CHAPTER 3

Manage the Prime Network Components: Gateway, Units, and AVMs

These topics describe the components in the Prime Network system: Gateway, units, AVMs, and VNEs. These topics explain how to check their properties, make changes, and verify their overall health. VNEs are described in greater detail in Configure VNEs and Troubleshoot VNE Problems, page 4-1.

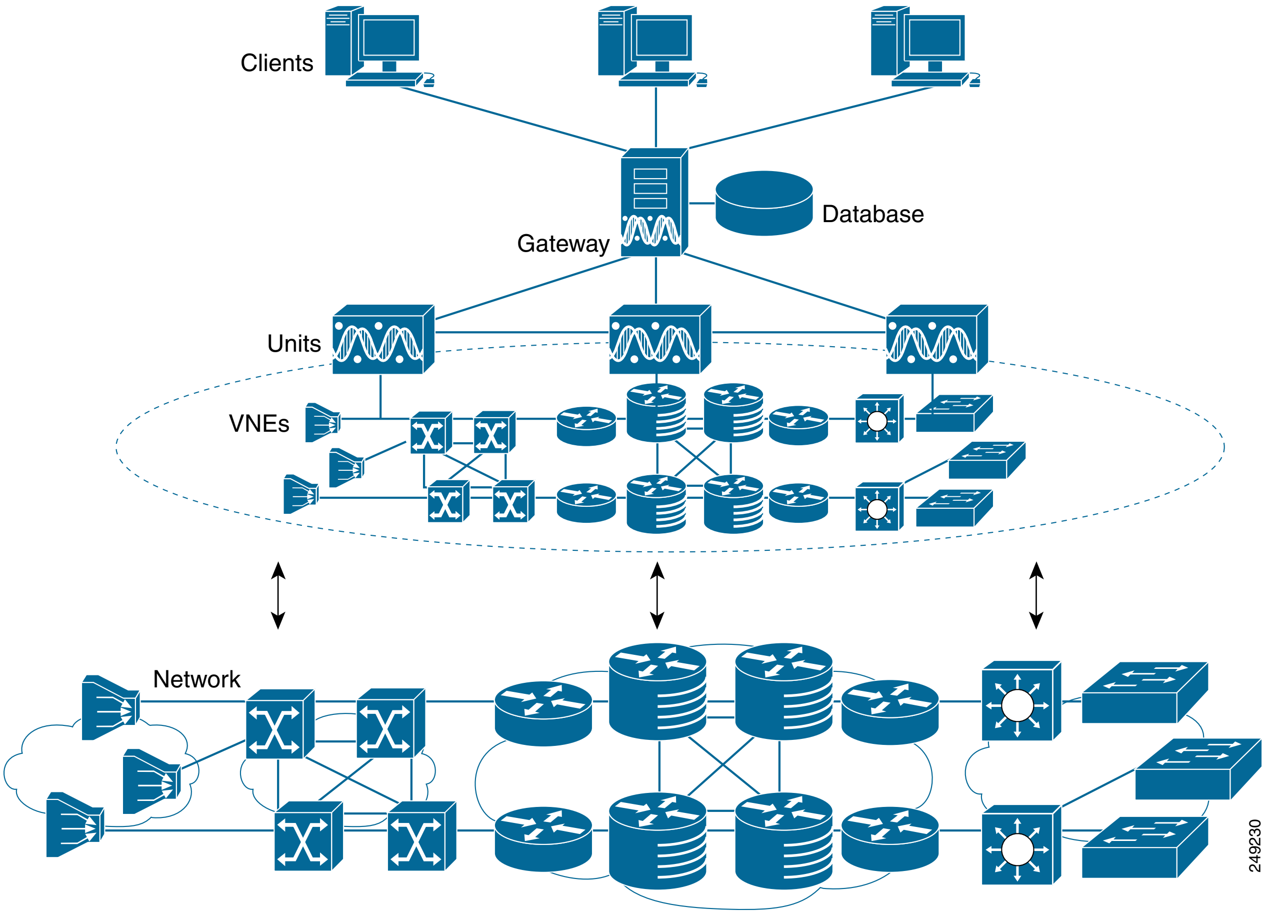
- Prime Network Architecture, page 3-1
- Get Basic Information (Gateway, Unit, AVM, and VNE), page 3-4
- Stop and Restart Prime Network Components, page 3-15
- Manage Client and User Sessions, page 3-20
- Update the Gateway IP Address in Prime Network, page 3-21
- Disable Prime Network Automatic Restarts, page 3-23
- Manage Configurations with Firewalls (Device Proxy), page 3-23
- Configure a Northbound Interface Layer, page 3-26
- Run a Command on All Units, page 3-27
- Delete a Prime Network Unit, page 3-27
- Create and Configure AVMs and Load Balancing, page 3-27
- Check the Overall System and Use the Diagnostics (Graphs Tool), page 3-34
- Track System-Related Events, page 3-43

VNEs are discussed in depth in Configure VNEs and Troubleshoot VNE Problems, page 4-1.

Prime Network Architecture

Prime Network was designed to handle very large and complex networks. The key to Prime Network scalability is its fully distributed, parallel-processing architecture. Elements in that architecture include Virtual Network Elements (VNEs), Autonomous Virtual Machines (AVMs), gateways, and units. For Figure 3-1 shows the Prime Network architecture.

Figure 3-1 Prime Network Architecture



Gateway Layer

The Prime Network gateway layer includes the gateway server, through which all Prime Network GUI client, OSS, and BSS applications access the Prime Network fabric. Each client connects to its designated gateway. The gateway enforces access control and security for all connections and manages client sessions. It maintains a repository for system settings, topological data, and snapshots of active alarms and events. The gateway also maps network resources to the business context, which enables Prime Network to contain information (such as VPNs and subscribers) that is not directly contained in the network and display it to northbound applications.

The gateway AVM process is AVM 11, which supports the majority of foundation services, including inventory and topology snapshots, VNE communications, authentication, authorization, and accounting (AAA) and administration services, session management, plug-ins, alarms, business objects, maps, and application services.

VNE Layer (Units, AVMs, and VNEs)

The Prime Network VNE layer comprises the interconnected fabric of units, AVMs, and VNEs.

Each *unit* manages a group of network elements. Units should be distributed in a way that ensures proximity to their network elements. Prime Network also provides a unit server high availability mechanism to protect the system in case a unit malfunctions. Unit availability is established in the gateway as the gateway runs a protection manager process which continuously monitors all units in the network. If the protection manager detects a unit that is malfunctioning, it automatically signals one of the standby servers in its cluster to load the configuration of the faulty unit (from the system registry), and to take over all of its managed network elements. You can designate a unit to act as an active or standby unit when you add it during installation.

AVMs are Java processes that provide the necessary distribution support platform for executing and monitoring multiple VNEs. As Java processes, AVMs have dedicated memory for executing and monitoring multiple VNEs in a distributed manner. AVMs and VNEs are generally distributed among unit servers in the system, but they can also reside together on a Prime Network gateway server.

Some AVMs are *reserved*, which means they are used by the system; other AVMs are *user-created*, which means they are used to host devices (VNEs). Prime Network contains a watchdog protocol process that monitors the AVMs, and restarts them if they have stopped. This is called AVM protection.

VNEs are autonomous, miniature engines that operate independently and in parallel. Each VNE is in charge of a single device. It maintains a real-time virtual model of the device, including its physical and logical inventories, and its connectivity references to its immediate neighbors. When a VNE is created, it identifies the NE and begins discovery after receiving the IP address and credentials of the NE. Collectively the VNEs maintain the complete inventory and connectivity information of the network. VNEs share information through peer-to-peer messaging that enables intelligent, scalable, cross-network processing, such as discovering connectivity, end-to-end service tracing, and topology-based correlation and root cause analysis.

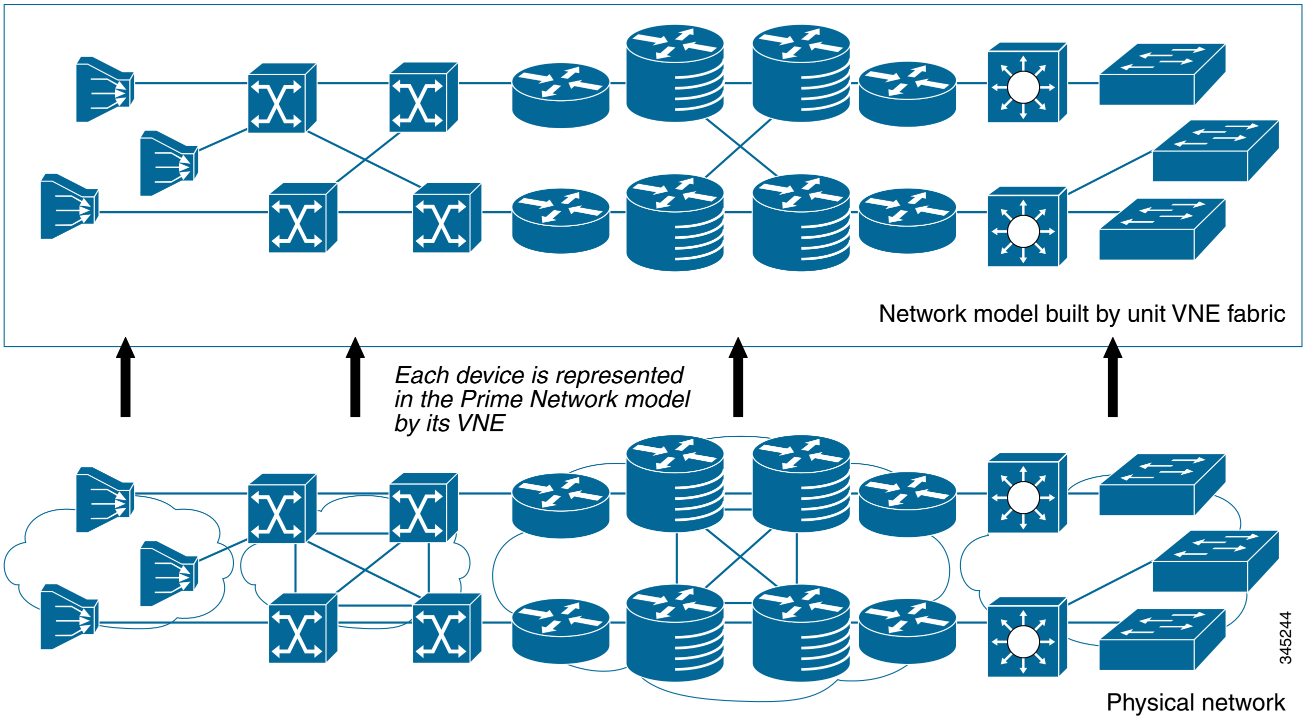
It is important to understand the difference between a VNE entity and a device entity in Prime Network.

- *Device entities* are displayed on maps in the Vision GUI client. From here you can view the device physical and logical inventory, and network-related connections.
- *VNE entities* are displayed in the Administration GUI client. A VNE entity in the Administration GUI client corresponds to a device entity shown on a Vision map. From the Administration GUI client you can check a VNE to see if there are any communication or modeling issues between the VNE and the device it represents.

Managing the network through a fabric of autonomous VNEs ensures scalability by avoiding any single computational bottleneck; it enables the Prime Network platform to grow along with the network. VNEs divide the network into modular self-contained blocks. The VNE layer accommodates network changes by adding or upgrading VNEs whenever network changes occur.

Essentially, the unit VNE fabric builds a virtual shadow of the real network, as shown in Figure 3-2.

Figure 3-2 VNEs Create a Model of the Network


Network model built by unit VNE fabric
Each device is represented in the Prime Network model by its VNE
345244
Physical network

Get Basic Information (Gateway, Unit, AVM, and VNE)

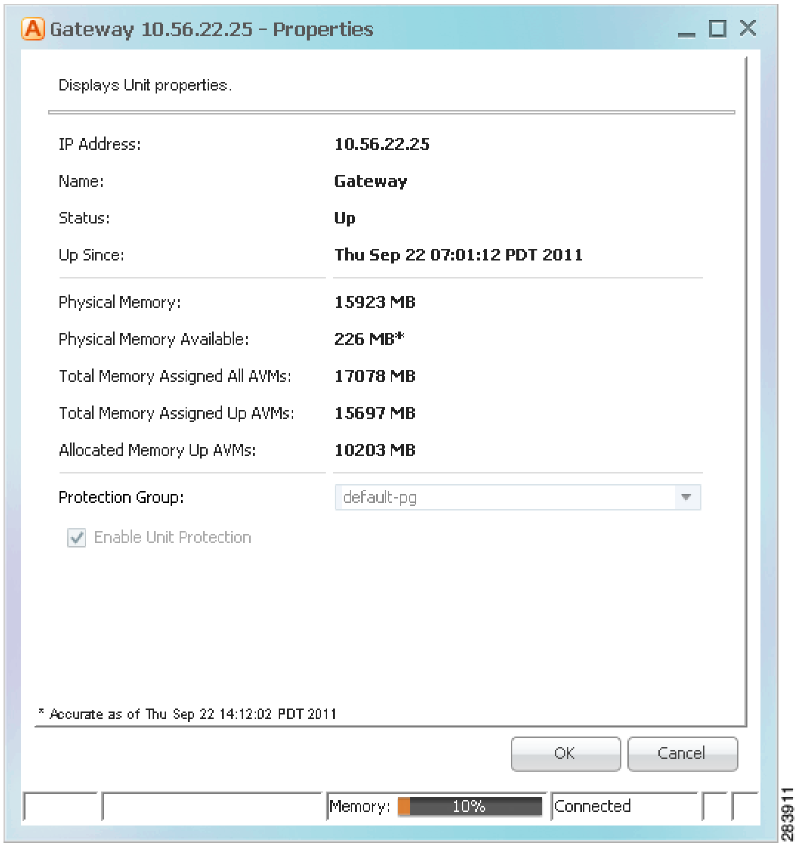
These topics explain how you can get the properties and current status of the Prime Network components:

- Get Gateway Status and Property Information, page 3-5
- Get Unit Status and Property Information, page 3-6
- Get AVM Status and Property Information (Including Reserved AVMs), page 3-8
- Get VNE Status and Property Information, page 3-12

Get Gateway Status and Property Information

The best practice for getting gateway information is to right-click the gateway in the navigation area and select **Properties**, as shown in Figure 3-3. The log for the gateway process is stored in *NETWORKHOME*/Main/logs/11.out.

Figure 3-3 Gateway Status and Properties



Gateway 10.56.22.25 - Properties

Displays Unit properties.

