ticket and events pane by clicking the arrows displayed below the device view panel.

## Viewing Single- and Multi-Chassis Devices, Clusters, Satellites and Their Redundancy Settings

To get an NE's chassis details, choose **Physical Inventory > Chassis**. Prime Network displays the chassis serial number and description, along with the equipment in each slot.

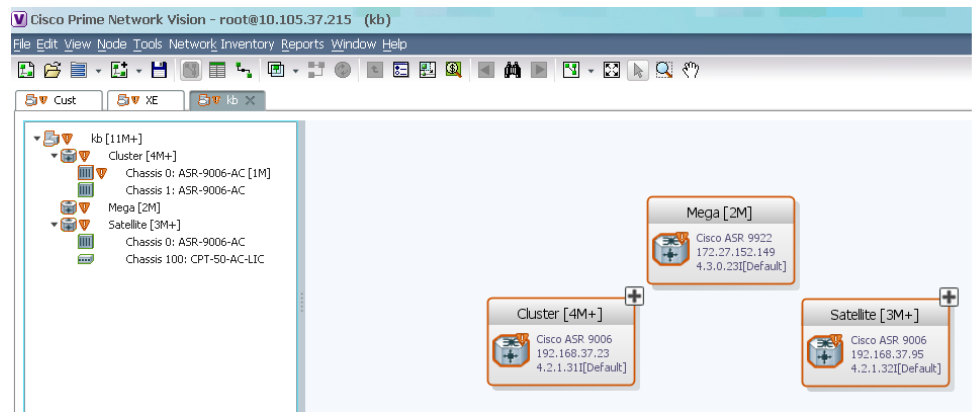
Icon	NE
	Chassis
	Cluster
	Satellite
	Shelf

If any items in the chassis inventory are black, it means the item was physically removed. You can verify this by checking the item status which should display Out. The other properties of the removed item reflect the most recent value that was updated from the device.

## Viewing Multi-Chassis Devices

Multi-chassis devices, such as Cisco ASR9000 and Cisco UCS devices, are grouped into aggregations and displayed as a single entity with a plus sign as shown in [Figure 8-4](#).

**Figure 8-4** Multichassis Devices in Map View



The physical ethernet links used for connecting the multi chassis devices are ICL (Inter Chassis Link) and IRL (Inter Rack Link). For more information on when each of these links are used, see [Viewing Cluster Inter-Rack Links \(IRLs\)](#), page 8-6 and [Viewing Satellites and Satellite Inter-Chassis Links \(ICLs\)](#), page 8-7.

## Viewing Redundant (Primary and Secondary) Devices

In the Failover Configuration, two ASA devices are connected to each other. When the primary device becomes unavailable due to failure or down time, then the secondary device takes over the function of the primary device. The ASA device supports the following two failover configurations:

- **Active/Active Failover**—Also called the group failover, this type of configuration is available only in multiple context mode. In this configuration, both the ASA devices are active and pass traffic. This lets you configure load balancing on your network. When one of the devices becomes unavailable, then its functions are taken over by the other device.

As mentioned earlier, this configuration has multiple contexts. The security contexts are divided into two failover groups. In other words, each device will have two failover groups.



**Note** By default, the admin context and any unassigned security contexts are members of failover group 1.

These groups can be in Active, Standby or a combination of Active and Standby modes. If Group 1 of the first ASA device is Active, then Group 1 of the second device must be in Standby mode. If Group 1 of the first ASA device (which is active) becomes unavailable, then Group 1 of the second device (which is in Standby mode) will become active. The same process applies for Group 2 contexts in both the devices.

- **Active/Standby Failover**—This type of configuration is available either on single or multiple context mode. In this configuration, only one of the units is active while the other one is in standby mode. When the active unit becomes unavailable, then the standby unit becomes active.

When there is a failover, and the secondary device takes over, syslogs are generated. You can view the syslog information in the “Latest Events” tab.

Figure 8-5 depicts the ASA failover scenario, along with the events that are generated after the failover:

Figure 8-5 ASA Failover topology with generated events

The screenshot displays the Cisco Prime Network Vision interface. At the top, a network diagram shows two ASA devices, 'Primary [1]' and 'Secondary [1]', connected to a central '6500\_VSS' device. Below the diagram, two 'Network Event Properties' windows are open, showing details for specific events related to failover. The bottom portion of the screenshot shows a table of network events.

Statis	Severity	Event ID	Time	Description	Location	Element Type	Detection Type	Ticket ID	Duplication Count	Reduction Count	Archived
✓	Information	20053	21-Oct-13 14:24:18	Switching To Paired Device Due To Failover	Secondary	Cisco ASA 5585	Syslog	220001	1	1	false
✓	Information	20014	21-Oct-13 14:24:18	Switching To Paired Device Due To Failover	Secondary	Cisco ASA 5585	Syslog	220001	1	1	false
✓	Information	14259	21-Oct-13 14:24:18	Switching To Paired Device Due To Failover	Primary	Cisco ASA 5585	Syslog	220002	1	1	false
✓	Information	14212	21-Oct-13 14:24:18	Switching To Paired Device Due To Failover	Primary	Cisco ASA 5585	Syslog	220002	1	1	false
✓	Warning	22762	21-Oct-13 14:18:51	Medium priority member down - Cleared due to ForceClear	6500_VSS#Aggregation Group 42	Cisco Catalyst 65.T	Service	210003	1	1	true
✓	Warning	21474	21-Oct-13 14:18:51	Low priority member down - Cleared due to ForceClear	6500_VSS#Aggregation Group 21	Cisco Catalyst 65.T	Service	210002	1	1	true
✓	Warning	14750	21-Oct-13 13:24:18	Chassis Connected	6500_VSS#1	Cisco Catalyst 65.T	Service	1	1	1	true
✓	Warning	16320	21-Oct-13 13:07:25	Medium priority member down	6500_VSS#Aggregation Group 42	Cisco Catalyst 65.T	Service	210003	1	1	true
✓	Warning	16277	21-Oct-13 13:07:25	Low priority member down	6500_VSS#Aggregation Group 21	Cisco Catalyst 65.T	Service	210002	1	1	true
✓	Warning	15848	21-Oct-13 13:07:25	Low priority member down	6500_VSS#Aggregation Group 21	Cisco Catalyst 65.T	Service	210002	1	1	true



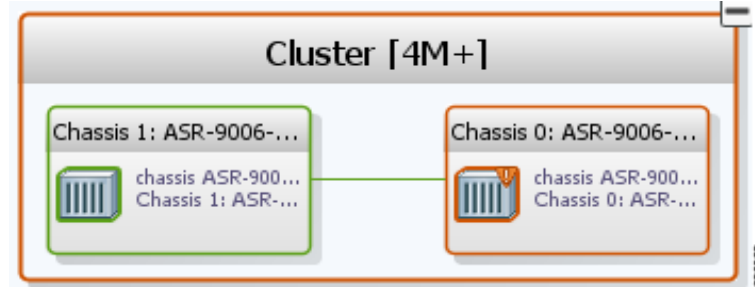
#### Note

These syslogs help Prime Network to identify the devices that are in active and standby mode. When an active device goes into standby mode, and the other device becomes active, Prime Network changes the IP address of these devices. For example, if the primary devices goes into standby mode, the secondary device will take over the IP address of the primary device and starts functioning immediately.

## Viewing Cluster Inter-Rack Links (IRLs)

Inter-Rack Links (IRLs) represent connectivity between the cluster chassis as shown in Figure 8-6.

Figure 8-6 Multiple Chassis in a Cluster



To view the cluster IRLs:

- 
- Step 1** Double-click the cluster device to open the Inventory window.
- Step 2** In the device's Logical Inventory, choose **Cluster IRL**. A list of cluster IRLs is displayed showing the following information:
- A End Point—Device or site that is the source of the link, hyperlinked to the inventory of the device or site.
  - Z End Point—Device or site that is the destination of the link, hyperlinked to the relevant entry in the inventory.
- 

### Viewing Satellites and Satellite Inter-Chassis Links (ICLs)

The Cisco ASR 9000 Series Router Satellite Network Virtualization (nV) service or the Satellite Switching System enables you to configure a topology in which one or more satellite switches complement one or more Cisco ASR 9000 Series routers, to collectively realize a single virtual switching system. In this system, the satellite switches act under the management control of the routers. The complete configuration and management of the satellite chassis and features are performed through the control plane and management plane of the Cisco ASR 9000 Series Router, which is referred to as the host.

