Cisco Prime Network 3.9
Administrator Guide

Revised: March 8, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-26487-01
CONTENTS

Preface iii

New and Changed Information xiv

Organization of This Guide xiv

Conventions xvii

Related Documentation xvii

Obtaining Documentation and Submitting a Service Request xviii

PART 1

Introduction

CHAPTER 1

Getting Started with Prime Network 1-1

Basic Steps for Deploying Prime Network 1-1

Launching the Prime Network Administration GUI Client 1-4

Using Prime Network with Cisco Prime Central 1-4

Parts of the Prime Network Administration Window 1-6

All Servers Windows 1-9

Gateway and Units Windows 1-11

AVMs Windows 1-14

Event Notification Window 1-16

Global Settings Windows 1-17

Automatic AVM Management Window 1-18

Event Management Settings Window 1-19

Job Manager Settings Window 1-20

License Report Window 1-21

Message of the Day Window 1-22

Polling Groups Window 1-23

Protection Groups Window 1-24

Report Settings Window 1-25

Security Settings Window 1-26

Scopes Window 1-29

Topology Window 1-31

Users Window 1-32

Workflow Engine Windows 1-33
Working with Prime Network Tables
  - Table Toolbar Options
  - Using Keyboard Shortcuts in Tables
  - Finding Text in a Table
  - Sorting a Table
  - Filtering Table Contents
  - Viewing Selected Rows
  - Exporting Tables to a File

PART 2
Basic Gateway and Unit Administration

CHAPTER 2
Basic Gateway Server Administration Tasks
  - Overview of the Prime Network Gateway
  - Viewing Gateway Properties in Prime Network Administration
  - Starting and Stopping the Gateway and Checking AVM Status
  - Creating a GUI Client Banner Message

CHAPTER 3
Basic Unit Server Administration Tasks
  - Overview of Prime Network Units
  - Viewing Unit Properties
  - Starting or Restarting a Unit and Checking AVM Status (networkctl)
  - Connecting and Disconnecting a Prime Network Unit
  - Deleting a Prime Network Unit

CHAPTER 4
Basic AVM and VNE Administration Tasks
  - Overview of AVMs
  - Understanding AVM Status
  - Viewing AVM Properties
  - Adding AVMs
  - Reducing AVM Loads and Checking AVM Status
  - Changing AVM Status (Start or Stop)
  - Moving and Deleting AVMs
  - Viewing VNE Status
  - Moving VNEs to a Different AVM
  - Deleting a VNE
CHAPTER 5  Licensing  5-1
  Licensing Overview  5-1
  Licensing for Upgrades from Cisco ANA 3.6.x and 3.7.x  5-2
  Licensing and Gateway Server High Availability  5-2
  Obtaining a License File  5-3
  Installing and Updating a License File  5-4
  Viewing the License Report  5-5
  Troubleshooting Licensing Issues  5-5
    License Violation Messages  5-6
    Stopping and Starting the License Server  5-6

CHAPTER 6  Configuring Event Notifications  6-1
  What Is the Event Notification Service?  6-1
  Viewing and Managing Existing Notification Services  6-2
  Configuring an Event Notification Service  6-3

CHAPTER 7  Managing User Security: Roles and Scopes  7-1
  Overview of User Authentication and Authorization  7-1
    External Authentication  7-2
    Prime Network User Roles  7-2
    Device Scopes  7-3
    Steps for Setting Up Users and Scopes  7-6
  Managing Global Security Settings  7-7
    Using an External LDAP Server for Password Authentication  7-7
      Prerequisites for Using LDAP  7-9
      Configuring Prime Network to Communicate with the External LDAP Server  7-10
      Importing Users from the LDAP Server to Prime Network  7-13
      Changing from External to Local Authentication  7-14
    Setting Global Password Rules  7-14
    Automatically Disabling Accounts for Inactive Users  7-15
  Creating and Managing Scopes  7-16
    Creating Device Scopes in Prime Network  7-16
    Viewing and Editing Existing Device Scopes  7-18
    Deleting a Device Scope from Prime Network  7-18
  Managing User Accounts and Controlling User Access  7-19
    Creating a New User Account and Viewing User Properties  7-19
    Viewing, Changing, and Disabling User Accounts and Device Scope Access  7-22
    Controlling User Access to Maps (Maps Tab)  7-23
Deleting a Prime Network User Account 7-24
Changing a User’s Prime Network Password 7-24