IP Address:	10.56.22.25
Name:	Gateway
Status:	Up
Up Since:	Thu Sep 22 07:01:12 PDT 2011
Physical Memory:	15923 MB
Physical Memory Available:	226 MB*
Total Memory Assigned All AVMs:	17078 MB
Total Memory Assigned Up AVMs:	15697 MB
Allocated Memory Up AVMs:	10203 MB
Protection Group:	default-pg

☑ Enable Unit Protection

* Accurate as of Thu Sep 22 14:12:02 PDT 2011

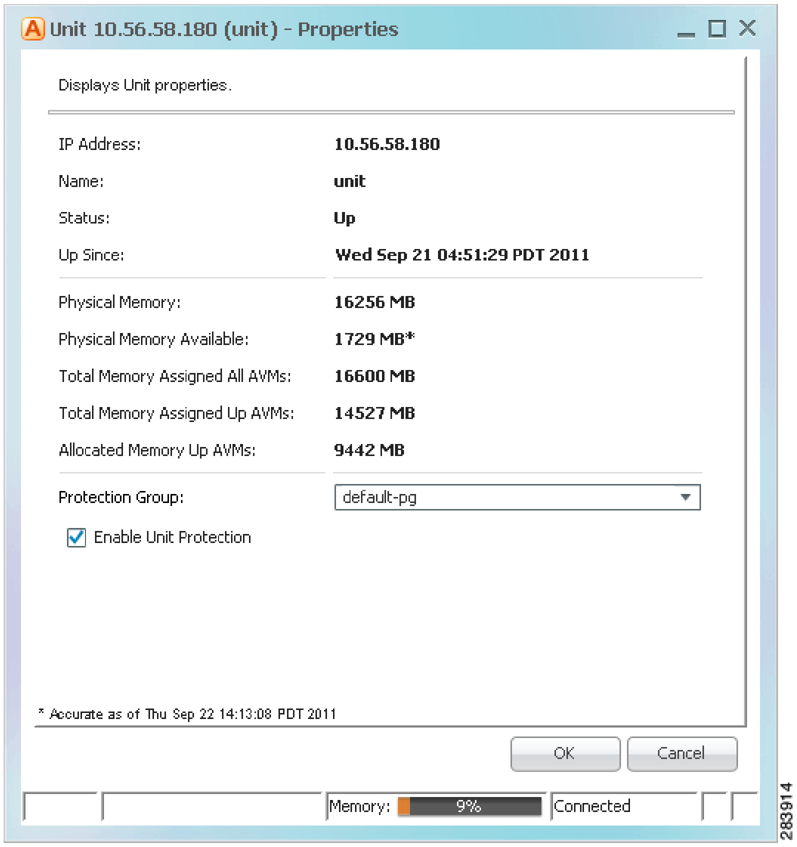
Column	Description
Name	Name of gateway.
IP Address	The IP address of the gateway as defined in Prime Network Administration.
Status	The status of the gateway.
Up Since	The date and time when the gateway was last loaded.
Physical Memory	The total physical memory on the gateway (both free and in use).
Physical Memory Available	Of the total physical memory on the gateway, amount of memory that has not been assigned to any AVMs.

Column	Description
Total Memory Assigned All AVMs	The total physical memory apportioned to all AVMs on the gateway (both user-created and reserved), regardless of whether the AVMs are up or down. This figure does not reflect the memory that is in use (that figure is represented by Allocated Memory Up AVMs). This total includes the additional 35% memory the operating system adds to the AVM size when the AVM is created. (See Add AVMs, page 3-28).
Total Memory Assigned Up AVMs	The total physical memory apportioned to Up AVMs on the gateway (both user-created and reserved AVMs). This figure does not reflect the memory is in use (that figure is represented by Allocated Memory Up AVMs). It includes the additional 35% memory the operating system adds to the AVM size when the AVM is created. (See Add AVMs, page 3-28).
Allocated Memory Up AVMs	The total physical memory being used by Up AVMs on the gateway (both user-created and reserved AVMs).
Protection Group	The cluster group that the gateway belongs to as part of the unit high availability mechanism and cannot be modified. If any units in the cluster go down, a standby unit will take over. By default, the gateway is assigned to the default-pg protection group.
Enable Unit Protection	Indicates that the gateway is using AVM protection and unit server high availability. These are the mechanism that ensure redundancy. They cannot be modified. See Overview of Unit and Process Protection, page 5-1.

Get Unit Status and Property Information

Units are created during the installation process as described in the *Cisco Prime Network 3.10 Installation Guide*. Like the gateway, the best practice for getting unit information is to right-click a unit in the navigation area and select **Properties**. Figure 3-4 provides an example of unit properties.

Figure 3-4 Unit Status and Properties



Displays Unit properties.

IP Address: 10.56.58.180
Name: unit
Status: Up
Up Since: Wed Sep 21 04:51:29 PDT 2011

Physical Memory: 16256 MB
Physical Memory Available: 1729 MB*
Total Memory Assigned All AVMs: 16600 MB
Total Memory Assigned Up AVMs: 14527 MB
Allocated Memory Up AVMs: 9442 MB

Protection Group: default-pg

☑ Enable Unit Protection

* Accurate as of Thu Sep 22 14:13:08 PDT 2011

Table 3-1 Unit Properties

Field	Description	
Name	Name of the unit server.	
IP Address	The IP address of the unit server. Units behind firewalls or NAT devices will have an IP address of **0.0.0.#**. This is an artificial IP address used by the gateway server.	
Status	Up	The unit process is reachable, was loaded, and has started.
	Down	The unit is reachable, but was stopped. This is the status when an **networkctl stop** command is issued. The unit is both operationally and administratively down.
	Unreachable	The unit cannot be reached by the gateway, so it cannot be managed.
	Disconnected	The unit was disconnected from the gateway (normally a temporary measure to address a problem). See Stop Unit Communication with the Gateway (Disconnect), page 3-17.
Up Since	The date and time that the unit was last started.	
Physical Memory	The total physical memory on the unit (both free and in use).	
Physical Memory Available	Of the total physical memory on the unit, amount of memory that has not been assigned to any AVMs.	

Table 3-1 Unit Properties (continued)

Field	Description
Total Memory Assigned All AVMs	The total physical memory *apportioned to all AVMs* (both user-created and reserved), regardless of whether the AVMs are up or down. This figure does not reflect the memory that is in use by AVMs (that figure is represented by Allocated Memory Up AVMs). This total includes the additional 35% memory the operating system adds to the AVM size when the AVM is created. (See Add AVMs, page 3-28).
Total Memory Assigned Up AVMs	The total physical memory *apportioned to Up AVMs* (both user-created and reserved). This figure does not reflect the memory is in use (that figure is represented by Allocated Memory Up AVMs). It includes the additional 35% memory the operating system adds to the AVM size when the AVM is created. (See Add AVMs, page 3-28).
Allocated Memory Up AVMs	The total physical memory being used by Up AVMs (both user-created and reserved AVMs).
Protection Group	If checked, the unit is using unit server high availability. The Protection Group drop-down lists shows the cluster that the unit belongs to. If any units in the cluster go down, a standby unit will take over. By default, all units are assigned to the default-pg protection group.
Enable Unit Protection	Indicates that the gateway is using AVM protection and unit server high availability. These are the mechanism that ensure redundancy. This should always be enabled. See Overview of Unit and Process Protection, page 5-1.

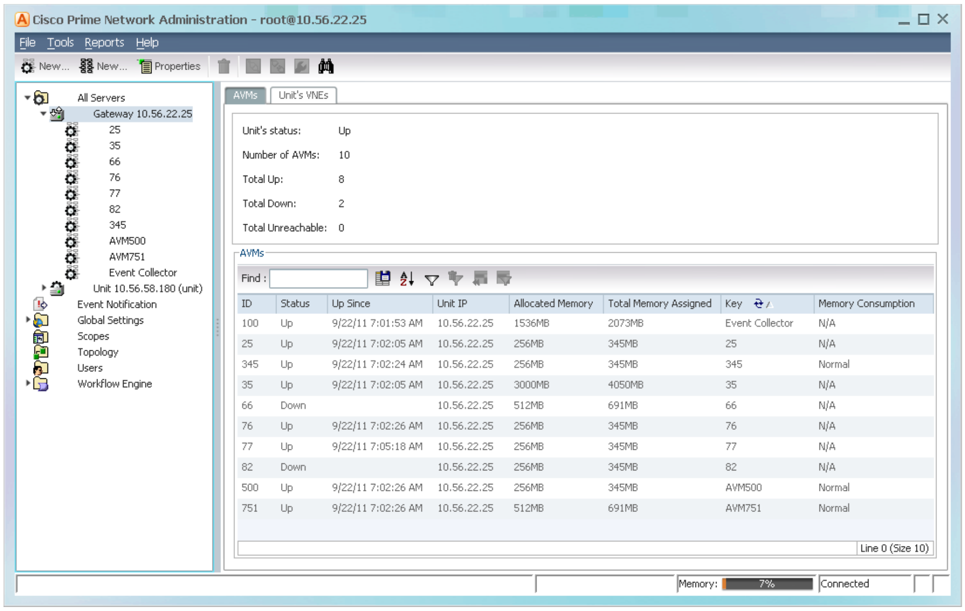
Get AVM Status and Property Information (Including Reserved AVMs)

When you select a gateway server or unit in the navigation tree, Prime Network displays all of its member AVMs. This includes reserved AVMs and user-created AVMs.

Reserved AVMs

Reserved AVMs are created by Prime Network and used for backend purposes. These AVMs cannot be edited or deleted. Some reserved AVMs are only installed on the gateway; others are installed on both the gateway and units. For example, in Figure 3-6, the gateway server has ten system and user-created AVMs.

Figure 3-5 Listing all AVMs in a Unit or Server



Unit's status: Up

Number of AVMs: 10

Total Up: 8

Total Down: 2

Total Unreachable: 0

AVMs

ID	Status	Up Since	Unit IP	Allocated Memory	Total Memory Assigned	Key	Memory Consumption
100	Up	9/22/11 7:01:53 AM	10.56.22.25	1536MB	2073MB	Event Collector	N/A
25	Up	9/22/11 7:02:05 AM	10.56.22.25	256MB	345MB	25	N/A
345	Up	9/22/11 7:02:24 AM	10.56.22.25	256MB	345MB	345	Normal
35	Up	9/22/11 7:02:05 AM	10.56.22.25	3000MB	4050MB	35	N/A
66	Down		10.56.22.25	512MB	691MB	66	N/A
76	Up	9/22/11 7:02:26 AM	10.56.22.25	256MB	345MB	76	N/A
77	Up	9/22/11 7:05:18 AM	10.56.22.25	256MB	345MB	77	N/A
82	Down		10.56.22.25	256MB	345MB	82	N/A
500	Up	9/22/11 7:02:26 AM	10.56.22.25	256MB	345MB	AVM500	Normal
751	Up	9/22/11 7:02:26 AM	10.56.22.25	512MB	691MB	AVM751	Normal

Table 3-2 lists the AVMs that are reserved by Prime Network. You can check the status of these AVMs either using the GUI client or **networkctl**.

Table 3-2 Reserved AVMs

AVM #	Purpose	Is installed on...		Can be checked using[1]...	
		GW	Unit	GUI	networkctl
AVM 0	High Availability/Switch AVM—Enables communication between the unit and other units, as well as the gateway. See Manage Redundancy for Units and Processes, page 5-1.	X	X	—	X
AVM 11	Gateway AVM—Manages the gateway server and other processes running on it. See Manage the Prime Network Components: Gateway, Units, and AVMs, page 3-1.	X	—	—	X
AVM 19	Auto-Add AVM—Used by auto-add mechanism. See How VNE Auto-Add Works, page 4-13.	X	—	—	X
AVM 25	Fault Agent AVM—Processes event information (in each unit), including updates and new correlation information, and generates new tickets when required. See Control Event Monitoring, page 9-1.	X	X	X	X
AVM 35	Service Discovery AVM—Performs Carrier Ethernet service discovery (for example, EVC). For large-scale deployments with many services, the memory for AVM 35 can be increased. (For information on how to do this and other capacity planning tasks, contact your Cisco account representative.)	X	—	—	X
AVM 66	Workflow engine AVM—Defines rules and dependencies to activate business and network processes. See Manage Workflows, Command Scripts, and Activations, page 10-1.	X	—	X	X
AVM 76	Job scheduler AVM/.	X	—	X	X

Table 3-2 Reserved AVMs (continued)

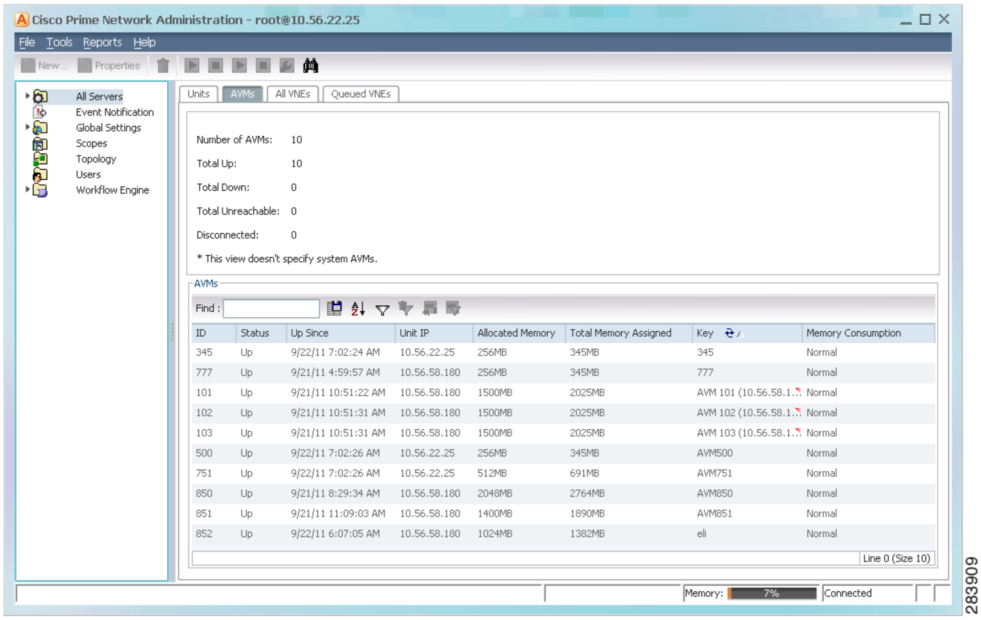
AVM #	Purpose	Is installed on...		Can be checked using[1]...	
		GW	Unit	GUI	networkctl
AVM 77	Reserved for use by Prime Network Change and Configuration Management (when installed).	X	—	X	X
AVM 78	VNE topology AVM—Distributes topology information among VNEs.	X	X	—	X
AVM 83	TFTP Server—Reserved for use by Prime Network Change and Configuration Management (when installed) if using TFTP.	X	X	—	X
AVM 84	Reports AVM—Manages the reporting framework.	X	—	—	X
AVM 99	Management AVM—Manages the unit and the other AVMs running on the unit (or gateway, if there are no separate units).	X	X	—	X
AVM 100	Event Collector AVM—Listens for and receives traps and syslog notifications from devices, and forwards them to corresponding VNEs. See Control Event Monitoring, page 9-1.	X	X	X	X

[1] You can also check AVM status using the system health and diagnostics tool; see Check the Overall System and Use the Diagnostics (Graphs Tool), page 3-34.