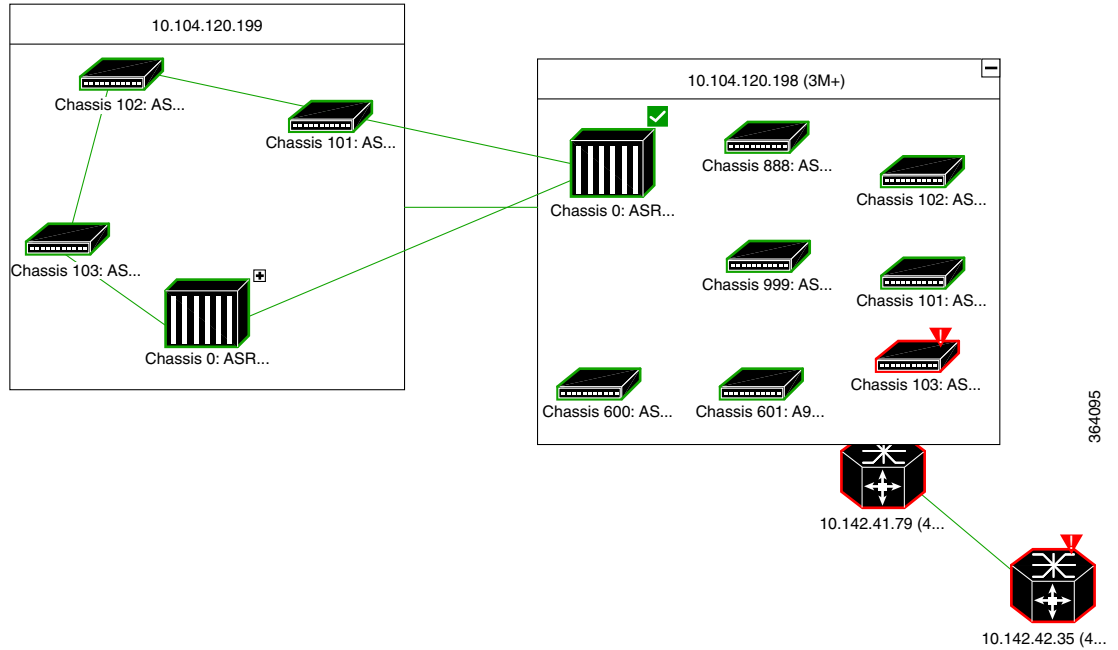
The Satellite nV system supports the dual-homed network architecture, based on which two hosts are connected to a satellite through the Satellite Discovery And Control (SDAC) Protocol. Both these dual-homed hosts act in the active/standby mode for the satellite. The standby host takes control of the satellite only when the active host is down. The two hosts can leverage the Inter-chassis Communication Protocol (ICCP) infrastructure to provide redundant Layer 2 and Layer 3 services for Satellite Ethernet interfaces. The network traffic is switched through the active host. In case of connection loss to the active host due failure such as cut cable and host or client connection interface failure, the standby host becomes the active host and the active host becomes the new standby host. The hosts communicate with each other using ORBIT/ICCP protocols.

The advanced satellite nV system network topologies can be realized based on one of these architecture:

- Hub and Spoke.
- Ring with Dual Home.
- Ring with Layer 2 Fabric.
- Linear and Cascade.

Figure 8-7 shows an example of a satellite ring topology.

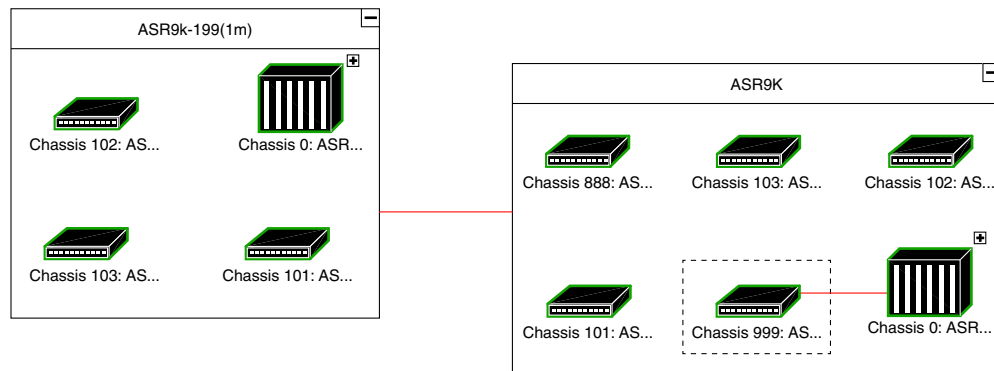
Figure 8-7 Satellite Ring Topology



364095

Figure 8-8 shows an example of a hub and spoke topology.

Figure 8-8 Hub and Spoke Topology

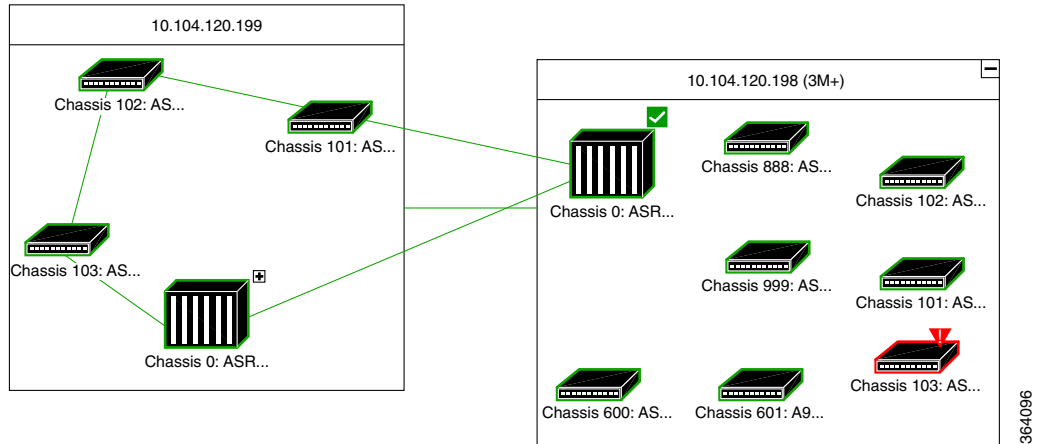


364097



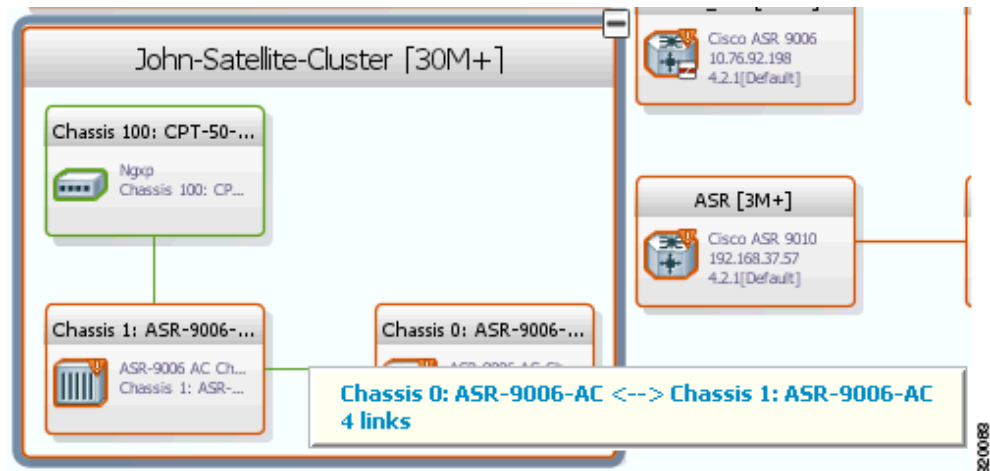
Figure 8-9 shows an example of a ring and cascade topology.

Figure 8-9 Ring and Cascade Topology



Satellites enhance the performance bandwidth of Cisco ASR 9000 NEs. Each satellite is modeled as a chassis in the host Cisco ASR 9000 physical inventory. Satellites are connected to host Cisco ASR 9000 using the physical ethernet links. The physical ethernet links act as the inter-chassis links (ICLs), connecting the satellite to other satellites or chassis in the host. Figure 8-10 provides an example.