CHAPTER 8
Backup and Restore 8-1
Back up Your Data 8-1
Overview of the Backup Procedure 8-1
Changing the Periodic Backup Time 8-3
Performing a Manual Backup 8-4
Restoring Prime Network Data 8-4

PART 3
Advanced Gateway and Unit Administration

CHAPTER 9
Advanced Administration for the Prime Network Gateway and Units 9-1
Managing Configurations with Firewalls (Device Proxy) 9-2
Restarting Prime Network In a Gradual Manner 9-5
Obtaining Diagnostic Information Using Graphs 9-6
Logging Into the Prime Network Monitoring Tool 9-7
Overview of the Prime Network Monitoring Window 9-7
Using the MC Loads Graphs 9-11
Understanding the Colors and Indicators 9-11
Common Uses for the MC Loads Page 9-13
Customizing Graphs with Address Bar Parameters 9-16
When Prime Network Monitoring Data is Purged 9-17
Automatic Overload Prevention (AOP/Safe Mode) 9-17
Changing the IP Address of the Gateway Server 9-21
Gateway Open Sessions Registry Settings 9-23

CHAPTER 10
Archiving and Purging Data 10-1
Prime Network Database Schemas 10-1
Archiving and Purging Data 10-4
How Data Purging Works 10-5
Customizing Archive and Purge Settings for the Fault Database and Event Archive 10-6
Customizing Purge Settings for Reports 10-8
Automatic Purging of Old Jobs 10-9
How Fault Data is Auto-Archived in the Database 10-9
CHAPTER 11

Working With an Embedded Database 11-1

Managing an Embedded Database 11-1

- Monitoring an Embedded Database and Understanding Error Messages 11-2
- Using the emdbctl Utility to Manage the Embedded Database 11-3
- Adding Additional Storage to an Embedded Database 11-5
- Purging Data and Checking Space on an Embedded Database 11-7

Backing Up an Embedded Database and Prime Network 11-10

- Overview of the Backup Procedure (With Embedded Database) 11-10
- Enabling Backups (Embedded Database) 11-11
- Performing a Manual Backup of an Embedded Database and Prime Network 11-12
- Changing the Database Backup Time 11-12
- Installing the Security Patches 11-13

Restoring an Embedded Database and Prime Network 11-13

CHAPTER 12

Workflow Administration Tasks 12-1

Workflows and the Workflow Engine Windows 12-1

- Viewing and Deleting Templates 12-3
- Viewing and Administering Workflows 12-4

CHAPTER 13

System Security 13-1

Communication Security 13-1

Device Communication Security: SSH and SNMPv3 13-4

Registry Security 13-6

User Authentication and Authorization 13-6

CHAPTER 14

Managing the Event Collector (AVM 100) 14-1

Overview of the Event Collector and Event Processing 14-1

- Configuring the Event Collector: Examples 14-6
- Enabling a Single Event Collector on a Gateway or a Unit 14-11
- Configuring and Enabling Multiple Event Collectors 14-12
- Registering VNEs with a Non-Default Event Collector 14-15
- Configuring Proxy AVM 25 for Units Not Connected to Database 14-15
- Disabling and Re-Enabling Event Archiving 14-16

CHAPTER 15

Utility Scripts 15-1

Changing Passwords: Prime Network Database Schemas 15-1

Changing Passwords: bosenable, bosconfig, and bosusermanager, and root 15-4
Changing Passwords: Diagnostics Tool 15-5
Running a Command on All Prime Network Units 15-5
Using the vne_creation_script to Add VNEs 15-5

CHAPTER 16
Unit Server High Availability and AVM Protection 16-1
Overview of Unit Server High Availability 16-1
Watchdog Protocol for AVM Protection 16-1
Unit N+m High Availability 16-2
Estimating the Impact of Unit or AVM Failures 16-4
Impact of Catastrophic AVM Process Failure 16-4
Impact of AVM Timeouts and Restarts 16-6
Impact of Unit Timeouts and Switchovers 16-8
Creating Unit Protection Groups and Designating Standby Units 16-8
Managing the Watchdog Protocol (AVM Protection) 16-10
High Availability Registry Settings 16-11