AVM Properties

If you select All Servers and click the All AVMs tab, Prime Network displays all of the user-created AVMs in the entire system. For example, in Figure 3-6, the entire system has 10 user-created AVMs.

Figure 3-6 Listing all User-Created AVMs in Prime Network



Number of AVMs: 10
Total Up: 10
Total Down: 0
Total Unreachable: 0
Disconnected: 0
* This view doesn't specify system AVMs.

AVMs

ID	Status	Up Since	Unit IP	Allocated Memory	Total Memory Assigned	Key	Memory Consumption
345	Up	9/22/11 7:02:24 AM	10.56.22.25	256MB	345MB	345	Normal
777	Up	9/21/11 4:59:57 AM	10.56.58.180	256MB	345MB	777	Normal
101	Up	9/21/11 10:51:22 AM	10.56.58.180	1500MB	2025MB	AVM 101 (10.56.58.1...	Normal
102	Up	9/21/11 10:51:31 AM	10.56.58.180	1500MB	2025MB	AVM 102 (10.56.58.1...	Normal
103	Up	9/21/11 10:51:31 AM	10.56.58.180	1500MB	2025MB	AVM 103 (10.56.58.1...	Normal
500	Up	9/22/11 7:02:26 AM	10.56.22.25	256MB	345MB	AVM500	Normal
751	Up	9/22/11 7:02:26 AM	10.56.22.25	512MB	691MB	AVM751	Normal
850	Up	9/21/11 8:29:34 AM	10.56.58.180	2048MB	2764MB	AVM850	Normal
851	Up	9/21/11 11:09:03 AM	10.56.58.180	1400MB	1890MB	AVM851	Normal
852	Up	9/22/11 6:07:05 AM	10.56.58.180	1024MB	1382MB	eli	Normal

Line 0 (Size 10)

The fields in the AVM table are described in Table 3-1. To see which fields are editable, right-click an AVM and select properties (refer to Table 3-4).

Table 3-3 AVM Properties in AVMs List

Field	Description	
ID	The AVM ID. This cannot be changed once the AVM is created. If Prime Network created the AVM using auto-add, it used the first available 3-digit number starting at 101.	
Status	Starting Up	When a **Start** (command) option is issued.
	Up	The AVM process is reachable, was loaded, and has started. This is the status when the AVM is created (and you selected Activate Upon Creation), and no problems are encountered.
	Shutting Down	When a **Stop** (command) option is issued and, while the command is being run, some processes are still running, the status of the AVM is Shutting Down.
	Down	The AVM process is reachable, but was stopped. This is the status when a **Stop** (command) is issued. The AVM is both operationally and administratively down.
	Unreachable	The AVM process cannot be reached by the gateway, so the AVM cannot be managed.
	Disconnected	The AVM is on a unit that was disconnected from the gateway (the unit has a Disconnected status).
Unit Data	IP Address	IP address of the parent unit server. Units behind firewalls or NAT devices will have an IP address of **0.0.0.#**. This is an artificial IP address used by the gateway server.
	Available Memory	The amount of memory that is currently available on the parent unit (note time stamp).
Allocated Memory	The total physical memory being used by the AVM. This field is editable but changing it requires an AVM restart to apply the change.	
Total Memory Assigned	The total physical memory assigned to the AVM when it was created. (The operating system adds an additional 35% to the AVM size. This additional memory is used by the operating system for backend tasks, leaving the desired amount of memory for use by VNEs.)	
Key	The name of the AVM as defined in Prime Network. The key uniquely identifies an AVM in the Prime Network system, across all units, thus enabling a transparent failover scenario in the system. Note that the key can be different from the ID (AVM number); the ID is listed in the AVMs table when you select the parent unit or gateway server. This field is editable but requires an AVM restart.	
	Auto-added AVMs	**AVM** *ID* **(**u*nit-ip***)**
	Manually created AVMs	**AVM***ID_nnn* (where *nnn* is a unique designator assigned by Prime Network)

Table 3-3 AVM Properties in AVMs List (continued)

Field	Description	
Memory Consumption	Indicates whether the AVM has surpassed its warning memory consumption warning threshold. Supported values are:	
	N/A	The AVM is a system AVM; memory consumption is not applicable.
	Normal	The AVM is within normal memory consumption.
	High	The AVM has exceeded its threshold and you should adjust its load. See Update the Gateway IP Address in Prime Network, page 3-21.

If you right-click a specific AVM and choose **Properties**, you can view the following additional details the AVMs. If you edit any fields, you must restart the AVM to apply your changes.

Table 3-4 Enable AVM Protection

Field	Description
Enable AVM Protection	If the check box is checked, AVM protection (the watchdog protocol) is enabled. For more information, see Chapter 5, "Manage Redundancy for Units and Processes". **Note** It is highly recommended that you do not disable this option if unit server high availability is enabled. If you change the option when the AVM is up, you must disable and re-enable the AVM for the change to take effect. This field is editable.

When moving an AVM, its status has a bearing on whether the process is automatically restarted. If its status is Up, it is restarted; if its status is down, it is not restarted. For more information about moving AVMs, see Move and Delete AVMs, page 3-33.

You can also get AVM diagnostic information using the system health and diagnostics tool. The tool provides a drill down feature so you can check user-defined AVMs health, errors or exceptions, and GC prints. See Check the Overall System and Use the Diagnostics (Graphs Tool), page 3-34.

Get VNE Status and Property Information

VNEs are the central building blocks of the Prime Network system. Each VNE is an autonomous, miniature engine that is in charge of a single device. But a VNE is an entity that only exists within Prime Network; the real device is a separate entity. These topics explain how to get basic status and property information for a VNE.

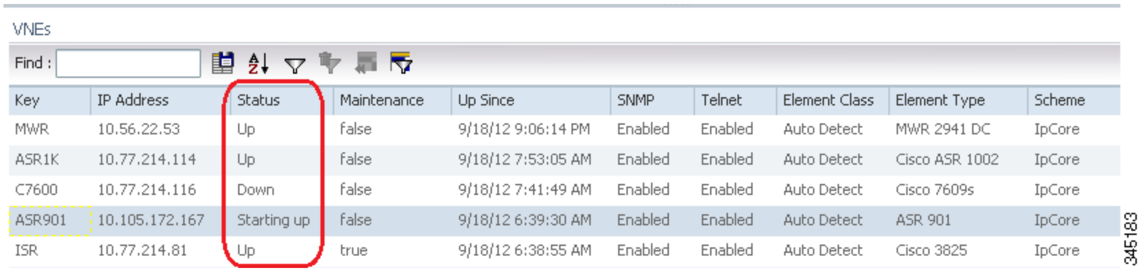
The VNE process must be completely functional in order for Prime Network to properly model and monitor a device. This administrative condition of the VNE is expressed through the *VNE status*.

For information on VNE investigation, modeling, and communication, and how to add or change VNEs, see Configure VNEs and Troubleshoot VNE Problems, page 4-1.

VNE Status

Figure 3-7 illustrates where the status of VNEs running on a selected AVM.

Figure 3-7 VNE Status in AVM Window



VNEs

Find :

Key	IP Address	Status	Maintenance	Up Since	SNMP	Telnet	Element Class	Element Type	Scheme
MWR	10.56.22.53	Up	false	9/18/12 9:06:14 PM	Enabled	Enabled	Auto Detect	MWR 2941 DC	IpCore
ASR1K	10.77.214.114	Up	false	9/18/12 7:53:05 AM	Enabled	Enabled	Auto Detect	Cisco ASR 1002	IpCore
C7600	10.77.214.116	Down	false	9/18/12 7:41:49 AM	Enabled	Enabled	Auto Detect	Cisco 7609s	IpCore
ASR901	10.105.172.167	Starting up	false	9/18/12 6:39:30 AM	Enabled	Enabled	Auto Detect	ASR 901	IpCore
ISR	10.77.214.81	Up	true	9/18/12 6:38:55 AM	Enabled	Enabled	Auto Detect	Cisco 3825	IpCore

This status is entirely user-directed, and is controlled by right-clicking the VNE and choosing an action. Table 3-5 lists the status you may see in a table of VNEs.

Table 3-5 VNE Status

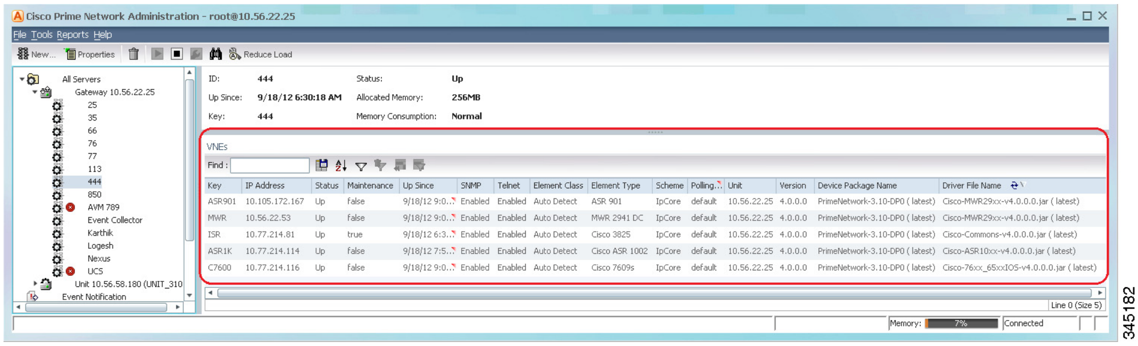
VNE Status	Description
Starting Up	A **Start** (command) option was issued.
Up	The VNE process is reachable, was loaded, and has started. This is the status when a **Start** command is issued (or when you create a VNE and choose **Start** as its initial status), and no problems are encountered (such as an overloaded server). You can move a VNE to maintenance mode to temporarily disable alarm processing. The VNE status will be Up but the value for Maintenance will be True.
Shutting Down	A **Stop** (command) option was issued and, while the command is being run, some processes are still running, the status of the VNE is Shutting Down.
Down	The VNE process is reachable, but was stopped. This is the status when a **Stop** command is issued. The VNE is both operationally and administratively down. VNEs that were in maintenance mode will move to the Down state in the following circumstances: • The VNE or AVM was moved. • The AVM was restarted, the unit was disconnected or switched to a standby server, or the gateway was restarted.
Unreachable	The VNE cannot be reached by the gateway, so the VNE cannot be managed. (Note that this is the VNE status, not the device status; the device may be fully reachable. See What is the Difference Between a VNE and a Device?, page 4-1.)
Disconnected	The VNE is on a unit that was disconnected from the gateway (the unit has a Disconnected status).

VNE Properties

VNEs can have a wide range of properties depending on how they were created. When a VNE is created, it identifies the NE by vendor, device family, device subfamily, device type and software version. Once the NE type is determined, the VNE begins discovery after receiving the IP address and credentials of a specific NE. It collects the basic inventory of the system, both physical and logical, and attempts to determine its place in the network topology.

You can get a wide range of information about a VNE by choosing its host AVM and looking at the VNEs table. Figure 3-8 shows an example of an AVM's VNEs table in the Administration GUI client.

Figure 3-8 List of VNEs in AVM Window



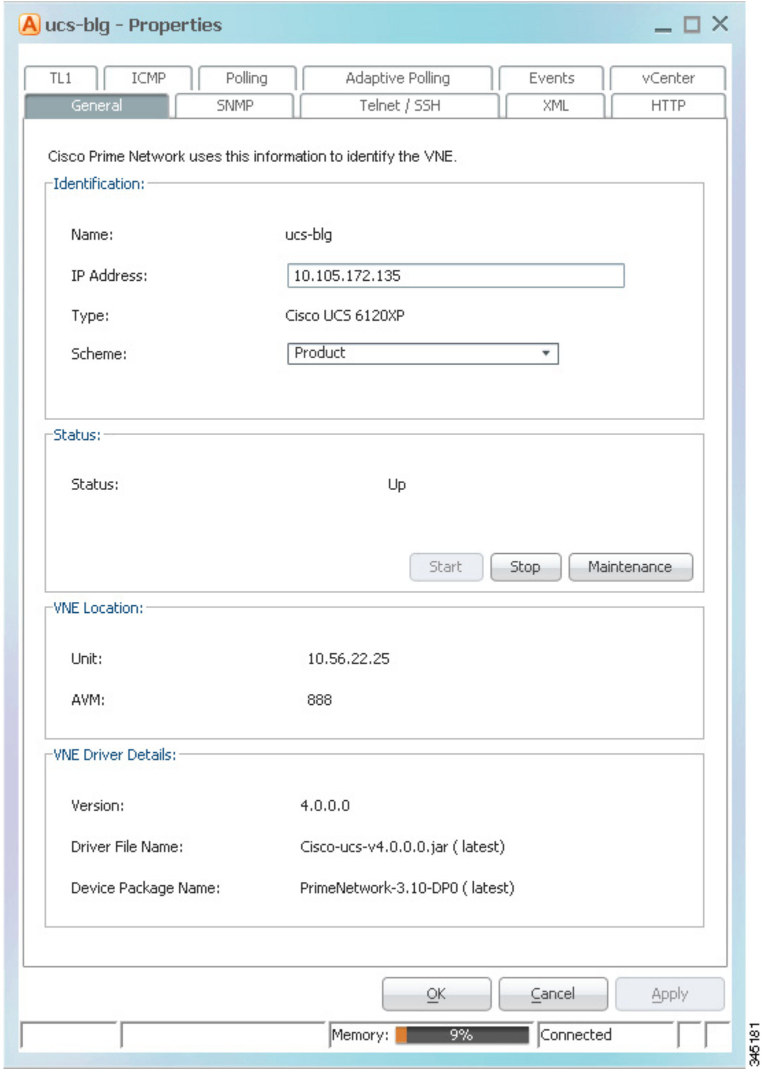
ID: 444 Status: Up
Up Since: 9/18/12 6:30:18 AM Allocated Memory: 256MB
Key: 444 Memory Consumption: Normal