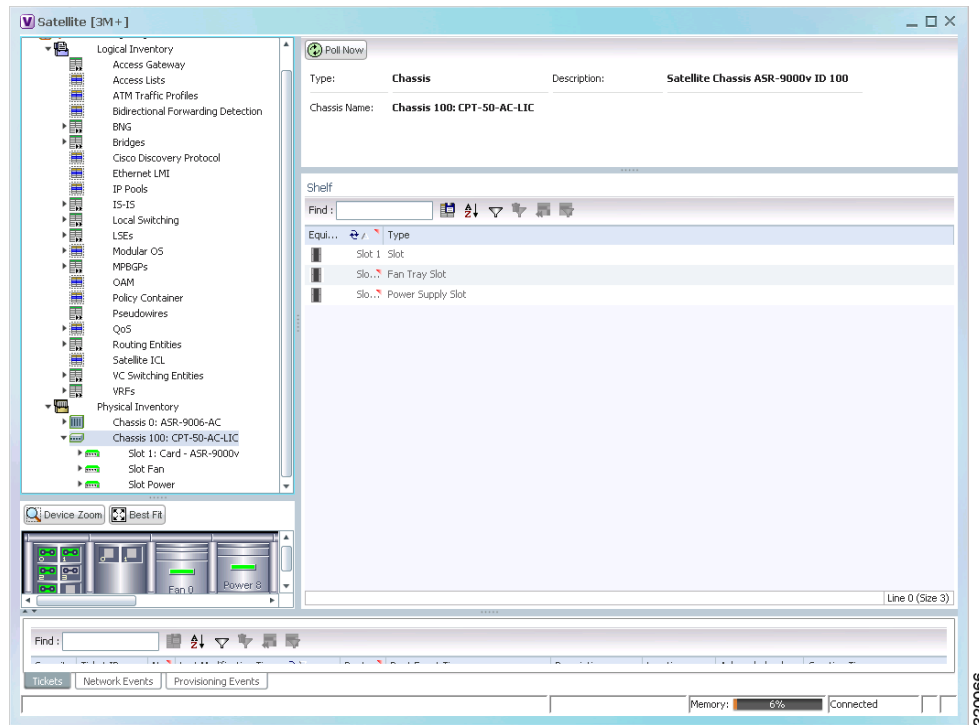
Figure 8-10 ICL Connecting a Satellite with a Chassis



To view the satellite properties and ICLs in physical inventory:

- Step 1** In the Vision client, double-click the device in which the satellite is configured.
- Step 2** In the **Inventory** window, expand the Physical Inventory node.
- Step 3** Click on the particular *Chassis* (the satellite is modeled as a chassis). Figure 8-11 shows an example of the satellite properties.

Figure 8-11 Satellite Properties



To view the satellite details and properties in logical inventory:

- Step 1** In the Vision client, double-click the device in which the satellite is configured.
- Step 2** In the **Inventory** window, expand the Logical Inventory node.
- Step 3** Click *Satellites*. The content pane shows the following information:

Field	Description
Satellite Discovery Protocol	The SDAC Protocol that provides the behavioral, semantic, and syntactic definition of the relationship between a satellite device and its host.
Redundancy Control Protocol	The ICCP protocol.
Associated Redundancy System	A link to the associated redundancy system.

- Step 4** Expand the Satellites node. Click on the particular satellite number. The properties of the satellite are displayed in the content pane.

Table 8-1 describes the properties of the satellite.

Table 8-1 Satellite Properties

Field	Description
Satellite ID	The identification number of the satellite.
Satellite Type	The type of the satellite.

Field	Description
Description	The description of the satellite.
IP Address	IP address of the satellite device.
MAC Address	MAC address of the satellite device.
Control Status	Control status of the satellite, whether it is connected or disconnected.
VRF	Virtual Routing and Forwarding (VRF) name, if the pool belongs to a VRF.
Associated Chassis	The chassis associated with the satellite.
Active Host or Standby Host	Displays Active Host if the host is active, else Standby Host is displayed.

**Step 5** Click the respective tabs on the content pane to view the details of satellite connections and satellite fabric links.

[Table 8-2](#) describes the details of satellite connections and satellite fabric links.

*Table 8-2 Satellite Connections and Satellite Fabric Links Details*

Field	Description
<b>Satellite Connections tab</b>	
Interface Name	The name of the interface.
Associated Entity	The associated entity of the interface.
Connection Status	Connection status of the satellite, whether it is connected or disconnected.
Connecting Entity	Shows the type of connection, whether it is to the remote or local host.
Connecting Interface	A link to the connecting entity.
Host Connected Interface	A link to the connected host.
<b>Satellite Fabric Links tab</b>	
Host Interface Name	The name of the host interface.
Associated Host Interface	The interface associated with the host.
Discovery Status	Discovery status of the satellite, whether it is Ready or Not Ready.
Configured Remote Ports	Remote ports that are configured.
Invalid Remote Ports	Remote ports that are invalid.

## Viewing ICCP Group Properties

To view the properties of the ICCP Group:

- Step 1** Double-click the satellite device to open the **Inventory** window.
- Step 2** Choose **Logical Inventory > Redundancy Systems**. Click the particular **ICCP Group**. The properties of the ICCP group are displayed on the content pane.

[Table 8-3](#) describes the properties of the ICCP redundancy group.

**Table 8-3** *ICCP Redundancy Group Properties*

Field	Description
ICCP Group	The name of the ICCP Group.
Local System ID	The address of the local system.
Peer System ID	The address of the peer system.
System MAC address	The MAC address of the local system.
Local System Role	The status of the local system, whether it is Active or Standby.
Redundancy Status	The redundancy status of the satellite.
Redundancy Protocol	The ICCP protocol that controls the redundancy groups.
Associated Active System or Associated Standby System	The associated system of the ICCP Group, either Active or Standby.
Application Usage	Application usage can either be mLACP or Satellite ORBIT.
Peer Monitoring Option	Method used to monitor the peer: IP Route-Watch or Bidirectional Forwarding Detection (BFD).

- Step 3** Click the respective tabs on the content pane to view the details of control interfaces and access data link aggregations.

[Table 8-4](#) describes the details of control interfaces and access data link aggregations.

**Table 8-4** *Details of Control Interfaces and Access Data Link Aggregations*

Field	Description
<b>Control Interfaces tab</b>	
Name	The name of the control interface.
Associated Entity	The associated entity of the interface.
Status	Status of the interface, whether it is Up or Unknown.

**Access Data Link Aggregations tab**

Interface Name	The name of the interface.
Associated Entity	A link to Ethernet Link Aggregation.

## Satellite ICL alarm support for 9000V Satellite


ICL alarm support is a specific requirement for ASR9000v satellite. It enables identifying the root cause for ICL links and bundle-ether links by generating the Link Down alarms whenever the ICL links go down.

ICL alarm support is applicable for single ICL links and bundle-Ethernet links. In case of bundle, if one of the links goes down, a member/port -down alarm is generated, whereas if all the links in the bundle are down, the ICL alarm is generated.

As part of correlation, ICL alarm Link Down due to admin down/oper down/unreachable needs is created as a separate ticket, and the other alarms like link down syslog, line down syslog and SNMP link down trap are correlated to ICL alarm.

## Viewing Cards, Fans, and Power Supplies and Their Redundancy Settings

To view cards, fans, and power supplies, choose **Physical Inventory > Chassis** and click the plus sign to expand the chassis inventory. Prime Network displays any cards, fans, and power supplies that are configured in the chassis slots.

Icon	NE
	Card, Subcard Fan, Power Supply

Fans are listed separately in a fan tray only if they can be separated; if fans cannot be separated, only the fan tray is displayed.



**Note**

Fans and power supplies are only displayed if they are Field Replaceable Units (FRUs).

If any item in a slot is black, it means the item was physically removed. You can verify this by checking the item status which should display Out. The other properties of the removed item reflect the most recent value that was updated from the device.

## Redundancy Support

Prime Network provides card redundancy information for Route Switch Processor (RSP) or Route Processor (RP) cards. To find out if redundancy is configured and whether an entity is the active or standby entity:

**Step 1** Choose **Physical Inventory > Chassis > Slot**.

**Step 2** To find out if redundancy is configured on the NE, check the Redundancy Configured field.

- Working—Redundancy is configured and enabled
- None—Redundancy is not configured
- N/A—Redundancy is not supported

**Step 3** To find out if the NE is the active or standby element, check the Redundancy State field.



**Note** **None** indicates that the card has been physically removed from the slot.

- Standby—The NE is the standby entity
- Active—The NE is not the standby entity  
RP card switchover syslog is supported in CRS and ASR 9K devices. When we remove one RP card from the device, the other card will automatically change to Active state. Even after reinserting the card, the other RP card will still remain in Active state.





**Note** For example, if there are two cards (RP 1 and RP 2), initially RP 1 is in Active state and RP 2 is Standby. When RP 1 card is removed, RP 2 card is automatically changed to Active state and will remain in Active state even after reinserting the RP 1 card.

**Step 4** If you have a Cisco ASR 9000 series and Cisco ASR 903 devices, you can also check the following.

Field	Description
Redundancy Info	Redundancy technology being used; for example Nonstop Routing (NSR), Stateful Switchover (SSO), or Route Processor Redundancy (RPR)
Redundancy Type ()	Stateful (SSO) or Stateless (RPR)

## Viewing Port Status and Properties and Checking Port Utilization

To view ports and pluggable transceivers, choose **Physical Inventory** > **Chassis** > *card* (or subcard) and click the plus sign to expand the card inventory. Prime Network displays any physical ports, logical ports, pluggable transceivers that are configured on the NE. Unmanaged ports are also displayed.