CHAPTER 17
Using Veritas Gateway Server High Availability 17-1
Veritas Gateway Server High Availability Architecture 17-1
Veritas Local Redundancy 17-6
Configuration Details for Veritas Local Redundancy (Dual-Node Cluster) 17-6
How Automatic Failover is Triggered (Veritas Local Redundancy) 17-11
Veritas Geographical Redundancy 17-13
Configuration Details for Veritas Geographical Redundancy (Global Cluster) 17-13
Understanding Manual Failover (Veritas Geographical Redundancy) 17-17
Veritas Geographical Redundancy Failure and Failback Scenarios 17-19
Mean Time to Repair Veritas Gateway Server High Availability Failures 17-22

CHAPTER 18
Using RHCS/ADG Gateway Server High Availability 18-1
Red Hat Cluster Suite (RHCS) Local Redundancy 18-1
Configuration Details for RHCS Local Redundancy 18-2
Failover and Switchover (RHCS Local Redundancy) 18-4
Managing RHCS Local Redundancy 18-5
Oracle Active Data Guard (ADG) Geographical Redundancy 18-8
Configuration Details for ADG Geographical Redundancy 18-8
Switchover/Failover Scenarios (ADG Geographical Redundancy) 18-12
Managing ADG Geographical Redundancy 18-14
Changing IP Addresses (ADG Geographical Redundancy) 18-22
PART 4

CHAPTER 19

Basic VNE Administration

VNE Administration: VNE Lifecycle and Creating VNEs

What Are VNE Communication and Investigation States? 19-1
  VNE Communication States 19-3
  VNE Investigation States 19-4
Choosing a VNE Scheme 19-5

Adding VNEs 19-11
  Cloning VNEs 19-14
  Creating VNEs Using a CSV File 19-17
  Creating VNEs for New Device Types 19-21
  Creating VNEs Using the Network Discovery Feature 19-23
    Discovery Profiles 19-24
    Network Discovery Results 19-26

Viewing and Editing VNE Properties 19-28
  VNE General Settings 19-29
  VNE SNMP Settings 19-31
  VNE Telnet/SSH Settings 19-32
  VNE XML Settings 19-38
  VNE HTTP Settings 19-39
  VNE ICMP Settings 19-39
  VNE Polling Settings 19-40
  VNE Events Settings 19-42
  Editing VNE Properties 19-43

Changing VNE Status and Lifecycle (Start, Stop, Maintenance) 19-44

Controlling Concurrent VNE Telnet Logins (Staggering VNEs) 19-45

CHAPTER 20

Troubleshooting VNE Modeling 20-1

Troubleshooting VNE Communication State Issues 20-1
  What Determines the VNE Communication State (Device Reachability)? 20-1
  Steps to Troubleshoot VNE Communication State Issues 20-3
Troubleshooting VNE Investigation State (Discovery) Issues 20-14
  Registry Settings for VNE Discovery Timeout and Investigation State Reporting 20-23

Opening a Bug Report 20-24

CHAPTER 21

VNE Updates 21-1

What Are Independent VNE Drivers and Device Packages? 21-1
How to Find Out if New Support is Available 21-2
Identifying VNE Driver Packages That Are Installed on the Gateway 21-3
Identifying Which Driver a VNE Is Using 21-4
Changing the Device Package a VNE Is Using 21-4
Downloading and Installing New Driver Files 21-5
Uninstalling a Device Package 21-7
Troubleshooting Driver Installations 21-8

PART 5
Advanced VNE Administration

CHAPTER 22
Customizing VNE Polling 22-1
CPU Utilization Problems: Where to Begin 22-2
Reduced Polling 22-2
  Basic Procedures and Customizations: Reduced Polling 22-4
  Advanced Customizations: Reduced Polling 22-8
Adaptive Polling 22-15
  Basic Customizations: Adaptive Polling 22-17
  Advanced Customizations: Adaptive Polling 22-18
VNE Polling Groups and Slow Polling 22-23
Smooth Polling 22-26
Smart Polling (On-Demand Polling) 22-27

CHAPTER 23
Unmanaged Network Segments (Cloud VNEs) and Dynamic/Static Links 23-1
Unmanaged Segments and Cloud VNEs 23-1
  Ethernet on Cloud VNEs 23-2
  Connecting the Cloud VNE to a Device 23-3
Creating and Deleting Static Links 23-8