Key	IP Address	Status	Maintenance	Up Since	SNMP	Telnet	Element Class	Element Type	Scheme	Polling...	Unit	Version	Device Package Name	Driver File Name
ASR901	10.105.172.167	Up	false	9/18/12 9:0...	Enabled	Enabled	Auto Detect	ASR 901	IpCore	default	10.56.22.25	4.0.0.0	PrimeNetwork-3.10-DP0 (latest)	Cisco-MWR29xx-v4.0.0.0.jar (latest)
MWR	10.56.22.53	Up	false	9/18/12 9:0...	Enabled	Enabled	Auto Detect	MWR 2941 DC	IpCore	default	10.56.22.25	4.0.0.0	PrimeNetwork-3.10-DP0 (latest)	Cisco-MWR29xx-v4.0.0.0.jar (latest)
ISR	10.77.214.81	Up	true	9/18/12 6:3...	Enabled	Enabled	Auto Detect	Cisco 3825	IpCore	default	10.56.22.25	4.0.0.0	PrimeNetwork-3.10-DP0 (latest)	Cisco-Commons-v4.0.0.0.jar (latest)
ASR1K	10.77.214.114	Up	false	9/18/12 7:5...	Enabled	Enabled	Auto Detect	Cisco ASR 1002	IpCore	default	10.56.22.25	4.0.0.0	PrimeNetwork-3.10-DP0 (latest)	Cisco-ASR10xx-v4.0.0.0.jar (latest)
C7600	10.77.214.116	Up	false	9/18/12 9:0...	Enabled	Enabled	Auto Detect	Cisco 7609s	IpCore	default	10.56.22.25	4.0.0.0	PrimeNetwork-3.10-DP0 (latest)	Cisco-76xx_65xxIOS-v4.0.0.0.jar (latest)

Column	Description
Key	The VNE name.
IP Address	The IP address of the device as defined in Prime Network Administration.
Status	Status of the VNE: Starting Up, Up, Shutting Down, Down, or Unreachable.
Maintenance	Indicates whether the VNE is (true) or is not (false) in maintenance mode.
Up Since	Date and time that the VNE was last started.
SNMP	Indicates whether SNMP is enabled (true) or disabled (false) on the VNE.
Telnet	Indicates whether Telnet is enabled (true) or disabled (false) on the VNE.
Element Class	VNE category, such as Auto Detect, Generic SNMP, Cloud, or ICMP.
Element Type	Device type (manufacturer name), such as Cisco 7204.
Scheme	Determines what data should be retrieved for each device, and which commands and protocols Prime Network should use to collect that data.
Polling Group	The name of the polling group. The entry in this column is blank if the polling group is an instance.
Unit	Name of the parent unit.
Version	Version of the VNE device driver that the VNE is currently using.
Device Package Name	Device Package that is installed on the gateway server. You can use this and the driver file name information to verify whether a newer driver is available, which might supply additional functionality.
Driver File Name	VNE device driver that is currently being used by the VNE.

To retrieve all of a VNE's properties, launch its Properties dialog. Figure 3-9 illustrates a VNE properties dialog.

Figure 3-9 VNE Properties



Cisco Prime Network uses this information to identify the VNE.

Identification:

Name: ucs-blg

IP Address: 10.105.172.135

Type: Cisco UCS 6120XP

Scheme: Product

Status:

Status: Up

VNE Location:

Unit: 10.56.22.25

AVM: 888

VNE Driver Details:

Version: 4.0.0.0

Driver File Name: Cisco-ucs-v4.0.0.0.jar (latest)

Device Package Name: PrimeNetwork-3.10-DP0 (latest)

Memory: 9%

Connected

All of the VNE properties are described in detail in VNE Properties Reference, page D-1. For information on how to add, manage, delete, and troubleshoot VNEs, see Configure VNEs and Troubleshoot VNE Problems, page 4-1.

Stop and Restart Prime Network Components

If you stop and restart the gateway server, you stop all active queries, flows, and transactions being run on the gateway, all units, all AVMs, and all VNEs. If you make changes to a component, such as an AVM, you normally only have to restart the individual component to apply your changes. If you install a new VNE driver, you only need restart the VNE, not the hosting AVM.

Note By default, Prime Network automatically restarts when the gateway server is rebooted. To disable this behavior, see Disable Prime Network Automatic Restarts, page 3-23.

Table 3-6 Impact of Stopping a Prime Network Component

Stopping this component...	...Stops all active queries, flows, and transactions on:	To stop or change a component's status, see:
VNEs	The single VNE. It may affect NEs to which it is connected. You can restart a VNE from the GUI client.	Stop, Start, and Move VNEs to Maintenance Mode, page 4-9
AVMs	The AVM, and all VNEs hosted by the AVM. You can restart an AVM from the GUI client. All VNEs in Maintenance mode are moved to Down.	Change AVM Status (Start or Stop), page 3-33
Units	The unit, all AVMs hosted by the unit, and all VNEs hosted by the AVMs. All VNEs in Maintenance mode are moved to Down. This action may cause VNEs to be reported as unreachable until the handshake protocols are complete. Upon restart, all AVMs are restarted at the same time which can be a resource-intensive operation. Consider gradually restarting all AVMs using the Administration GUI client. If you need more control, you can configure AVMs to not restart when the unit is restarted.	Stop Unit Communication with the Gateway (Disconnect), page 3-17 or Restart Prime Network In a Gradual Manner, page 3-18
Gateway	The gateway, all units hosted by the gateway, all AVMs hosted by the units, and all VNEs hosted by the AVMs. All VNEs in Maintenance mode are moved to Down. Same impact as for units, times the number of units in the system. **Note** If you are using gateway server high availability, start and stop the gateway using the appropriate application or CLI commands, not **networkctl**. Stopping the applications using the regular application commands without the awareness of the cluster software can cause the service group to failover.	Use networkctl to Stop and Start Components, page 3-19 or Restart Prime Network In a Gradual Manner, page 3-18

If you need to restart Prime Network but want to restart AVMs in a controlled manner, see Restart Prime Network In a Gradual Manner, page 3-18.

Stop Unit Communication with the Gateway (Disconnect)

Disconnecting a unit allows you to temporarily stop unit-gateway communication so you can fix the unit problem without having to reinstall the unit when you are done (units can only be added using the installation script). For example, say a unit's Ethernet card goes down and the unit becomes unreachable. You could do the following:

1. Disconnect the unit from the gateway, and move all AVMs and VNEs to a temporary unit.
2. Fix the Ethernet card problem.
3. Reconnect the unit to the gateway.
4. Move all AVMs and VNEs back to the unit.

As this scenario shows, even if a unit is in the Disconnected state, you can still, add, delete, start, stop, and update AVMs and VNEs on the unit.

Disconnecting a unit that is part of a protection group does not trigger starting the standby unit because unit protection is also disabled on the active unit that is being disconnected. Prime Network will not allow you to disconnect a unit that is the designated standby unit.

Reconnecting the unit restarts the unit and all AVMs and VNEs. Unit information is uploaded to the gateway server, and registry information is downloaded to the unit from the gateway.

Note Before you disconnect a unit, if the Event Collector (AVM 100) is enabled on the unit, enable an Event Collector on *another* unit or the system will drop events. You must configure devices to forward events to the new Event Collector, and enable AVM 100 on another unit, as described in Enabling a New Event Collector on a Unit, page 9-12.

To disconnect a unit:

Step 1 In the Prime Network Administration window, select **All Servers**.

Step 2 Right-click the unit and choose **Disconnect**.

Step 3 If the unit is running, a warning will be displayed that says

Step 4 Confirm your choice. You can now delete the unit as described in Delete a Prime Network Unit, page 3-27.

Similarly, if you want to reconnect a unit, right-click the unit and choose **Connect**.

Restart Prime Network In a Gradual Manner

Note If you are using gateway server high availability, start and stop the gateway using the Veritas Cluster Manager application or CLI commands, not **networkctl**. Stopping the applications using the regular application commands without the awareness of the cluster software can cause the service group to failover.

When you use the **networkctl start** or **restart** command, all user-defined AVMs (AVMs containing VNEs) start at the same time. This can be a resource-intensive operation on a very loaded system. It can also cause unwanted side effects for systems with an external authentication server (such as TACACS). In such cases, it is better to gradually start all AVMs.

If the Prime Network system is running, you can use the Prime Network Administration GUI to bring up AVMs one by one. However, because the AVMs normally restart in a manner of minutes, this method may not give you the control you want. You can reconfigure AVMs to *not* restart when the system is restarted. Then you can start the AVMs manually, once Prime Network Administration is running.

Disable the user-defined AVMs on each unit, as follows.

Note Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

Before You Begin

Prepare a list of the AVMs you do not want to automatically restart, and the IP addresses of the units that are hosting the AVMs.

Step 1 Log into the gateway as *pnuser* (where *pnuser* is the operating system account for the Prime Network application, created when Prime Network is installed; an example of *pnuser* is **pn310**).

Step 2 Change to the Main directory by entering the following command:

```
# cd $ANAHOME/Main
```

Step 3 For each AVM you do not want to auto-restart, change the registry key named **enable** to **false** using the **runRegTool.sh** script:

- For user-created AVMs that are hosted by the gateway server, use the following command:

  runRegTool.sh -gs *gateway-IP* **set 127.0.0.1 “avm99/services/bsm/***avm-id***/enable” false**

  In this example, the AVM ID is 207 and is hosted by the gateway:

  ```
  # ./runRegTool.sh -gs 127.0.0.1 set 127.0.0.1 "avm99/services/bsm/avm207/enable" false
  ```

- For user-created AVMs that are hosted by another unit, use the following command:

  runRegTool.sh -gs *gateway-IP* **set** *unit-IP* **“avm99/services/bsm/***avm-id***/enable” false**

  In this example the AVM is AVM 30, and it is hosted by a unit with the IP address 172.23.240.12:

  ```
  # ./runRegTool.sh -gs 127.0.0.1 set 172.23.241.12 "avm99/services/bsm/avm301/enable"
  false
  ```

Step 4 When you have finished reconfiguring the AVMs, restart the gateway:

```
# cd $ANAHOME/Main
# networkctl restart
```

Step 5 Gradually start the individual AVMs using the Prime Network Administration GUI (see Change AVM Status (Start or Stop), page 3-33).

Note You should monitor the unit's CPU usage while starting an AVM, and only start additional AVMs when the unit CPU usage is stable.

Use networkctl to Stop and Start Components

Note By default, Prime Network automatically restarts if the gateway is rebooted. To disable this behavior, see Disable Prime Network Automatic Restarts, page 3-23.

You can use the **networkctl** command to check the status of all unit processes (including user-created AVMs). Restarting a unit stops all AVM and VNE processes on the unit, and then restarts them. Because system saves information within the process memory, restarting a unit causes some of the information to disappear. Therefore, recovering all information that was stored in the process memory prior to the restart takes as long as the longest full system polling cycle. Data that was persisted (stored in the unit) is available immediately. (Persistency is described in Change Settings That Control VNE Data Saved After Restarts, page 12-37.

Keep these items in mind when restarting a unit:

- Some of the VNEs running on the unit will be reported as unreachable.
- All active queries, flows, and transactions that are currently being run within the unit's VNEs are stopped.

To start or restart a unit:

Step 1 Log into the *unit server* as *pnuser* and change to the Main directory:

```
# cd $ANAHOME/Main
```

Step 2 Enter the following, substituting **start** or **restart** for *option*:

```
# networkctl option
```

The unit begins loading. The process might take a while to complete.

For more information on working with AVMs and understanding their status, see Get AVM Status and Property Information (Including Reserved AVMs), page 3-8.

Manage Client and User Sessions

These topics explain how to use the Session Manager GUI to monitor and terminate user sessions, how to set a system-wide idle time for all client sessions, and how to configure the maximum number of client sessions that can be open at one time.

- Monitor and Terminate User Sessions, page 3-20
- Configure Session Idle Times and Maximum System-Wide Sessions, page 3-20

Monitor and Terminate User Sessions

The Session Manager GUI helps you manage all Prime Network GUI and NBI client sessions. You can terminate sessions and ask users to log back in, or just kill sessions completely. The Session Manager uses the HTTPS protocol and authentication method.

To open the Session Manager, enter **`https://`*`gateway_ip`*`:6081/ana/services/session_mgr`** in your browser where *`gateway_ip`* is the gateway IP address. The Session Manager lists the following information about currently open sessions for that gateway.

Table 3-7 Information Displayed by Session Manager

Field	Description
Session ID	Session identifier (internal).
Application	Prime Network client application being used: Prime Network Vision, Prime Network Manage (Administration), or eventvision (Prime Network Events). No application is listed for the NBI.
Client Type	Prime Network client type being used: STLS (web), bql (BQL NBI), or app (application).
User ID	User identifier (internal).
Username	Name of user that is logged into the session.
Client ID	Client identifier (internal).
CAS	If true, indicates that the user authentication was performed by Central Authentication Server (the user navigated to the Session Manager from a ticket or from a Cisco Prime Central installation).
Manage	Tools for administering the session: • **kill** terminates the session. • **ask login** terminates the session and requests that the user log back in (users will see a popup message with this information).

Configure Session Idle Times and Maximum System-Wide Sessions

By default, the Prime Network gateway will not disconnect GUI client sessions regardless of how long the session has been inactive. You change this behavior and set a client inactivity timer if needed.

In addition, you can control the maximum number of clients, system-wide, that can connect to a gateway at one time. Once this number is exceeded, the gateway will refuse client connections. By default this is set to 150 connections. (User accounts also have a setting for limiting connections per user.)

The registry entry and default value are provided in Table 3-8.

Note Do not exceed the value of 150 maximum open sessions. Doing so can negatively impact system performance.

Table 3-8 Registry Setting for Gateway Open Sessions

Registry Entry	Description	Default Value
sessionIdleTime	Client inactivity timer; when exceeded, the gateway should close the connection with a client (in milliseconds)	0
maxOpenSessions	Maximum number (system-wide) of sessions that may be open with the gateway (includes both GUI client and BQL sessions)	150

This example changes the client session idle time to 30 minutes. When 30 minutes are exceeded, the gateway will automatically disconnect the idle clients.

Step 1 Log into the gateway as *pnuser* and change to the Main directory by entering the following command.

```
# cd $ANAHOME/Main
```

Step 2 To change the client inactivity timer, use this command. In this example the timer is changed to 30 minutes:

```
# ./runRegTool.sh -gs gateway-IP set 127.0.0.1
"avm11/services/sessionmanager/sessionIdleTime" 1800000
```

Update the Gateway IP Address in Prime Network

Note This feature is only supported on configurations that meet *both* of the following criteria:

- The gateway and unit are installed on the same server.
- The system is running Linux and has an embedded database.

It is not supported on configurations with units installed on separate servers.

If the IP address of the gateway server is changed, you must also change several items in the registry so that system components can continue to communicate properly. Prime Network provides a script called **change_gw_ip.pl** that updates the following registry files:

- avm66.xml—Changes the database path entry
- persistency.xml—Changes the entries for the main database and Event Archive database schemas.
- avm0.xml—Changes the uplink entry between the gateway and its units.

The script will also restart all units to update the units with the new gateway information. The script also makes the changes that are required when using Prime Network Change and Configuration Management.

Before You Begin

- Make sure you have the old and new IP addresses for the gateway server.
- Re-configure the devices to forward events to the new IP address of the gateway server if the Cisco Event Listener (AVM 100) is enabled and is running on the gateway server.