Icon	NE
	Port Logical Port Pluggable Transceiver
	Unmanaged Port

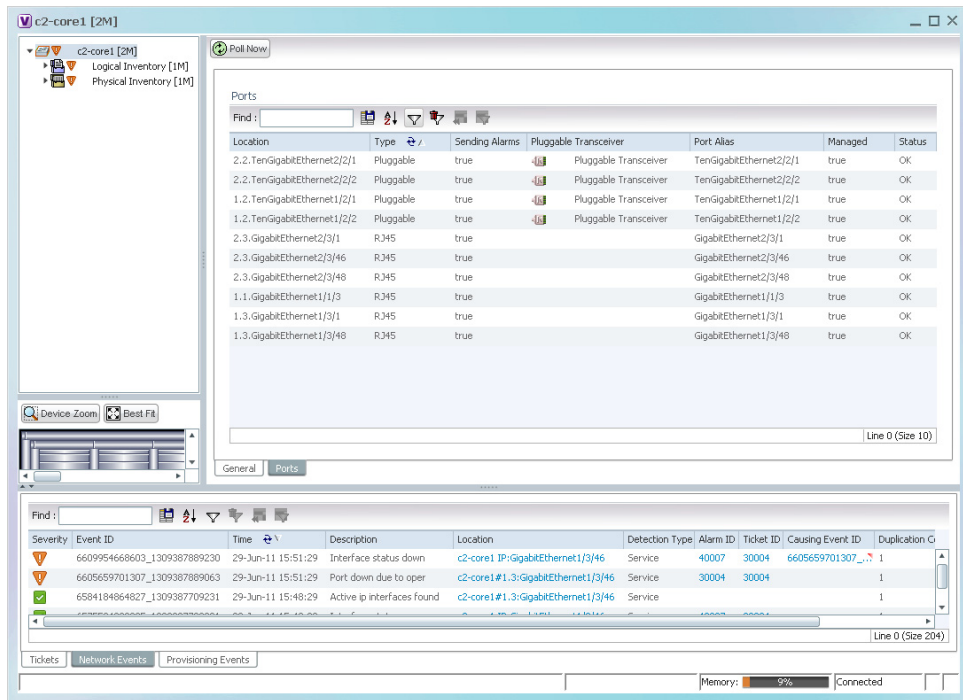
These topics explain how to view the ports on an NE, their status, and their configuration.

- [Checking the Status of All Ports on a Device \(or Ports on a Card\)](#), page 8-15
- [Drilling Down Into a Port's Configuration Details \(Including Services and Subinterfaces\)](#), page 8-17
- [Checking a Port's Utilization](#), page 8-19
- [Disabling a Port's Alarms](#), page 8-20

### Checking the Status of All Ports on a Device (or Ports on a Card)

To display all of the ports on a device, open the inventory window. Do not expand the inventory; just select the device as shown in [Figure 8-12](#).

Figure 8-12 Listing All Ports on a Network Element



Prime Network displays the following information about all ports that are configured on the device. If the device has any unmanaged ports, they are also displayed.



Tip

To export the port list from the Vision client, click the Export to CSV button in the toolbar.

Field	Description
Location	Location of the port in the device, using the format <i>slot.module/port</i> , such as 1.GigabitEthernet1/14.
Type	Port type, such as RJ45 or Pluggable.
Sending Alarms	Whether or not the port is configured for sending alarms: True or False.
Pluggable Transceiver	For the Pluggable port type, indicates that the port can hold a pluggable transceiver.
Port Alias	Name used in the device CLI or EMS for the port.
Managed	Whether or not the port is managed: True or False.
Status	Port status: OK or one of the following: <ul style="list-style-type: none"> <li>Major—Port is operationally down</li> <li>Disabled—Port is administratively down (someone purposely shut the port down)</li> <li>Out—Port has been physically removed</li> </ul>



If any ports in the inventory are black, it means the item was physically removed. You can verify this by checking its operational status which should display Out.

To display all of the ports on a specific card's physical inventory, choose the card you are interested in. Prime Network displays the same information as in [Figure 8-12](#), except only for the ports that are configured on the card you selected.

## Drilling Down Into a Port's Configuration Details (Including Services and Subinterfaces)

To drill down into a port's inventory, choose **Physical Inventory > Chassis > card > port**. [Figure 8-13](#) shows the physical inventory for a pluggable fiber optic port (managing these types of ports is discussed in [Viewing Virtual Connection Properties, page 26-5](#)).

**Figure 8-13** Viewing the Configuration Details for a Pluggable Fiber Optic Port

The screenshot displays the configuration details for a pluggable fiber optic port. The interface is divided into several sections:

- Location Information:**
  - Type: Pluggable
  - Location: 1.0.ATM1/0/0
  - Sending Alarms: true
  - Port Alias: ATM1/0/0
  - Managed: true
  - Status: OK
- Pluggable Transceiver:**
  - Connector Type: Fiber Optic
  - Pluggable Type: SFP
  - Connector Description: OC3 SR-1/STM1 MM
  - PID: 10-2078-01SFP
  - Connector Serial Number: OCP11417512
  - Pluggable Port State: In
- Atm on port: 1/0/0:**
  - Interface Type: N/A
  - ATM Address: 41432e31:35:33:33:36:30:32:30:30:30:30:30:30
  - Description: Atm on port: 1/0/0
  - Tx Allocated Bandwidth: 0.0 bps
  - Tx Maximum Bandwidth: 0.0 bps
  - Tx UBR Allocated Bandwidth: 149.76 Mbps
  - Tx CBR Allocated Bandwidth: 0.0 bps
  - VC Table Size: 2
  - Max Speed: 0.0 bps
  - Rx Allocated Bandwidth: 0.0 bps
  - Rx Maximum Bandwidth: 0.0 bps
  - Rx UBR Allocated Bandwidth: 299.52 Mbps
  - Rx CBR Allocated Bandwidth: 0.0 bps
- OC3:**
  - Admin Status: Up
  - Oper Status: Up
  - Port Type: SONET
  - Last Changed: 19-Jul-11 12:42:47
  - Scrambling: On
  - Maximum Speed: 155.52 Mbps
  - Loopback: Port Description:
  - MTU: 4470
  - Clocking: Line
  - Specific Type: OC3
  - Internal Port: false
  - Ss Ctps Table Size: 0

Callouts in the image:

- 1:** Points to the 'Physical Inventory' tree on the left.
- 2:** Points to the 'Location Information' section.
- 3:** Points to the 'Disable Sending Alarms' button.
- 4:** Points to the 'Port Utilization Graph' section.

1	Poll Now button—Poll the device and update the information as needed. This choice is available for any type of port.
2	Context-Sensitive Buttons—Action buttons (actual buttons depend on port type). In this fiber optic port example, you can also display virtual circuit (VC) information, cross-connect data for incoming and outgoing ports, and encapsulation data for incoming and outgoing traffic.
3	Disable Sending Alarms button—Turns alarms on or off (for advanced users only). This choice is available for any type of port.
4	Port Utilization Graph button—Displays the selected port traffic statistics: Rx/Tx Rate and Rx/Tx Rate History. This choice is not available for ATM, E1/T1, or ATM IMA interfaces that are included in an IMA group.
—	Show DLCI Table button (not displayed)—Displays data-link connection identifier (DCLI) information for the selected port.

If any ports in the inventory are black, it means the item was physically removed. You can verify this by checking its operational status which should display Out.

Although a subinterface is a logical interface defined in a device, Prime Network displays all of its configuration parameters, as shown in [Figure 8-14](#).

**Figure 8-14** Viewing the Configuration Details for a Port with Subinterfaces

The following table lists the subinterface properties that are not self-explanatory. The subinterface configuration determines which properties are displayed. Double-click any properties that are hyperlinks to view additional properties.

Field	Description
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q.
Operational State	Operational state of the subinterface.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface, hyperlinked to the VRF properties in the inventory window.
VRF Name	Name of the VRF.
Is MPLS	Whether this is an MPLS interface: True or False.
VC	Virtual connection (VC) configured on the interface, hyperlinked to the VC Table window. (For more information about VC properties, see <a href="#">Viewing ATM Virtual Connection Cross-Connects</a> , page 26-6.)
Tunnel Edge	Hyperlinked entry to the specific tunnel edge in logical inventory.
Binding	Hyperlinked entry to the specific bridge or pseudowire in logical inventory.

### Viewing the Services That Are Configured on a Port

A physical port's configuration details can include services that are provisioned on the port. Information that is displayed includes:

- Physical layer information.
- Layer 2 information, such as ATM and Ethernet.
- Subinterfaces used by a VRF.

For more information on the services, check the logical inventory. See [Viewing the Logical Properties of a Device \(Traffic, Routing, Information, Tunnels, Data Link Aggregations, Processes\)](#), page 8-21.


## Checking a Port's Utilization

Prime Network provides a tool that displays a port's current Rx/Tx Rate and historical rate information. These graphs are for physical ports only. Port utilization graphs are not available for ATM, E1/T1, or ATM IMA interfaces that are included in an IMA group. Whether you can run these commands depends on your permissions. See [Vision Client Permissions](#), page B-1.

- 
- Step 1** Open the inventory window and select the required port in physical inventory.
- Step 2** In the Ethernet CSMA/CD section, click **Port Utilization Graph**. You may have to scroll down the properties area to display this tool.

The following information is displayed in the Port Statistics dialog box:

Rx Rate	Reception rate (percentage)
Rx Rate History	Graphical representation of reception rate history
Tx Rate	Transmission rate (percentage)
Tx Rate History	Graphical representation of transmission rate history

**Step 3** Click  to close the Port Statistics dialog box.

---

## Disabling a Port's Alarms

By default, alarms are enabled on all ports. If you expect a port to go down, you can disable alarms on the port so that no alarms are generated or displayed in the ticket and events pane. To disable alarms on ports:

- 
- Step 1** Open the inventory window for the required device.
- Step 2** To disable alarms on individual ports, right-click the port and choose **Disable Sending Alarms**. The Sending Alarms field displays the value *false*, indicating that the alarm for the required port has been disabled, and the content pane displays the Enable Sending Alarms button.
- Step 3** To disable alarms on one or more ports at the same time:
- a. In the inventory window, click the **Ports** tab.
  - b. In the Ports table, select the required ports. You can select multiple ports by using the Ctrl and Shift keys.
  - c. Right-click one of the selected ports, and choose **Disable Sending Alarms**. In response, the Sending Alarms field displays the value *false* for the selected ports.
- 

To enable alarms, use the previous procedure but choose **Enable Sending Alarms**.

## Viewing the Pluggable Optics of Break-Out Mode Capable ports in Physical Inventory

An external physical port could be broken down into multiple sub ports if it supports the break out functionality. For example, a 100 Giga port can be broken into ten 10-giga ports. In this case, each and every port must be modeled. However, a single pluggable optic must be maintained for each of these ports.

In Prime Network, the ports and the pluggable optics for a NCS6008 device are modeled separately. The pluggable optic as well as the port must be shown separately and at the same level for this device.

To view the pluggable optic details for a NCS device:

- 
- Step 1** Right-click the NCS device and choose the **Inventory** option.
- Step 2** In the Inventory menu, expand the **Physical Inventory** node.
- Step 3** Choose **Chassis > Slot > port**. In the content pane, view the **Associated Pluggable** field under the **Ethernet CSMA/CD** section. The pluggable transceiver links to the associated slot.



**Note** You can view the **Associated Pluggable** field only when the pluggable transceiver is available in MIB.

---

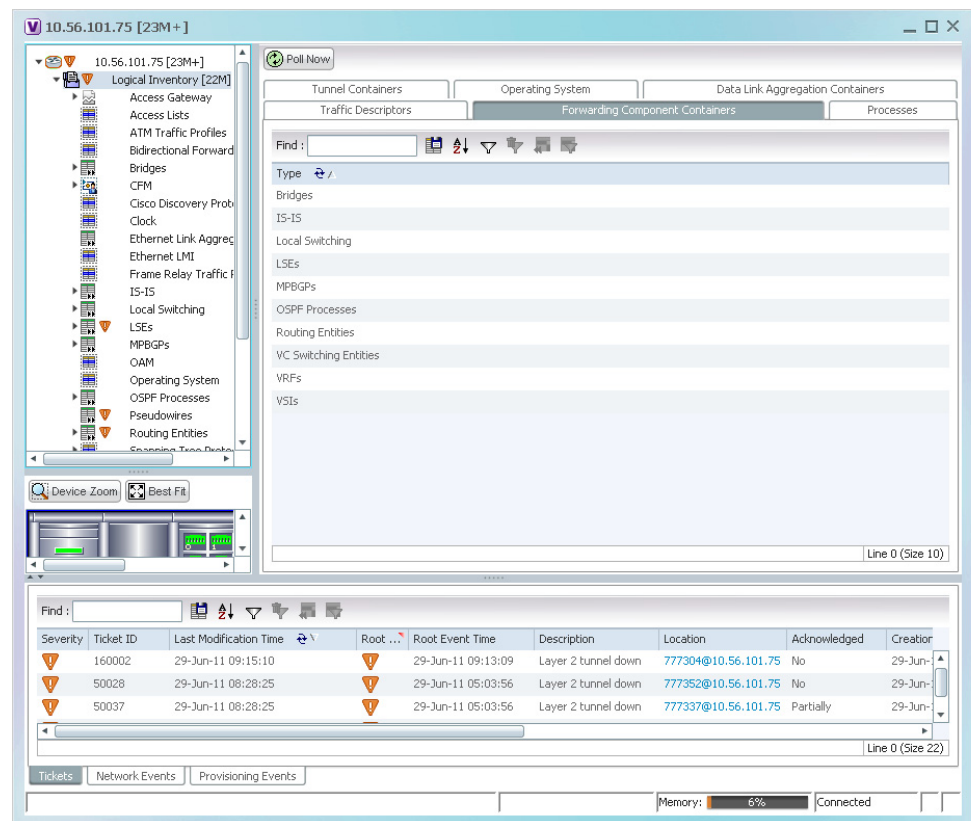
Step 4

Step 5 view the pluggable port in the **Associated Pluggable** field under the **Ethernet CSMA/CD** section.

## Viewing the Logical Properties of a Device (Traffic, Routing, Information, Tunnels, Data Link Aggregations, Processes)

The logical inventory lists configuration data, forwarding, and service-related components that affect traffic handling in the element. Figure 8-15 shows an example of the Forwarding Component Containers for a Cisco 7604 router. All of the items listed in the tab are configured on the device. If something is not displayed, that means it has not been configured on the device.

Figure 8-15 Logical Inventory—Forwarding Components for Cisco 7604 Router



These topics describe the information you can obtain when you click the various Logical Inventory tabs.

- [Viewing a Device's Traffic Descriptors, page 8-22.](#)
- [Viewing a Device's Forwarding Components, Device and VRF Routing Tables, and IP Interfaces, page 8-22.](#)
- [Viewing a Device's Tunneling Containers, page 8-23.](#)

- [Viewing a Device's Data Link Aggregation Containers](#), page 8-23.
- [Viewing Management Processes that Are Running on a Device](#), page 8-23.
- [Viewing a Device's Operating System Details \(and K9 Security\)](#), page 8-25.

## Viewing a Device's Traffic Descriptors

Traffic descriptors can include access lists, ATM and Frame Relay traffic profiles, OAM, forwarding tables, and so forth. To find out which traffic descriptors are configured on a device:

- 
- Step 1** In the Inventory window, choose Logical Inventory.
- Step 2** Click the Traffic Descriptors tab. It lists the traffic descriptors that are configured on the NE—for example, ATM and Frame Relay traffic profiles or OAM.
- Step 3** Click a traffic descriptor container in the logical inventory for information on that container. For example, if you choose **Logical Inventory > OAM**, you can view the OAM local port and its admin status.
- 

## Viewing a Device's Forwarding Components, Device and VRF Routing Tables, and IP Interfaces

To find out which forwarding components are configured on a device:

- 
- Step 1** In the Inventory window, choose Logical Inventory.
- Step 2** Click the Forwarding Components Container tab. It lists the forwarding components that are configured on the NE—for example, bridges, routing entities, local switching, VRFs, and so forth.
- Step 3** Click a forwarding component container in the logical inventory for information on that container. For example, if you choose **Logical Inventory > Routing Entities > Routing Entity**, you can view all interface types configured on the devices, such as Ethernet, GigabitEthernet, loopback, VLAN, and so forth.
- Click the IP Interfaces tab to see the IP address, associated entity, and so forth
  - Click the IPv4 (or IPv6) Routing Table tab to see the destination, hops, and so forth
- 

You can also use the following commands to view a device's routing table and the routing table of a selected VRF. The devices that support these commands are listed in the [Addendum: Additional VNE Support for Cisco Prime Network 5.0](#). Whether you can run these commands depends on your permissions. See [Vision Client Permissions](#), page B-1.

Command	Navigation	Description
Show > IP Route	Logical Inventory > Routing Entities > Routing Entity > Commands	Displays the device routing table.

Command	Navigation	Description
Show > VRF IP route	Logical Inventory > VRFs > VRF > Commands	Displays the routing table of a selected VRF.
Show > IP > Interface Brief	NE > Commands	Lists all IP interfaces on the device.

## Viewing a Device's Tunneling Containers

Tunneling containers can include GRE tunnels, pseudowires, traffic engineering tunnels, and so forth.