To update the registry with the new IP address of the gateway:

Step 1 Stop all applications that are running on the gateway server.

- For an embedded database, log in as the Oracle user and run the following commands:

```
# cd $ANAHOME/Main/scripts/embedded_db
#./emdbctl--stop
```

- For an external database:

```
# cd $ANAHOME/Main
# networkctl stop
```

Step 2 If you have an external database, stop the database process. (For embedded databases, this step is not required because the internal database is stopped by the command used in Step 1.)

Step 3 Confirm that the database is stopped. If it is not, login in as the database user and issue the following command:

ORACLE_HOME/**product/***product-version***/db_1/bin/dbshut**

Step 4 Start the **change_gw_ip.pl** script as follows:

```
# cd $ANAHOME/Main/scripts
# change_gw_ip.pl
```

In the following example, the old IP address is 10.56.57.50, the new IP address is 10.56.22.47, and 10.56.56.111 is the IP address of the unit that is connected to the gateway.

```
This action can only be performed after Oracle DB and OS were updated. Continue? (y/n): y
Please enter the old IP Address: 10.56.57.50
Please enter the new IP Address: 10.56.22.47
Updated: /export/home/pn310/Main/registry/persistency.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/0.0.0.0/persistency.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/127.0.0.1/persistency.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/avm66.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/avm0.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/10.56.56.111/persistency.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/10.56.56.111/avm0.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/10.56.56.111/avm99.xml
Updating units...
```

Step 5 If you want to undo the changes (by not restarting the gateway), cancel the procedure as follows:

```
ANA GW and units are about to be restarted. Continue? (y/n): n
Would you like to undo the changes? (y/n): y
Stopping Units...
Updated: /export/home/pn310/Main/registry/persistency.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/0.0.0.0/persistency.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/127.0.0.1/persistency.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/avm66.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/avm0.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/10.56.56.111/persistency.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/10.56.56.111/avm0.xml
Updated: /export/home/pn310/Main/registry/ConfigurationFiles/10.56.56.111/avm99.xml
Updating units...
Done.
```

Step 6 If you want to commit the changes and restart the units and gateway, proceed as follows:

```
ANA GW and units are about to be restarted. Continue? (y/n): y
Stopping Units...
executing: ssh 10.56.56.111 networkctl stop
Stopping AVMs...done.
Restarting GW...
Stopping AVMs...done.
Starting MVM.............................................Done.
Starting Gateway.................................................................Done.
```

Step 7 Verify that Prime Network is running properly:

```
# cd $ANAHOME/Main
# networkctl status
```

Step 8 Verify that the Oracle database is running properly using your preferred method.

Disable Prime Network Automatic Restarts

By default, the Prime Network will automatically start whenever the gateway server is rebooted. If you wish to disable this feature, run the following procedure from the gateway. The change will be populated to all units in the system.

Step 1 Log into the gateway as *pnuser* and change to the Main directory.

```
# cd $ANAHOME/Main
```

Step 2 Issue this command to disable Prime Network from starting when the server is rebooted:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/system/startup" false
```

(If you want to re-enable this feature, specify **true**.)

The change is automatically applied; you do not need to restart the gateway.

Manage Configurations with Firewalls (Device Proxy)

Prime Network can manage gateways, units, and devices that are behind firewalls, as long as the system is configured as described in this topic.

Servers and Units Behind Firewalls

If a gateway server is behind a firewall, you must open ports on the firewall. The gateway will to need publicly addressable IP address.

If any unit servers are located behind firewalls or NAT devices:

- The unit is displayed in Prime Network Administration GUI client with an IP address of **0.0.0.#**. This is an artificial IP address used by the gateway server.
- You do not have to open special ports for the units. The units will always initiate communications.

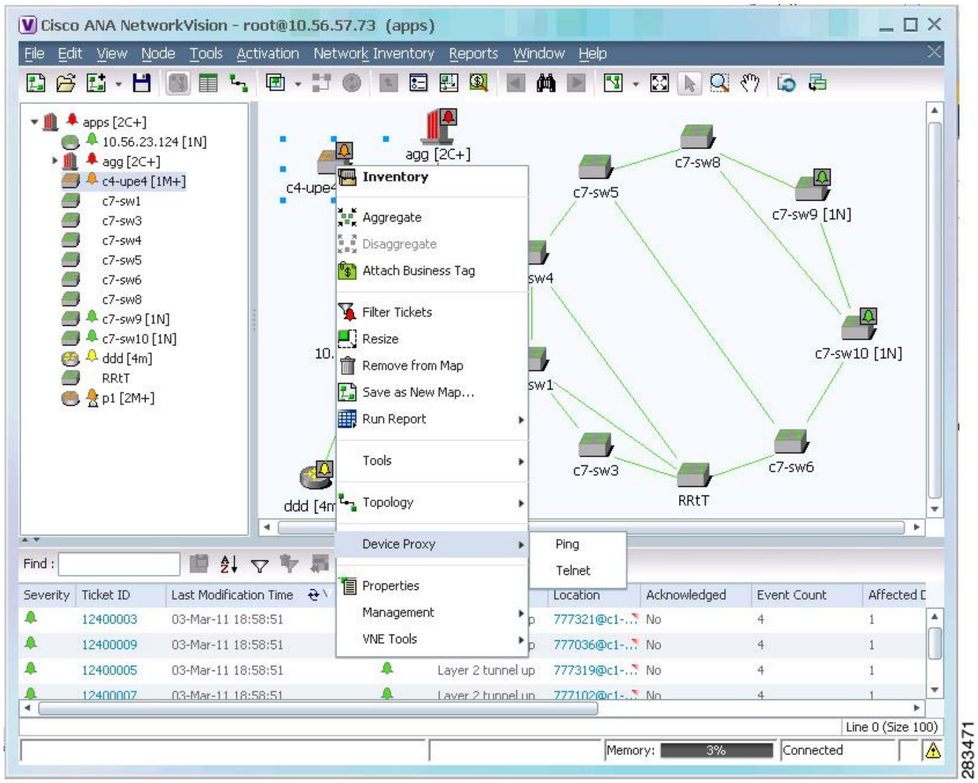
- An Event Collector (AVM 100) must be running on at least one of the units behind the firewall. If you have several NAT sites with similar configuration, an Event Collector must be running on at least one unit at each site.

Managed Devices Behind Firewalls

If there is a firewall between a GUI client and a managed device, all attempted Telnet connections to the device will fail. For these cases Prime Network provides a device proxy feature that, when enabled, routes connections from the client through the gateway server and the appropriate unit in order to reach the device. Supported connections are Telnet, Ping, and SSH.

Once this solution is configured, if a user right-clicks a device in a Prime Network Vision map, the user will see the menu items displayed in Figure 3-10.

Figure 3-10 Right-Click Menu When Device Proxy Feature is Enabled (Prime Network Vision)



Severity	Ticket ID	Last Modification Time			Location	Acknowledged	Event Count	Affected D
	12400003	03-Mar-11 18:58:51		p	777321@c1-...	No	4	1
	12400009	03-Mar-11 18:58:51		p	777036@c1-...	No	4	1
	12400005	03-Mar-11 18:58:51		Layer 2 tunnel up	777319@c1-...	No	4	1
	12400007	03-Mar-11 18:58:51		Layer 2 tunnel up	777102@c1-...	No	4	1

Choosing **Device Proxy > Ping** or **Device Proxy > Telnet** launches an SSH client that logs into the gateway server and passes the device and unit IP address to the gateway. The gateway then opens another SSH client to the unit, and the unit executes the protocol command on the selected device. The session then opens on the user's client, and the user has to enter the appropriate password (configured in the following procedure). You can optionally configure the feature so that the user does not have to enter a password; in that case only SSH keys are used for authentication. All ping sessions are closed after 120 seconds' expiration.

Configuring this solution consists of the following steps:

1. Creating the dedicated SSH user accounts on the gateway and all units using the **create_ssh_user.pl** script.
2. Configuring the SSH connections between the gateway and all units using the **create_ssh_tunnel.pl** script.
3. Enabling the feature from the Administration GUI client.

Once the feature is enabled, when a user logs into a Prime Network Network Vision client and connects to the gateway, the new choices will be available when the user right-clicks a device in a map.

Before You Begin

- This procedure does not apply to configurations where a unit is also behind a firewall or NAT.
- Port 22 must be open between the client and gateway for this solution to work.

To configure a device proxy:

Step 1 Log into the gateway server as root and change to the $ANAHOME/local/scripts/proxy directory.

```
# cd $ANAHOME/local/scripts/proxy
```

Step 2 Create the dedicated SSH user accounts on the gateway using the **create_ssh_user.pl** script. This creates the user (named **proxy**) and SSH keys. The command uses the following format:

create_ssh_user.pl -new_user_password *ssh_proxy_user_passwd* [**-home_dir** *dir*] **-ana_user** *ana_user*

The script uses the following arguments:

Field	Description
-ana_user *ana_user*	Name for *ana_user* (also called *pnuser* in our documentation). This is the operating system account for the Prime Network application, created when Prime Network is installed. A common example of *pnuser* is **pn310**.
-new_user_password *ssh_proxy_user_passwd*	SSH password for *proxy_user*. This is the password you must enter when you use the device proxy feature from Prime Network Vision map.
-home_dir *directory*	(**create_ssh_user.pl** only) Home directory that will be created for the proxy user. The default is /export/home/proxy.

For example (in this case Prime Network will use the default home directory):

```
# ./create_ssh_user.pl -new_user_password proxyadmin -ana_user pn310
```

Step 3 If your setup also has units, perform the following two steps.

a. From each unit, run the **create_ssh_user.pl** command (as shown in Step 2).

b. From the gateway (only), configure the SSH connections between the gateway and all units using the **create_ssh_tunnel.pl** script. The gateway will connect to all of the units and update the keys. The command uses the following format:

```
create_ssh_tunnel.pl -ana_user ana_user -new_user_password ssh_proxy_user_passwd
```

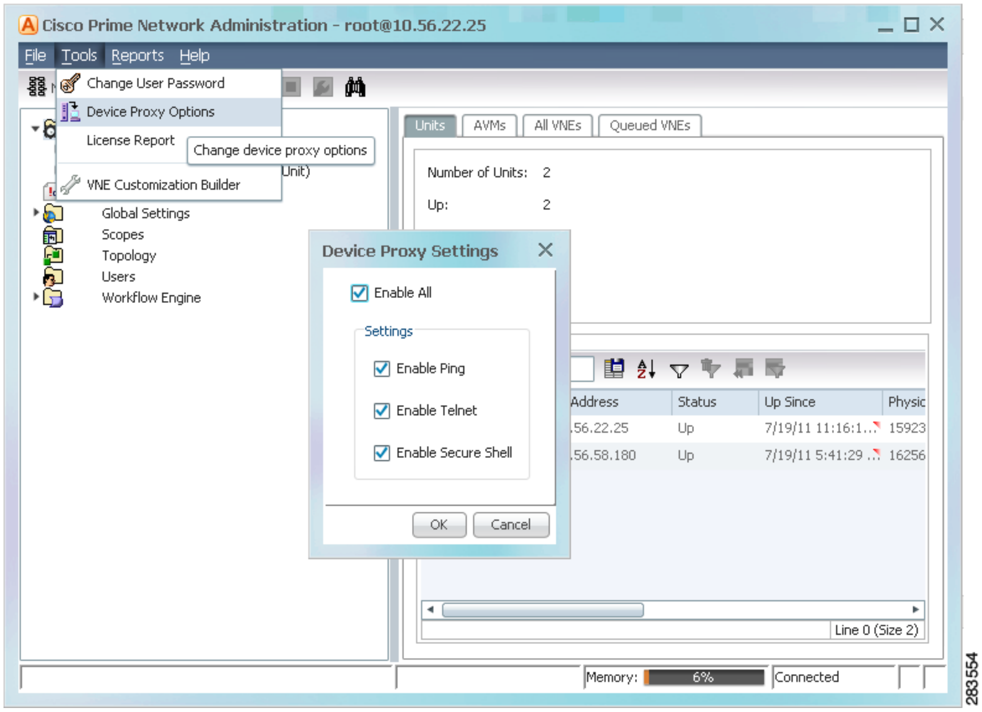
For example, to create a dedicated SSH tunnel for the user created in Step 2:

```
# ./create_ssh_tunnel.pl -ana_user pn310 -new_user_password proxyadmin
```

The script will display a status message confirming that the authorized_keys file was created on all of the units.

Step 4 Enable the device proxy feature in the Prime Network Administration client.To use this feature, choose **Tools > Device Proxy Options** as shown in Figure 3-11.

Figure 3-11 Enabling the Device Proxy Feature



Number of Units: 2

Up: 2

Device Proxy Settings

☑ Enable All

Settings

☑ Enable Ping

☑ Enable Telnet

☑ Enable Secure Shell

Address	Status	Up Since	Physic
.56.22.25	Up	7/19/11 11:16:1...	15923
.56.58.180	Up	7/19/11 5:41:29 ...	16256

Line 0 (Size 2)

Memory: 6% Connected

Configure a Northbound Interface Layer

You can configure Prime Network to support (licensed separately) Multi-Technology Operations Systems Interface (MTOSI) and 3GPP northbound interfaces. To do this, you must install a standalone integration layer package.

The standalone integration layer server allows Prime Network to expose MTOSI and 3GPP APIs over Service Oriented Access Protocol (SOAP).

To set up a standalone integration layer, refer to the instructions in the *Cisco Prime Network 3.10 Installation Guide*. For information about the 3GPP and MTOSI OSS integration, see the *Cisco Prime OSS Integration Guide for MTOSI and 3GPP*.

Run a Command on All Units

The script **rall.csh** runs a given command on all units (not on the gateway), as follows:

```
# $ANAHOME/rall.csh script
```

where *script* is the script name.

The following script example restarts all units:

```
# $ANAHOME/rall.csh ./Main/networkctl restart
```

Delete a Prime Network Unit

Follow this procedure to delete a unit. You can delete units that have a status of Down, Unreachable, or Disconnected.

Before You Begin

Delete all the VNEs and unreserved AVMs before deleting a unit; see Move and Delete AVMs, page 3-33. The reserved AVMs cannot be deleted.

Use this procedure to remove a unit:

Step 1 In the Prime Network Administration window, select **All Servers**.

Step 2 Right-click the unit that you want to remove, then choose **Delete**. A warning message is displayed.

Step 3 Click **Yes** to proceed or **No** to cancel the operation. A confirmation message is displayed.

Step 4 Click **OK**. The unit is deleted and is no longer displayed in the navigation pane and content area.

Create and Configure AVMs and Load Balancing

These topics explain how to create, stop, start, and perform other management operations on AVMs. It also explains how the load balancing feature works, which signals you when an AVM is approaching its memory threshold.

- Add AVMs, page 3-28
- Manage AVM Memory and Thresholds (Load Balancing), page 3-31
- Change AVM Status (Start or Stop), page 3-33
- Move and Delete AVMs, page 3-33

For information on reserved (system) AVMs and how to get information on general AVM properties, see Get AVM Status and Property Information (Including Reserved AVMs), page 3-8.

Add AVMs

When an AVM is created, it is given number (*AVM ID*) that is unique to the unit and between 101-999. AVMs 0-100 are reserved by Prime Network (see Table 3-2 on page 3-9 for a list of reserved AVMs). Every AVM requires a dedicated TCP port, and the port is created using the following naming convention:

AVM-ID + 2000

For example, if you created AVM 711, it would use port 2711. The appropriate TCP port must be available or the AVM creation will fail, unless you stop the application that is using the port before you create the AVM. (A complete list of ports used by Prime Network is provided in the *Cisco Prime Network 3.10 Installation Guide*.)

Each AVM has its own log in *NETWORKHOME*/Main/logs.

If possible, always add AVMs using the auto-add feature. Prime Network will select a unit for the AVM based on memory usage in the system. When you add an AVM (either automatically or manually), the operating system adds an additional 35% to the AVM size. This additional memory is used by the operating system for backend tasks, leaving the desired amount of memory for use by VNEs. Table 3-9 shows how much default memory is assigned to AVMs when they are created.

Table 3-9 Memory Assigned to AVMs

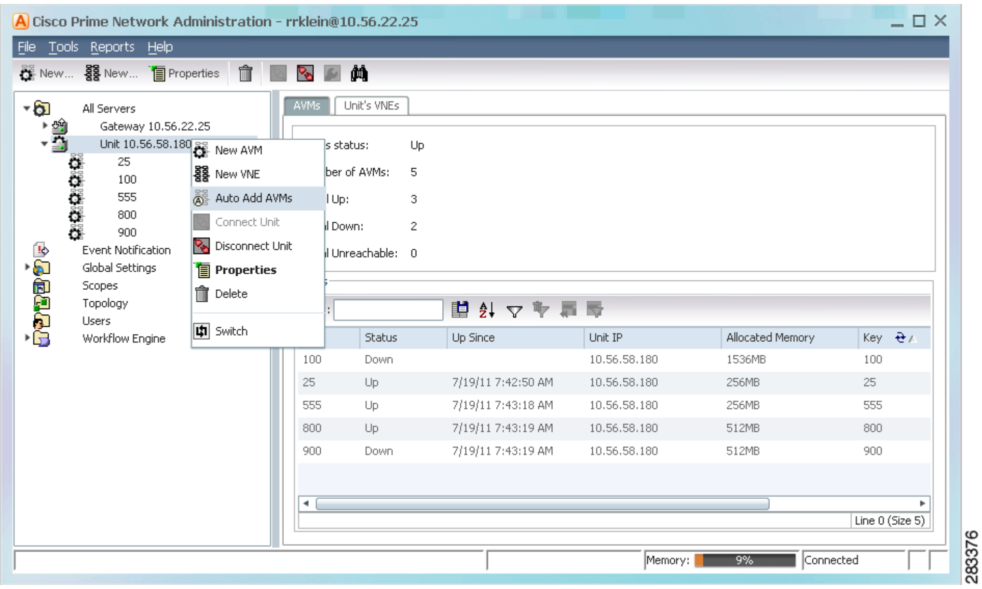
Method	Memory Assigned to AVM (Default)	Total Physical Memory Assigned to AVM
Auto-added AVMs	1500 MB	2025 MB
Manually added AVMs	256 M	345 MB

Auto-Add AVM (Recommended)

Prime Network automated AVM management simplifies the process of creating AVMs and assigning them to units, and monitoring AVM memory load so that it does not adversely impact the system.

When you use the *AVM auto-add* feature, Prime Network automatically creates new AVMs using the global properties (memory size and threshold) you specify in the Global Settings area of Prime Network Administration. Prime Network will choose the most appropriate unit for you (or you can specify the one you want to use). This is done through the GUI client Auto-Add AVMs option, as shown in Figure 3-12.

Figure 3-12 AVM Auto-Add



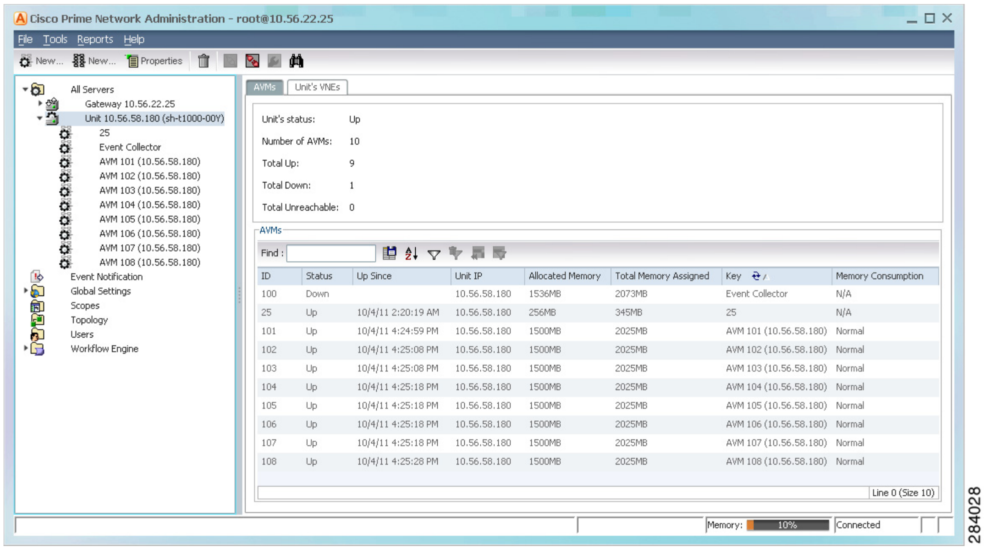
s status: Up
ber of AVMs: 5
l Up: 3
l Down: 2
l Unreachable: 0

	Status	Up Since	Unit IP	Allocated Memory	Key
100	Down		10.56.58.180	1536MB	100
25	Up	7/19/11 7:42:50 AM	10.56.58.180	256MB	25
555	Up	7/19/11 7:43:18 AM	10.56.58.180	256MB	555
800	Up	7/19/11 7:43:19 AM	10.56.58.180	512MB	800
900	Down	7/19/11 7:43:19 AM	10.56.58.180	512MB	900

Line 0 (Size 5)

To auto-add AVMS, right-click the desired unit and choose **Auto Add AVMs**. Prime Network will create eight AVMs to the unit and start the AVMs. Figure 3-13 shows an example of a unit with auto-added AVMs. Prime Network uses the first available 3-digit number (starting at 101) as the *AVM ID*, and the 3-digit number appended with the parent unit's IP address as the *AVM key*.

Figure 3-13 Unit Listing Auto-Added AVMs



Unit's status: Up
Number of AVMs: 10
Total Up: 9
Total Down: 1
Total Unreachable: 0

ID	Status	Up Since	Unit IP	Allocated Memory	Total Memory Assigned	Key	Memory Consumption
100	Down		10.56.58.180	1536MB	2073MB	Event Collector	N/A
25	Up	10/4/11 2:20:19 AM	10.56.58.180	256MB	345MB	25	N/A
101	Up	10/4/11 4:24:59 PM	10.56.58.180	1500MB	2025MB	AVM 101 (10.56.58.180)	Normal
102	Up	10/4/11 4:25:08 PM	10.56.58.180	1500MB	2025MB	AVM 102 (10.56.58.180)	Normal
103	Up	10/4/11 4:25:08 PM	10.56.58.180	1500MB	2025MB	AVM 103 (10.56.58.180)	Normal
104	Up	10/4/11 4:25:18 PM	10.56.58.180	1500MB	2025MB	AVM 104 (10.56.58.180)	Normal
105	Up	10/4/11 4:25:18 PM	10.56.58.180	1500MB	2025MB	AVM 105 (10.56.58.180)	Normal
106	Up	10/4/11 4:25:18 PM	10.56.58.180	1500MB	2025MB	AVM 106 (10.56.58.180)	Normal
107	Up	10/4/11 4:25:18 PM	10.56.58.180	1500MB	2025MB	AVM 107 (10.56.58.180)	Normal
108	Up	10/4/11 4:25:28 PM	10.56.58.180	1500MB	2025MB	AVM 108 (10.56.58.180)	Normal

Line 0 (Size 10)

You can edit AVM properties by right-clicking the AVM, choosing **Properties**, and making your changes. The changes will require an AVM restart to take effect.

Add AVMs Manually

To manually create an AVM:

Step 1 Expand the All Servers branch and select the unit or gateway that will host the AVM.

Step 2 Open the New AVM dialog box by right-clicking the required unit (or gateway), then choose **New AVM**. To view an existing AVM, right-click the AVM and select **Properties**.

Step 3 Enter the following information to create a new AVM. The unit does not have to be up to create the AVM.

Field	Description
ID	The name (a number) of the AVM as defined in Prime Network. It must be a unique number on the unit, between 101-999. AVMs 0-100 are reserved and cannot be used. The AVM will use the TCP port (*AVM_nnn* + 2000). For example, if you create AVM 711, port number 2711 will be dedicated to that AVM. The appropriate TCP port must be available or the AVM creation will fail, unless you stop the application that is using the port before you create the AVM. (A complete list of ports used by Prime Network is provided in the *Cisco Prime Network 3.10 Installation Guide*.)
Key	A string that uniquely identifies an AVM in the Prime Network system, across all units, thus enabling a transparent failover scenario in the system. The key is displayed as **AVM***ID_nnn,* where *nnn* is an designator assigned by Prime Network for tracking purposes.
Allocated Memory	The maximum memory that can be used by the AVM, in megabytes. If you need deployment information and recommendations, such as AVM memory requirements, contact your Cisco account representative. **Note** When you create an AVM manually rather than using auto-add, the default AVM size is *not* determined by the setting specified in **Global Settings > Automatic AVM Management**. That setting is only applied to auto-added AVMs.
Activate on Creation	Loads the AVM into the bootstrap of the unit. This changes the administrative status of the AVM to Up and ensures that the AVM is loaded on subsequent restarts of the unit. By default this option is *not* checked, and the newly created AVM has an administrative status of Down.
Enable AVM Protection	By default this check box is checked, enabling the watchdog protocol on the AVM. For more information, see Manage Redundancy for Units and Processes, page 5-1. **Note** Do not disable this option.

Step 4 Click **OK**. The new AVM is added to the selected unit, is displayed in the content area.

Manage AVM Memory and Thresholds (Load Balancing)

The *AVM load balancing* feature continuously monitors the memory used by AVMs that contain at least one VNE. Because VNE memory consumption can change with network configuration changes, it is critical to ensure that AVM memory overflows are quickly addressed. If an AVM is red or has a icon next to it, the AVM has exceeded its memory threshold. When you click the **Reduce Load** option from the GUI client, Prime Network automatically calculates which VNEs should be moved, and which AVM they should be moved to, in order to reduce the load. This is reported in a dialog box, and you can approve or reject the move.

The load balancing features rely on Prime Network to identify a *safe target AVM*. A safe target AVM has the following characteristics:

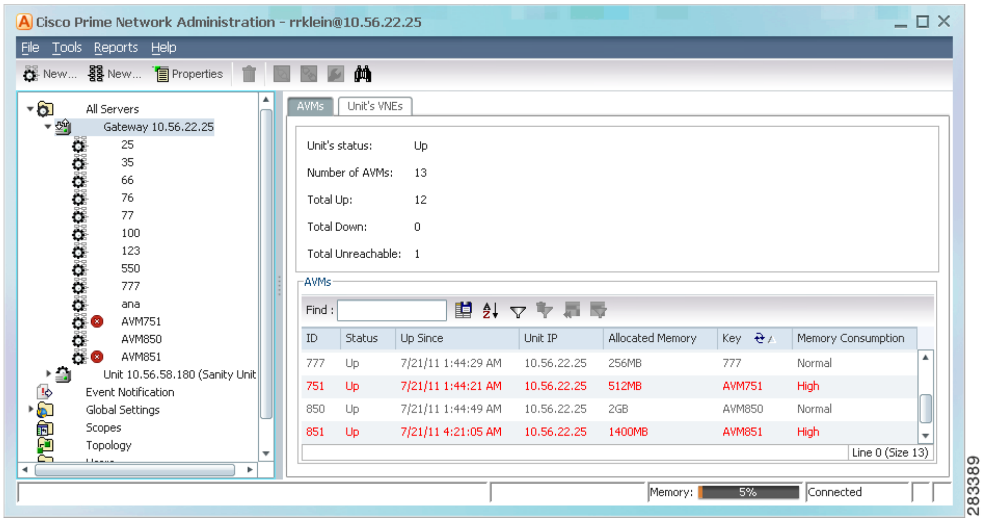
- All of its VNEs are modeled (the discovery process is not running).
- Its available memory is below the AVM Memory Warning Threshold (specified in **Global Settings > Automatic AVM Management**).
- It is not experiencing any memory consumption problems.

If a safe target AVM is not found, Prime Network waits 2 minutes and tries again.