- 
- Step 1** In the Inventory window, choose Logical Inventory.
  - Step 2** Click the Tunneling Containers tab. It lists the tunneling containers that are configured on the NE—for example, GRE, pseudowire, traffic engineering tunnels, and so forth.
  - Step 3** Click a tunneling container in the logical inventory for information on that container. For example, if you choose **Logical Inventory > Traffic Engineering Tunnels**, you can view the TE tunnel name, admin and operational status, outgoing label, lockdown status, and so forth.
- 

## Viewing a Device's Data Link Aggregation Containers

Use this procedure to view data link aggregation containers such as Ethernet Link Aggregations. ICL and transport are the two types of ethernet link bundles where ICL link type represents the ethernet link bundle between Cisco ASR 9000 device and satellite chassis or between two satellite chassis. Transport link type represents the ethernet link bundle between two Cisco ASR 9000 devices.

- 
- Step 1** In the Inventory window, choose **Logical Inventory**.
  - Step 2** Choose **Logical Inventory > Ethernet Link Aggregation** to view the aggregation type, bandwidth, aggregation control protocol, load balance type (Source and Destination MAC, Source IP, or Destination IP), link type, and so forth.
- 

## Viewing Management Processes that Are Running on a Device

Use this procedure to find out which management processes are running on a devices. These processes can include BFD, CFM, CDP, clock, E-LMI, ICCP redundancy, IP SLA responder, LLDP, REP, STP, VTP, and so forth.

- 
- Step 1** In the Inventory window, choose Logical Inventory.
  - Step 2** Click the Processes tab. It lists the management processes that are configured on the NE—for example, BFD, LLDP, clock, E-LMI, and so forth.

- Step 3** Click a process container in the logical inventory for information on that container. For example, if you choose **Logical Inventory > Bidirectional Forwarding Detection**, you can view the source and destination IP, the protocols, state, and so forth for a BFD session.

## Viewing Technologies and Services Configured on a Device

The inventory window provides detailed information on the different services and technologies configured on a devices. The Vision client may also provide configuration commands that are specific to those technologies and services. See these topics for information on to drill down into a device's inventory to get this information.

To get information about this technology/service on a device:	See:
Carrier Ethernet—CDP, LLDP, STP, REP, HSRP, access gateways, Ethernet Link Aggregation groups, mLACP, provider backbone, EFPs, EVC services, ethernet flow domains VLANs, unassociated bridges, ethernet flow point cross-connects, VPLS and H-VPLS, Pseudowires, Ethernet services, IP SLA, IS-IS, OSPF	<a href="#">Managing Carrier Ethernet Configurations, page 18-1</a>
Carrier Grade NAT—CGNs, VRFs, address pools	<a href="#">Monitoring Carrier Grade NAT Configurations, page 20-1</a>
DWDM—OTU and ODU alarms, FEC info, counter information, performance statistics	<a href="#">Managing DWDM Networks, page 16-1</a>
CFM, E-LMI, L-OAM	<a href="#">Managing Ethernet Networks Using Operations, Administration, and Maintenance Tools, page 19-1</a>
Y.1731 IPSLA—Performance management statistics and probes	<a href="#">Managing IP Service Level Agreement (IP SLA) Configurations, page 22-1</a>
MPLS services—MPLS over IPv6 (6VPE0, MPLS-TP tunnels, VPNs, VRFs, IP interfaces, MPLS-TE, RSVP, BGP, VRRP, Bundle Ethernet	<a href="#">Managing MPLS Networks, page 17-1</a>
IP and MPLS Multicast nodes and protocols, address family (IPv6) profiles, multicast label switching, multicast routing entities	<a href="#">Monitoring IP and MPLS Multicast Configurations, page 23-1</a>
MToP services—SAToP and CESoPSN pseudowire, virtual connections, IMA groups, TDM, channelization, MLPPP and MLPPP links, MPLS pseudowire over GRE, network clock, CEM and virtual CEM, SONET, APS	<a href="#">Managing Mobile Transport Over Pseudowire (MToP) Networks, page 26-1</a>
SBCs—DBEs, SBEs, performance statistics	<a href="#">Managing Session Border Controllers (SBCs), page 24-1</a>
AAA—AAA groups, dynamic authorization profiles, RADIUS and diameter global configurations, charging configurations	<a href="#">Monitoring AAA Configurations, page 15-1</a>



To get information about this technology/service on a device:	See:
IP pool monitoring and configuration	<a href="#">Managing IP Address Pools, page 14-1</a>
BNG—Policy containers and QoS profiles, BBA groups, subscriber access points, DHCP, dynamic configuration and PPP templates	<a href="#">Monitoring BNG Configurations, page 25-1</a>
Mobile technologies—GPRS/UMTS networks (GGSN, GTPU, APNs, GTPP, eGTP, SGSN); LTE networks (SAE-GW, P-GW, S-GW, QCI-QoS mapping, LAC, HSGW, home agent, foreign agent, ePDG, PDSN, LMA); operator polices, APN remaps and profiles; active charging services	<a href="#">Managing Mobile Networks, page 27-1</a>
Data centers—Virtual port channels, Cisco FabricPath, virtualized resources (hypervisors and compute servers, virtual machines, data stores, clusters, resource pools)	<a href="#">Managing Data Center Networks, page 28-1</a>
Cable technologies—Cable ports and interfaces, upstream and downstream configurations, QAM, DEPI, L2TP, MAC domains, narrowband channels	<a href="#">Monitoring Cable Technologies, page 29-1</a>
ADSL2+ and VDSL2—XDSL traffic descriptors, DSL bonding groups, supported transport models, one-to-one and TLS access profiles	<a href="#">Monitoring ADSL2+ and VDSL2 Technologies, page 30-1</a>

## Viewing a Device's Operating System Details (and K9 Security)

All devices will display the software version running on the device when you open the NE inventory window and select the NE at the very top of the navigation area (see [Figure 8-2 on page 8-3](#) for an example). Depending on the operating system and device type, you can drill down into more operating system details using one of these methods.

If you need to change the software image on an NE, use the procedures described in [Managing Device Software Images, page 9-3](#).



Note

Not all devices will display the same fields; it depends on the device type, operating system, and device configuration.

Open the logical inventory and click the Operating System tab. For groups of devices (such as Nexus data center aggregations), choose **Logical Inventory** > *Nexus management node* > **Operating System**.

Field	Description
Is K9Sec	If the operating system K9 security feature is enabled (true) or disabled (false)
Family	Cisco family, based on the device platform
SDR Mac Addr	(Cisco IOS XR only) Secure Domain Router (SDR) MAC address
Software Version	Operating system software version
Boot Software	System image information
ROM Version	Bootstrap software version

For some Cisco IOS-XR devices, more information will be displayed in the Operating System tab, or by choosing **Logical Inventory > Modular OS**.

Field	Description
Boot Software	System image information
SDR Name	SDR name
SDR Id	SDR identifier
ROM Version	Bootstrap software version
RAM Size	Size (kilobytes) of device processor RAM
<b>OS Packages Table</b>	
Package Info	Package information in the format <i>device:package-version</i> , such as <code>disk0:hfr-admin-3.9.3.14</code>
Package Description	Description of the package, such as FPD (Field Programmable Device) Package
Composite Name	Name of composite package with date and time, such as: Tues Feb 8 20:37:07.966 UTC <code>disk0:comp-hfr-mini-3.9.3.14</code>

## Updating the Inventory (Poll Now)

Prime Network polls devices according to settings that configured when the device is added to Prime Network. By default, Prime Network uses its reduced polling mechanism (also called event-based polling) and polls the device when a configuration change syslog is received. In other words, updates are driven by incoming events. Only the affected areas of the NE are polled, and the modeling information is immediately updated.

For example, if you see in the device inventory properties that an NE is in the Currently Unsynchronized investigation state and you suspect an event was dropped, you should perform a manual poll of the device. Or, if you make a manual device configuration change and want to update the Prime Network model, poll the NE that you reconfigured.

Be sure you perform the poll from the right point in the inventory. Follow the below points:

- If one container is populated or dependent on another table (parent table), update the parent table. For example, the GRE tunnels container and the ARP entities container are generated from the IP Interface table. When the IP Interface table is polled, the IP address will be populated and the GRE tunnel and ARP entity properties will be updated accordingly.
- Perform the poll from the most efficient location in the NE. For example, do not poll the entire device if you only made a small change.

When you are ready to perform the poll, select a device in a map, or an NE in a device's physical or logical inventory, and click **Poll Now**.

## Changing the NE Host Name

This procedure changes the system name of the network device. After you poll the device, the hostname is updated in the Vision client. Because the NE's information is saved by Prime Network using an ID that cannot be modified, all of the NE's information (such as its ticket history) remains associated with

the NE. Whether you can run this command depends on your permissions. See [Permissions for Vision Client NE-Related Operations, page B-4](#). You can verify whether a device supports this command by checking the information in the [Addendum: Additional VNE Support for Cisco Prime Network 5.0](#).

- 
- Step 1** Right-click an NE and choose **Commands > Configuration > System > Remove host name**.
- Step 2** Click **Execute Now** to remove the device's current host name. The device's hostName value is set to null, and the name is deleted from Prime Network object.
- Step 3** Right-click the NE and choose **Commands > Configuration > System > Add host name**.
- Step 4** Enter the new host name and click **Execute Now**.
- Step 5** Right-click the NE and choose **Poll Now** to update the NE information in the Prime Network inventory.
- 

## Changing the SNMP Configuration and Managing SNMP Traps

These commands change these SNMP properties on the real device. If you change the device SNMP configuration, you must also change the settings on the VNE (the model of the device that is maintained by Prime Network). Otherwise, Prime Network will not be able to properly communicate with and model the device. Whether you can run these commands depends on your permissions. See [Appendix B, "Permissions Required to Perform Tasks Using the Prime Network Clients"](#). You can verify whether a device supports these commands by checking the information in the [Addendum: Additional VNE Support for Cisco Prime Network 5.0](#). From Prime Network 5.0 onwards, to collect the inventory data with the device details, the Vision client, the Command builder, Command manager, and Transaction manager communicates with the devices using SNMPv2 PDUs.

To create a Discovery profile with SNMPV2 credentials, user can create or Run a Discovery Profile, create a VNE, run the job. To change the SNMPV2 version, if required, you need to run the script in PN when the Prime Network is in "Down" status. For more information see the "Using Network Discovery to Add VNEs" section in the [Prime Network 5.0 Administrator Guide](#).

- 
- Step 1** Right-click a device in the map, or choose the (top-level) device name in the inventory window.
- Step 2** Use the following commands to change the device configuration. When you launch the command, click **Preview** to see the actual commands that will be sent to the device.

To do the following:	Right-click device and choose:
Change the SNMP configuration (community settings, read-write access control, view-based access control, group settings, and so forth)	<b>Commands &gt; Configuration &gt; System &gt; SNMP &gt; Add SNMP Configuration</b> <b>Commands &gt; Configuration &gt; System &gt; SNMP &gt; Update SNMP Configuration<sup>1</sup></b> <b>Commands &gt; Configuration &gt; System &gt; SNMP &gt; Remove SNMP Configuration</b>
Enable, disable, and remove traps by choosing them from a drop-down list	<b>Commands &gt; Configuration &gt; System &gt; SNMP &gt; Add Traps</b> <b>Commands &gt; Configuration &gt; System &gt; SNMP &gt; Enable Traps</b> <b>Commands &gt; Configuration &gt; System &gt; SNMP &gt; Remove Traps</b>

1. The "Update SNMP configuration" command is not applicable for Cisco UBR10K and RFGW10 cards.

- Step 3** To change the SNMP configuration on the device VNE:
- Right-click the NE and choose **Properties**.
  - Click **VNE Details**.
  - In the VNE properties window, click the SNMP tab and change the settings so they are consistent with the changes you made in the previous step.
  - Click the **Enable SNMP** radio button.



**Note** When VNE is configured to use SNMPV1/V2 for discovery, ensure that the device must also be enabled with SNMPV1.

The screenshot shows the 'asr9k - Properties' dialog box with the 'SNMP' tab selected. The 'Enable SNMP' checkbox is checked. The 'SNMP V2' radio button is selected and highlighted with a red box. Below this, there are sections for 'SNMP V1/V2 Settings' and 'SNMP V3 Settings'. The 'SNMP V1/V2 Settings' section includes fields for 'Community', 'Read', and 'Write', all containing asterisks. The 'SNMP V3 Settings' section includes dropdowns for 'Authentication' and 'Encryption' (both set to 'No'), and text boxes for 'User', 'Password', and 'Password'.

- Click **OK**.

**Step 4** Right-click the NE and choose **VNE Tools > Stop VNE**.

**Step 5** When the device icon turns red, right-click the NE and choose **VNE Tools > Start VNE** and Prime Network will poll the device.

# Changing Device Port Properties and Disabling Ports

The following commands change the port properties of the real device. Whether you can run these commands depends on your permissions. See [Appendix B, “Permissions Required to Perform Tasks Using the Prime Network Clients”](#). You can verify whether a device supports these commands by checking the information in the *Addendum: Additional VNE Support for Cisco Prime Network 5.0*.

- Step 1** Locate the port in the physical inventory.
- Step 2** Change the port configuration using the commands in the following table. When you launch the command, click **Preview** to see the actual commands that will be sent to the device.

To make the following change on a port:	Right-click port in Physical Inventory and choose:
Change port status: Disable (Shutdown) or enable (No Shutdown)  For example, shutting down a port prevents a known fault from continuing to generate events	<b>Commands &gt; Configuration &gt; System &gt; Change Port Status</b>
Configure the descriptive information that is displayed in Prime Network clients when the port is selected such as customer information or business case details)  (You can also label ports using business tags; see <a href="#">Labelling NEs to Associate Them with Customers (Business Tags)</a> , page 4-9)	<b>Commands &gt; Configuration &gt; System &gt; Add Port Description</b>  <b>Commands &gt; Configuration &gt; System &gt; Remove Port Description</b>  <b>Commands &gt; Configuration &gt; System &gt; Update Port Description</b>
Change port characteristics such as bindings, contexts, link aggregations, and so forth	<b>Commands &gt; Configuration &gt; System &gt; Modify Port</b>
Assign a port to a VLAN assignment (enter a VLAN between 1-4094); or deassign a port from a VLAN. When assigned, the port can communicate only with or through other devices in that VLAN. When deassigned, you can move a port to a new VLAN.  Other VLAN actions are described in <a href="#">Working with VLANs</a> , page 18-62.	<b>Logical Inventory &gt; Routing Entities &gt; Routing Entity &gt; interface &gt; Commands &gt; Configuration &gt; Assign Port to Vlan</b>  <b>Logical Inventory &gt; Routing Entities &gt; Routing Entity &gt; interface &gt; Commands &gt; Configuration &gt; DeAssign Port To Vlan</b>

- Step 3** Select the port and click **Poll Now** to synchronize the map information with the new device information.



**Note** Be sure you perform the poll from the right location in the inventory or your changes may not be reflected correctly in Prime Network. See [Updating the Inventory \(Poll Now\)](#), page 8-26.

# Changing Device Interface Properties and Disabling Interfaces

The following commands change the interface properties of the real device. Whether you can run these commands depends on your permissions. See [Appendix B, “Permissions Required to Perform Tasks Using the Prime Network Clients”](#). You can verify whether a device supports these commands by checking the information in the [Addendum: Additional VNE Support for Cisco Prime Network 5.0](#).

- Step 1** Locate the interface in the logical inventory.
- Step 2** Change the interface configuration using the commands in this table. In some cases, a command will affect the interface and its parent port. When you launch the command, click **Preview** to see the actual commands that will be sent to the device.

To make the following change on a port:	Right-click:
Disable or enable an interface and port (for example, disabling faulty interface so it will not continue to generate errors)	<p><b>Logical Inventory &gt; Routing Entities &gt; Routing Entity &gt; interface &gt; Commands &gt; Configuration &gt; System &gt; Enable Interface</b></p> <p><b>Logical Inventory &gt; Routing Entities &gt; Routing Entity &gt; interface &gt; Commands &gt; Configuration &gt; System &gt; Disable Interface</b></p>
Change or remove descriptive information that is displayed in Prime Network clients (for example, customer information or business details) when the interface or port is selected.  (You can also label interfaces and ports using business tags; see <a href="#">Labelling NEs to Associate Them with Customers (Business Tags)</a> , page 4-9.)	<p><b>Logical Inventory &gt; Routing Entities &gt; Routing Entity &gt; interface &gt; Commands &gt; Configuration &gt; Update Interface Configuration</b></p> <p><b>Logical Inventory &gt; Routing Entities &gt; Routing Entity &gt; interface &gt; Commands &gt; Configuration &gt; Remove Interface Configuration</b></p>
Configure a software-only interface that emulates an interface. If the virtual interface receives traffic, it immediately reroutes it back to the device.	<b>Logical Inventory &gt; Routing Entities &gt; Routing Entity &gt; Commands &gt; Configuration &gt; Add Loopback Interface</b>
Configure descriptive information that is displayed in Prime Network clients (for example, customer information or business details) when the interface or port is selected.  (You can also label ports using business tags; see <a href="#">Labelling NEs to Associate Them with Customers (Business Tags)</a> , page 4-9.)	<b>Physical Inventory &gt; interface &gt; Commands &gt; Configuration &gt; Add Interface Configuration</b>

- Step 3** Right-click the appropriate logical inventory routing entity and choose **Poll Now** to synchronize the map information with the new device information.



**Note** Be sure you perform the poll from the right location in the inventory or your changes may not be reflected correctly in Prime Network. See [Updating the Inventory \(Poll Now\)](#), page 8-26.

## Changing Server Settings for DNS, NTP, RADIUS, and TACACs

The following commands change the server settings on the real device. Whether you can run this command depends on your permissions. See [Appendix B, “Permissions Required to Perform Tasks Using the Prime Network Clients”](#). You can verify whether a device supports these commands by checking the information in the *Addendum: Additional VNE Support for Cisco Prime Network 5.0*.