Note You can also get AVM diagnostic information using the system health and diagnostics tool to check user-defined AVMs health, errors or exceptions, and GC prints. See Prevent System Overloads (Advanced Overload Prevention/Safe Mode), page 8-23.

Whenever a VNE is started, shut down, or removed, Prime Network checks AVM memory. If the total memory used reaches or exceeds the warning threshold, the Prime Network GUI signals the problem by coloring the AVM red, as shown in Figure 3-14.

Figure 3-14 AVM Memory Consumption Indicator in Units Windows



Unit's status: Up

Number of AVMs: 13

Total Up: 12

Total Down: 0

Total Unreachable: 1

AVMs

ID	Status	Up Since	Unit IP	Allocated Memory	Key	Memory Consumption
777	Up	7/21/11 1:44:29 AM	10.56.22.25	256MB	777	Normal
751	Up	7/21/11 1:44:21 AM	10.56.22.25	512MB	AVM751	High
850	Up	7/21/11 1:44:49 AM	10.56.22.25	2GB	AVM850	Normal
851	Up	7/21/11 4:21:05 AM	10.56.22.25	1400MB	AVM851	High

Line 0 (Size 13)

Balance the AVM Load

To balance an AVM load, right-click a user-created AVM and choose **Reduce Load**. Alternatively you can choose the AVM and then click the following toolbar icon, which is activated in when an AVM is selected.

Icon	Description
	Triggers the load balancing mechanism for the selected user-created AVM.

When you select **Reduce Load**, Prime Network identifies the VNE that is consuming most of the AVM memory. It identifies another AVM that is up and has sufficient free memory, and displays a dialog box confirming that it can move a VNE to that AVM. If no AVM is found, consider manually moving VNEs or adding new AVMs.

Change the AVM Load Balancing Threshold

To change the memory threshold for all user-created AVMs in the system (the point at which Prime Network flag a problem, as shown in Figure 3-14), use the following procedure.

Step 1 Select **Global Settings > Automatic AVM Management**.

Step 2 In the AVM Warning Threshold area, enter the threshold at which warnings should be displayed. For example, 90% means that when AVM memory consumption exceeds 90% of its total memory, the display will change as shown in Figure 3-14 on page 3-31.

Adjust the Memory Size for Auto-Added AVMs

This procedure changes the default values that are applied to AVMs when the AVMs are created using the AVM auto-add feature. The changes will be applied to all new auto-added AVMs.

Step 1 Select **Global Settings > Automatic AVM Management.**

Step 2 In the AVM Sizing field, configure the following.

Field	Description
Default AVM Size	The memory size to be used for auto-added AVMs. The default is 1500 MB.
Unit Reserved Memory	The percentage of memory that a unit should keep in reserve. If a unit exceeds its reserved memory, Prime Network will not add auto-added AVMs to the unit. The default unit reserved memory is 10%.

Step 3 Click **Apply**.

Change AVM Status (Start or Stop)

You can use the Prime Network Administration GUI to start or stop an AVM. When you stop an AVM, all the VNEs in the AVM are stopped. VNEs that were in maintenance mode will move to Down, and the Maintenance indicator in the AVMs window will display **false**.

If an AVM is red or has a 🟥 icon next to it, the AVM has exceeded its memory threshold. See Manage AVM Memory and Thresholds (Load Balancing), page 3-31.

Note Any change in status of the AVMs may take some time to be applied. For example, when running the **Stop** command, it may take several minutes before the status changes from Shutting Down to Down.

To start or stop an AVM:

Step 1 Expand the All Servers branch, then select the required AVM.

Step 2 Right-click the AVM, then choose **Actions > Start** or **Actions > Stop**.

The AVM is started or stopped, and the appropriate status is displayed in the content area.

Move and Delete AVMs

You can move user-created AVMs from one unit to another unit. AVMs 0-100 are reserved and cannot be moved.

Note If the unit hosting an AVM is down, disconnect the unit *before* moving the AVMs. See Stop Unit Communication with the Gateway (Disconnect), page 3-17.

After an AVM is moved, it is reloaded, maintaining the status it was in before the move. The only exception is if a VNE was in maintenance mode. After the move, these VNEs will be in the Down state and the Maintenance indicator (in the AVMs window) will change to **false**.

Alarm persistency information is saved when you move an AVM to another unit. For more information, see Change Settings That Control VNE Data Saved After Restarts, page 12-37.

When you delete a running AVM, the AVM is stopped and then removed. AVM registry information in the specified unit is deleted. Prime Network will not allow you to stop an AVM if any VNEs are running on the AVM. You cannot delete reserved AVMs (see Table 3-2 on page 3-9 for a list of reserved AVMs).

Move an AVM

To move an AVM:

Step 1 In Prime Network Administration, right-click the selected AVM, then choose **Move AVM**.

Step 2 Browse to and select the unit (branch) where you want to move the AVMs.

Step 3 Click **OK**. The AVM is moved and now appears beneath the selected unit.

Note Because the system is asynchronous, changes may not appear in the GUI immediately. It may be a few minutes until the GUI client receives a notification from the server and is updated.

For information about moving VNEs, see Move VNEs to Another AVM, page 4-37.

Delete an AVM

Before you delete and AVM, remove all VNEs from the AVM, or the operation will fail. See Delete VNEs, page 4-38.

To delete an AVM:

Step 1 Select the required AVM in the navigation tree. You may select multiple rows.

Step 2 Right-click to display the menu, then choose **Delete**. A warning message is displayed.

Step 3 Click **Yes**. A confirmation message is displayed.

Step 4 Click **OK**. The selected AVM is deleted from the selected unit.

Note Because the system is asynchronous, changes may not appear in the GUI immediately. It may be a few minutes until the GUI client receives a notification from the server and is updated.

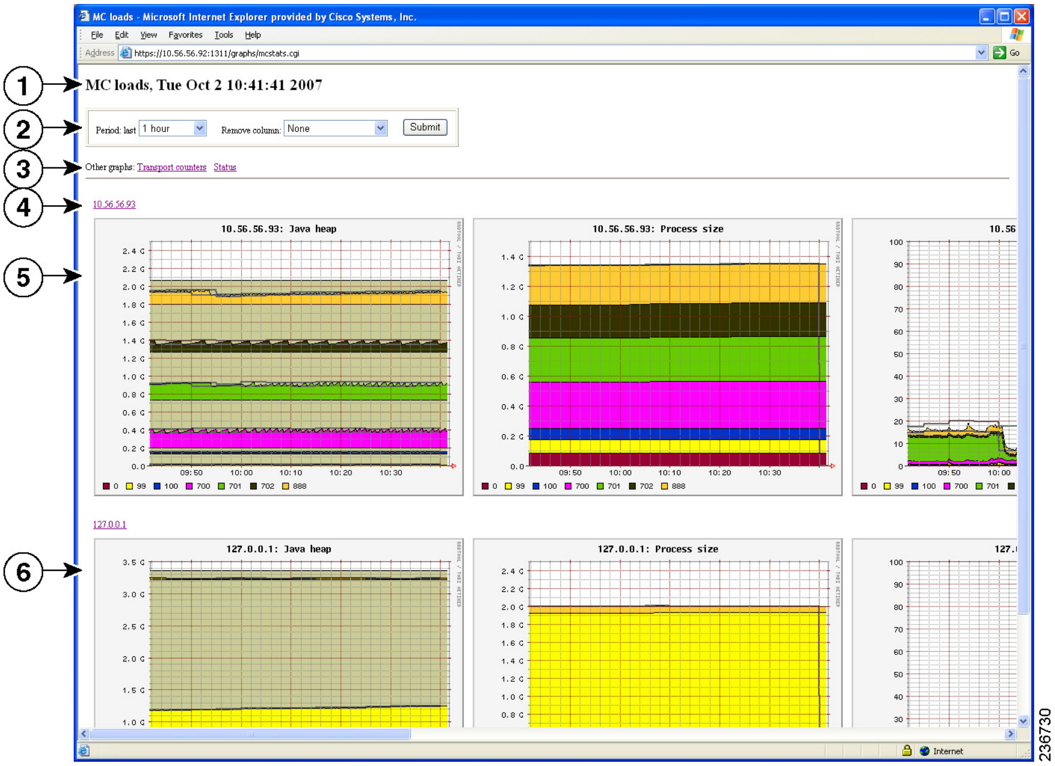
Check the Overall System and Use the Diagnostics (Graphs Tool)

Whenever a System event of note occurs, it is displayed in the Events GUI client. This includes a variety of events, such as an AVM not responding, events being dropped, a unit switching on due to a failover, and many others. You can also create regular reports that can generate system information you want. For more information, see the *Cisco Prime Network 3.10 User Guide*.

Prime Network also a web-based diagnostics tool that tracks how the gateway, units, and individual AVMs are operating—Java heap, dropped messages, CPU usage, and so forth. This data is provided in the form of graphs so you can quickly identify problems.

Figure 3-15 shows the default page that is displayed when you first log into the Prime Network Monitoring tool; it is called the MC Loads page.

Figure 3-15 MC Loads Page—All Servers (Default)



MC loads - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address https://10.56.56.92:1311/graphs/mcstats.cgi

MC loads, Tue Oct 2 10:41:41 2007

Period: last 1 hour Remove column: None Submit

Other graphs: Transport counters Status

10.56.56.93

127.0.0.1

1
2
3
4
5
6
File Edit View Favorites Tools Help
Go
10.56.56.93: Java heap
10.56.56.93: Process size
10.56
127.0.0.1: Java heap
127.0.0.1: Process size
127.
2.4 G 2.2 G 2.0 G 1.8 G 1.6 G 1.4 G 1.2 G 1.0 G 0.8 G 0.6 G 0.4 G 0.2 G 0.0
1.4 G 1.2 G 1.0 G 0.8 G 0.6 G 0.4 G 0.2 G 0.0
100 90 80 70 60 50 40 30 20 10 0
3.5 G 3.0 G 2.5 G 2.0 G 1.5 G 1.0 G
2.4 G 2.2 G 2.0 G 1.8 G 1.6 G 1.4 G 1.2 G 1.0 G 0.8 G
09:50 10:00 10:10 10:20 10:30
■ 0 ■ 99 ■ 100 ■ 700 ■ 701 ■ 702 ■ 888
Internet
236730

1	Current date and time on the selected server.
2	Toolbar that controls the sampling period represented in the graphs, and the graph types that are displayed.
3	Web page options: • MC Loads—Load statistics for the gateway and unit servers. Clicking on an IP address hyperlink launches a drill-down page showing all AVMs. • Transport—Transport switch counters page showing incoming and outgoing traffic rates, dropped messages, and flood counts. • Status—Status information about the graphs service—whether the service is up for all units, and when the data was last polled.
4	Hyperlinks for the gateway and units. The gateway is always 127.0.0.1; units are represented by their IP address. Drill down to a gateway or unit by clicking its hyperlink. This launches a display of information for each AVM on the gateway or unit.
5	Unit and gateway servers rows. Each row represents one unit server. Each color represents an AVM on the unit. The graphs that are organized by column, and the display is controlled by the Remove column drop-down list in the toolbar. (Servers and units run their own graphs processes; units copy the collection results to the gateway server.)
6	Gateway row. Each row represents one gateway server. Each color represents an AVM on the gateway. The graphs are organized by column, and the display is controlled by the Remove column drop-down list in the toolbar.

Types of Information You Can Get

The MC Loads page is generally the most useful source of information because it provides a wide variety of diagnostic information:

Type of Data	Description
Java Heap	The sizes of the Java heaps in the AVM processes.
Process Size	AVM memory process sizes.
CPU %	AVM CPU usage.
GC Time	AVM Java Garbage Collector (GC) activity.
Dropped Messages	The number of messages dropped in the Prime Network transport messaging mechanism. This can happen when the system is under a heavy load.
Logged Lines	The number of lines written to AVM logs.
CPU Total	The system CPU metrics for Prime Network unit operation.

Transport Counters Page

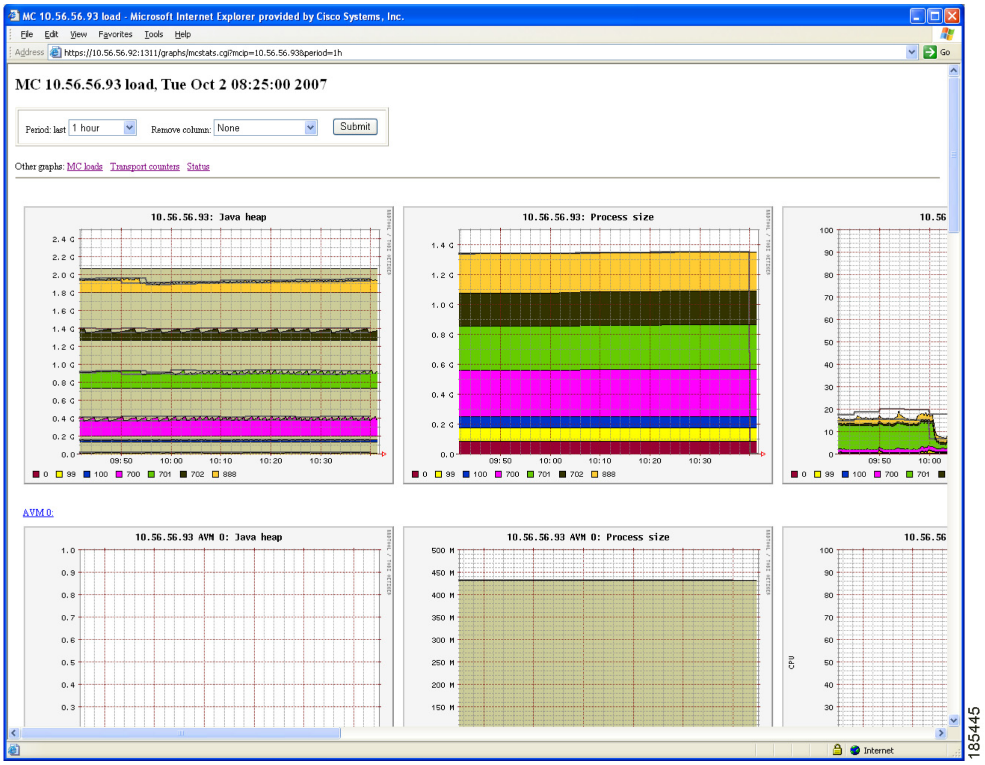
The Transport Counters page shows the following information

Type of Data	Description
Traffic	The number of traffic frames and traffic bytes sent and received.
Drops	The number of dropped frames and dropped bytes, both outgoing and incoming.
Floods	The number of flood frames and flood bytes generated and received.

What Do the Colors and Indicators Mean?

When you click an IP address from the main MC Loads page (illustrated in Figure 3-15 on page 3-35), Prime Network Monitoring displays a drill-down page for the specific server. Figure 3-16 illustrates a drill-down page for the unit server with the IP address 10.56.56.93. The first row displays a combined AVM graph, and the following rows display individual AVM information.

Figure 3-16 MC Loads Page—Drill-down to Specific Server



MC 10.56.56.93 load - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address https://10.56.56.92:1311/graphs/mcstats.cgi?mcip=10.56.56.93&period=1h

MC 10.56.56.93 load, Tue Oct 2 08:25:00 2007

Period: last 1 hour Remove column: None Submit

Other graphs: MC loads Transport counters Status

AVM 0:

All graphs have two horizontal grey lines that mark the highest and lowest values that were collected during the sampling period. The graph itself represents the average of those values.

Figure 3-17 Grey Line Indicators in the MC Loads Graphs

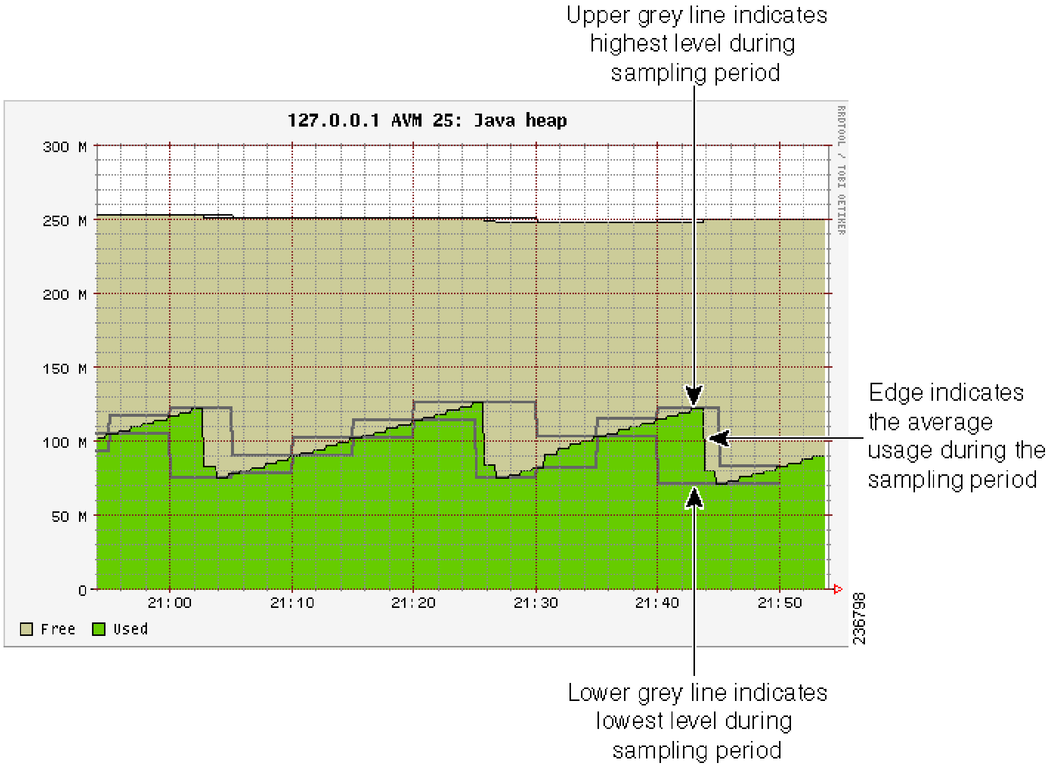
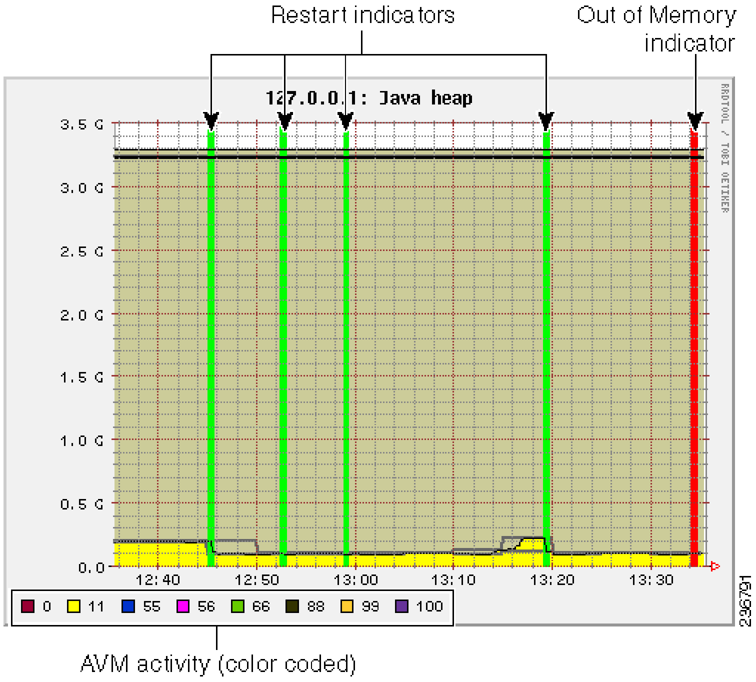


Figure 3-18 illustrates some other indicators you may see on MC Loads graphs:

- A color-coded list of AVMs on the server (gateway or unit). These appear in composite graphs, which represent behavior for AVMs on a server. The list is provided below the graph.
- On the Java heap graph, an out-of-memory indicator (a red vertical line) is displayed when an AVM runs out of memory. This is displayed in any graphs that provide Java heap information.
- On all graphs, a restart indicator (a green vertical line) shows when a specific AVM, or the entire server, was restarted.

Figure 3-18 Color Indicators in the MC Loads Graphs



Finally, any breaks in the data (blank vertical areas in the graph) mean that data could not be collected for that period.

Use the Tool (Examples)

The web-based tool uses the username admin; the password is configured by the network-conf script during installation. You can change the username and password as described in Change Password for Diagnostics (Graphs) Tool, page 11-12). When you log in for the first time, download and install the security certificate. The tool uses the HTTPS protocol and authentication method.

To access the Prime Network Monitoring tool:

Step 1 Enter **`https://`*`gateway_ip`*`:1311/graphs`** in your browser where *`gateway_ip`* is the gateway IP address.

A security alert is displayed regarding the site certificate.

Step 2 Click **Yes**, and enter the username and password.

By default, the tool displays load statistics collected during the past hour for the gateway and unit servers (the MC Loads graphs; see Figure 3-15 on page 3-35). You can select a sampling period by choosing from the Period drop-down list and clicking **Submit**.

The following are some examples of how you can use the MC Loads page:

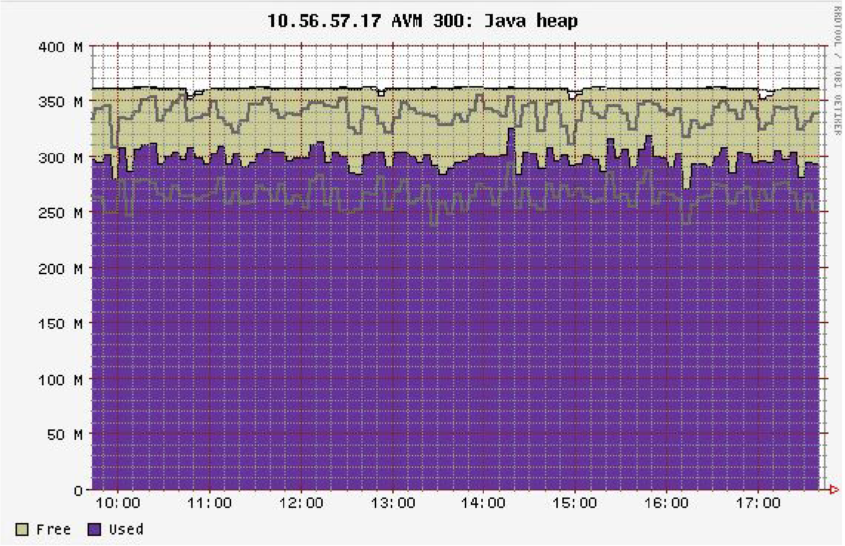
- Check the Java heap on AVM 11 on the gateway server as in indicator of gateway memory usage.
- Drill down to specific user-defined AVMs (that are hosting VNEs) to examine their health, look for errors or exceptions, and watch GC prints.

- Check the Dropped Messages graph of each unit and gateway, paying special attention to AVM 25 (the Event Persistence AVM, which would indicate drops related to event handling).
- Ensure that the GC is not taking more than 20-30 seconds (except at system startup).

The following topics provide examples of some of these uses and how to interpret the graphs on the MC Loads page.

AVM Memory Consumption

For memory consumption, we recommend that 30% of the AVM memory remain free (in a steady state). The Java heap graph provides a visual way to check this rate. The following example shows that approximately 15% of the memory is available.

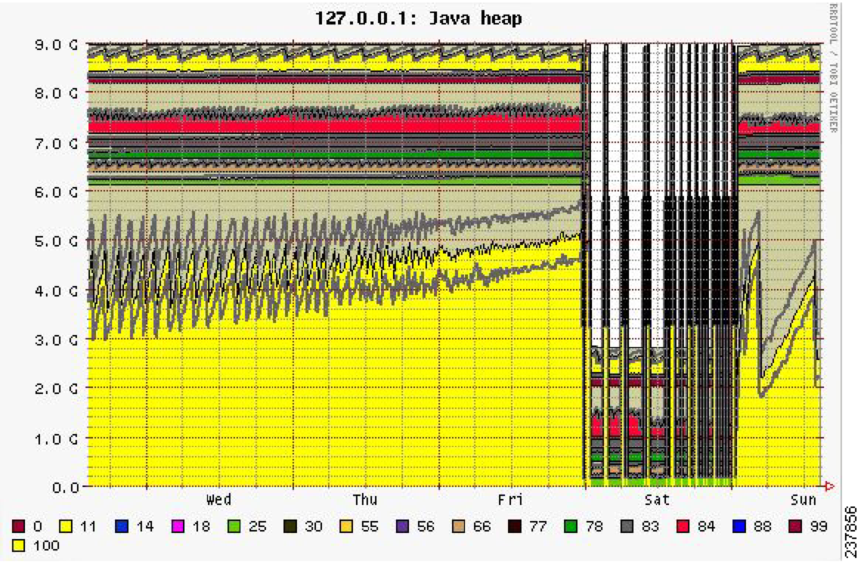


Stable memory consumption, or a constant sawteeth-shaped graph, reflects a healthy AVM. The sawtooth graph indicates the normal behavior of the Java GC, which releases unused objects on a regular basis. This behavior is expected but should not be followed by an overall growth in the memory consumption.

Few unique cases to consider when looking at Prime Network heap graphs:

- Very high and wide sawtooth—The AVM has extra memory available for allocation; GC runs in a low priority thread and is triggered as less memory is available. A suggested response is to add more VNEs to the AVM in a gradual manner, monitoring the AVM memory usage during the process.
- Very sharp sawtooth over a short period of time—The system is attempting to deallocate memory and is triggering GC very frequently. This may result from an AVM being too overloaded with VNEs, or specific VNEs being very large and busy. Depending on your use case, suggested responses are to allocate more memory to the AVM, reduce the number of VNEs in the AVM, or reduce the VNE polling cycles.

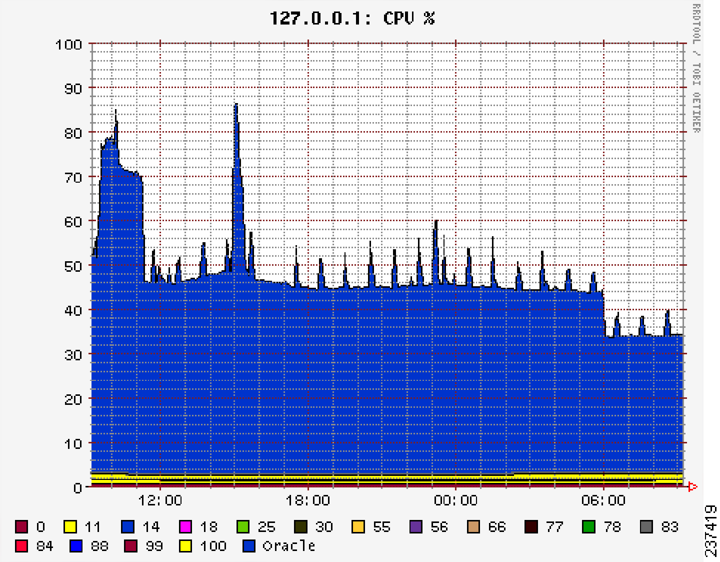
A gradual increase in the graph indicates that the AVM is using increasingly more memory. If there was no change to the AVM content, or to the network managed by the VNEs in the AVM, this may indicate a memory leak. In the following example, there is a memory leak in AVM 11.



High CPU Example

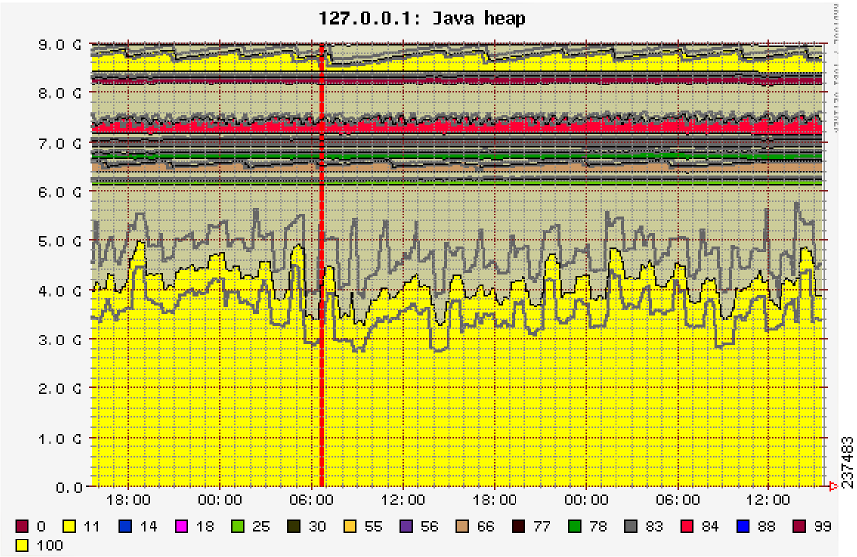
In this example, the system is configured with an embedded database and the Oracle process is causing high CPU usage.

Note In this example the Oracle process is experiencing a high CPU event. However, at system startup, it is also normal for AVMs to consume 100% of the CPU for a short period of time.



Fatal AVM Error (AVM Restart) Example

This example shows a fatal AVM error that caused an AVM restart. Common causes of this problem are out-of-memory errors and core dumps.



Change Sampling Periods and Refresh Settings

The following table shows the different sampling rates for the data that is collected, based on their age. Data is discarded after 28 days.

Age of Data	How Data is Saved
Up to 3 hours old	Data is saved every 15 seconds.
3-24 hours old	Data is diluted to a sampling rate of 300 seconds.
24 hours to 7 days old	Data is diluted to a sampling rate of 15 minutes.
7-28 days old	Data is diluted to a sampling rate of 2 hours.
More than 28 days old	Data is discarded.

You can change the graph display by entering additional parameters in the browser URL field, in an HTTP GET format. Table 3-10 describes the parameters you can use, along with examples.

Table 3-10 Available Graph Parameters

Parameter	Description
period	The sampling period in the following format: **&period=***xn* where *x* is a number, and *n* is the unit of time measurement: **h** (hours), **m** (months), **d** (days), or **w** (weeks). The following entry creates a sample period of 18 hours: **&period=18h**
end	The ending time for the sampling period (in relation to the **period** time) in the following format: **&end=-***xn* The time format is the same as for **period**. The following entry creates a sample period from that four hours long, and ends 2 days before the current time: **&period=4h&end=-2d**
refresh	Refreshes the graph page ever x seconds, in the following format: **&refresh=***x* Because Prime Network graph data is collected every 20 seconds, *x* should be larger than 20. The following entry sets the page refresh to every 30 seconds. **&refresh=30**
width, height	The width and height of the graph in pixels, in the following format: **&width=***x***&height=***x* The following entry draws the graph as 800x600 pixels: **&width=800&height=600**

Track System-Related Events

The following table shows from where you can get historical information on events that occurred on the gateway, units, AVMs, and VNEs. For these methods you can tailor your search or reports by specifying keywords (such as *gateway* or *unit*) or event types.

Information Type	Refer to:
Recent System and Security events	System and Security tabs in Event GUI client
Historical data on System and Security events for a specific time period and/or specific events	From the main menu, choose **Reports > Run Report > Events Reports > Detailed Non-Network Events**