### Configure DNS

Command	Description
DNS > Add DNS Server	Assigns the device to a Domain Name System (DNS) server to manage translating the host name to and from the device IP address.
DNS > Remove DNS Server	

### Configure a Device NTP Server

Command	Description
NTP > Add NTP Server	Assigns the device to a Network Time Protocol (NTP) server to manage clock synchronization.
NTP > Remove NTP Server	

### Configure RADIUS or TACACS Server on Device

Command	Description
TACACS > Add Tacacs Server	Assigns the device to a Terminal Access Controller Access-Control System (TACACS) server to manage authentication (uses TCP or UDP).
TACACS > Remove Tacacs Server	
TACACS+ > Add Tacacs+ Server	Assigns the device to a TACACS+ server to manage authentication (uses TCP).
TACACS+ > Remove Tacacs+ Server	
RADIUS > Add Radius Server	Assigns the device to a Remote Authentication Dial In User Service (RADIUS) server to manage centralized authentication, authorization, and accounting (uses UDP).
RADIUS > Remove Radius Server	

# Suppressing Service Alarms on Virtual Interfaces

In Prime Network Vision, you can suppress or unsuppress virtual interfaces related service alarms by using the Runregtool commands.

You can suppress or unsuppress ipv4/ipv6 virtual interface service alarms on a Device series or VNE levels.

**Table 8-5** Suppress or Unsupress Service Alarms on Device Series Level

<b>Suppress Service Alarms on Devices Series</b>	
<b>Service Alarm Name</b>	<b>Command</b>
Dual Stack IP removed on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore/software versions/default version/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template
Dual Stack IP added on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore/software versions/default version/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template
Dual Stack IP removed on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore-evne/software versions/default version/eventmanager/types//Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template
Dual Stack IP Added on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore-evne/software versions/default version/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/ignore-template
<b>Unsuppress Service Alarms on Device Series</b>	
<b>Service Alarms Name</b>	<b>Command</b>
Dual Stack IP removed on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore/software versions/default version/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/persistent-template



Table 8-5 Suppress or Unsuppress Service Alarms on Device Series Level

Suppress Service Alarms on Devices Series	
Dual Stack IP Added on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/⟨⟨Device_Series_Name⟩⟩/i pcore/software versions/default version/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/persistent -template
Dual Stack IP removed on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/⟨⟨Device_Series_Name⟩⟩/i pcore-evne/software versions/default version/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/persistent -template
Dual Stack IP Added on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/⟨⟨Device_Series_Name⟩⟩/i pcore-evne/software versions/default version/eventmanager/types/Dual stack IP Changed/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/persistent -template

Table 8-6 Suppress or Unsuppress Service Alarms on VNE Level

Suppress Service Alarms	
Service Alarms Name	Command
Dual Stack IP Removed on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm⟨⟨AVM_ID⟩⟩/agents/da/⟨⟨VNE Name⟩⟩/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/ignore-tem plate
Dual Stack IP Added on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm⟨⟨AVM_ID⟩⟩/agents/da/⟨⟨VNE Name⟩⟩/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/ignore-tem plate
Unsuppress Service Alarms	
Service Alarms Name	Command

Table 8-6 Suppress or Unsuppress Service Alarms on VNE Level

Suppress Service Alarms	
Service Alarms Name	Command
Dual Stack IP Removed on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm<<AVM_ID>>/agents/da/<<VNE Name>>/eventmanager/types/Dual stack IP removed on Virtual Interface/default" eventmanager/templates/sub-event/persistent-template
Dual Stack IP Added on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm<<AVM_ID>>/agents/da/<<VNE Name>>/eventmanager/types/Dual stack IP added on Virtual Interface/default" eventmanager/templates/sub-event/persistent-template

You can also suppress or unsuppress virtual interface IPs of false alarms in Tickets on a Device series or VNE.

Use the following commands to suppress or unsuppress Virtual Interface IPs.

Table 8-7 Suppress or Unsuppress Service Alarms on the Tickets Tab

Suppress	
Service Alarms Name	Command
Dual Stack IP Removed on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore/software versions/default version/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP removed on Virtual Interface/is-ticketable" false
Dual Stack IP Added on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/<<Device_Series_Name>>/ipcore-evne/software versions/default version/eventmanager/applications/event-correlation/application-data/sub-applications/com.sheer.metrocentral.framework.eventapplication.eventcorrelation.SendAlarmMessageUtil/types/Dual stack IP added on Virtual Interface/is-ticketable" false
Unsuppress	
Service Alarms Name	Command

Table 8-7 Suppress or Unsuppress Service Alarms on the Tickets Tab

<b>Suppress</b>	
<b>Service Alarms Name</b>	<b>Command</b>
Dual Stack IP Removed on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/⟨⟨Device_Series_Name⟩⟩/ip core/software versions/default version/eventmanager/applications/event-correlat ion/application-data/sub-applications/com.sheer. metrocentral.framework.eventapplication.eventc orrelation.SendAlarmMessageUtil/types/Dual stack IP Changed/Dual stack IP removed on Virtual Interface/is-ticketable" true
Dual Stack IP Added on Virtual Interface	runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/⟨⟨Device_Series_Name⟩⟩/ipco re-evne/software versions/default version/eventmanager/applications/event-correlatio n/application-data/sub-applications/com.sheer.metr ocentral.framework.eventapplication.eventcorrelati on.SendAlarmMessageUtil/types/Dual stack IP Changed/Dual stack IP added on Virtual Interface /is-ticketable" true

Table 8-8 Suppress or Unsuppress in the Tickets Tab on VNE Level

<b>Suppress</b>	
<b>Service Alarms Name</b>	<b>Command</b>
Dual Stack IP Removed on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm⟨⟨AVM_ID⟩⟩/agents/da/⟨⟨VNE Name⟩⟩/eventmanager/applications/event-corr elation/application-data/sub-applications/c om.sheer.metrocentral.framework.eventapplic ation.eventcorrelation.SendAlarmMessageUtil /types/Dual stack IP removed on Virtual Interface/is-ticketable" false
Dual Stack IP Added on Virtual Interface	runRegTool.sh 127.0.0.1 set "avm⟨⟨AVM_ID⟩⟩/agents/da/⟨⟨VNE Name⟩⟩/eventmanager/applications/event-corr elation/application-data/sub-applications/c om.sheer.metrocentral.framework.eventapplic ation.eventcorrelation.SendAlarmMessageUtil /types/Dual stack IP added on Virtual Interface/is-ticketable" false
<b>Unsupress</b>	
<b>Service Alarms Name</b>	<b>Command</b>

Table 8-8 Suppress or Unsuppress in the Tickets Tab on VNE Level

Suppress	
Service Alarms Name	Command
Dual Stack IP Removed on Virtual Interface	<pre>runRegTool.sh 127.0.0.1 set "avm&lt;&lt;AVM_ID&gt;&gt;/agents/da/&lt;&lt;VNE Name&gt;&gt;/eventmanager/applications/event-corr elation/application-data/sub-applications/c om.sheer.metrocentral.framework.eventapplic ation.eventcorrelation.SendAlarmMessageUtil /types/Dual stack IP removed on Virtual Interface/is-ticketable" true</pre>
Dual Stack IP Added on Virtual Interface	<pre>runRegTool.sh 127.0.0.1 set "avm&lt;&lt;AVM_ID&gt;&gt;/agents/da/&lt;&lt;VNE Name&gt;&gt;/eventmanager/applications/event-corr elation/application-data/sub-applications/c om.sheer.metrocentral.framework.eventapplic ation.eventcorrelation.SendAlarmMessageUtil /types/Dual stack IP added on Virtual Interface/is-ticketable" true</pre>

After configuring commands to the device, you can assign the loopback of ipv4 or ipv6 in the Virtual template, change the assignment of loopback of ipv4 or ipv6 in the Virtual template or remove or add the ipv6 or ipv4 address from the loopback.

## Changing Assignment of Loopback for both ipv4 and ipv6 in the Virtual Template

To change the assignment of loopback for both ipv4 and ipv6, follow the below steps:

- 
- Step 1** Log in to a device. For example, asr1k.
  - Step 2** Change the assigned Loopback with ipv4 and ipv6.
  - Step 3** Choose **Logical Inventory > Routing Entities > Routing Entity**, and then click the **Network Events** Tab in the Prime Network Vision and **Service Alarms** Tab in the Prime Network Event Vision to verify the Service Alarms for Virtual Interfaces.
  - Step 4** Execute the RunReg tool to block the Virtual Interfaces. For example, you can use RunReg tool command either at the devices series or VNE Level or in the Tickets tab on device series.
  - Step 5** Repeat steps 1 through 4. The Virtual Interfaces does not show in Prime Network.
-