CHAPTER 24
Device Reachability 24-1
  VNE Management Communication Policies and How To Change Them 24-1
  How Prime Network Determines Protocol Reachability 24-3
Customizing Protocol Reachability Testing 24-7

CHAPTER 25
VNE Collectors and Command Priorities 25-1
  What Are Collectors and Command Priorities? 25-1
  Considerations for Using Fast Commands and Fast Collectors 25-2
  Expedited Commands and Activation Scripts and Fast Collectors 25-3
Configuring a Command With the “Fast” Command Priority 25-4
Creating a Fast Collector for a VNE 25-5

CHAPTER 26
VNE Persistency Mechanism 26-1
Persistency Overview 26-1
Alarm Persistency 26-2
Instrumentation Persistency 26-6
Topology Persistency 26-7

PART 6
Appendixes

APPENDIX A
Device Configuration Tasks for VNE Creation A-1
Why Device Configuration Tasks Are Important A-1
Validating Devices Before Adding VNEs (Cisco IOS XR) A-2
Cisco IOS, Cisco IOS XE, and CatOS Devices—Required Settings A-2
Cisco IOS XR Devices—Required and Recommended Settings A-3
Cisco StarOS Devices—Required Settings A-5
  SNMP Community A-5
  SNMP Trap A-5
  Reduced Polling A-6
Cisco Nexus OS—Required Settings A-7
All Cisco Devices Added Using SSH—Required, Recommended, and Rollback Device Settings A-8
SNMP Traps and Informs—Required Device Settings A-8
Syslogs—Required Device Settings A-13
IP Address Configuration for Traps, Syslogs, and VNEs A-14
Cisco Carrier Packet Transport Devices A-15

APPENDIX B
Prime Network Log Files B-1
  How Prime Network Saves Log Files B-1
  Changing Log File Behavior B-2
  Log Files B-2

APPENDIX C
Working with the Registry C-1

INDEX
Preface

This guide describes how to administer Cisco Prime Network (Prime Network) using the Prime Network Administration GUI client, utility scripts, and registry modifications.

Prime Network Administration is the GUI application designed to simplify and facilitate administration. It interacts with the Prime Network registry to query and modify configuration information. You must have Administrator privileges—that is, the Administrator user access role must be assigned to your user account—in order to use the Prime Network Administration GUI. This guide is intended for use by trained administrators.

This preface contains the following sections:

- New and Changed Information, page xiv
- Organization of This Guide, page xiv
- Conventions, page xvii
- Related Documentation, page xvii
- Obtaining Documentation and Submitting a Service Request, page xviii
New and Changed Information

The following table describes information that has been added or changed since this guide was first published.

Table 1  New and Changed Information in This Document

<table>
<thead>
<tr>
<th>Date Released</th>
<th>Revision</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 8, 2013</td>
<td>Resolved CSCud16392—In the device prerequisites, added a missing SNMPv3</td>
<td>SNMP Traps and</td>
</tr>
<tr>
<td></td>
<td>command that configured the write community on a device. If not set,</td>
<td>Informs—Required</td>
</tr>
<tr>
<td></td>
<td>Change and Configuration Management would not be able to back up the</td>
<td>Device Settings,</td>
</tr>
<tr>
<td></td>
<td>device’s configuration.</td>
<td>page A-8</td>
</tr>
<tr>
<td></td>
<td>Resolved CSCue38276—For standby units, corrected text to say that units</td>
<td>Overview of Unit</td>
</tr>
<tr>
<td></td>
<td>can only be configured during the Prime Network installation process.</td>
<td>Server High Availability,</td>
</tr>
<tr>
<td></td>
<td>Resolved CSCue51561—Corrected description of maintenance mode to say</td>
<td>page 16-1</td>
</tr>
<tr>
<td></td>
<td>that when a VNE is in maintenance state, it does not process traps and</td>
<td></td>
</tr>
<tr>
<td>September 6, 2012</td>
<td>syslogs. Also clarified that maintenance VNEs do passively participate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in correlation flows.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resolved CSCsz62728—Added a note that tells users they should not change</td>
<td>Why Device Configuration Tasks</td>
</tr>
<tr>
<td></td>
<td>a device’s default packet size because doing so could cause responses to</td>
<td>Are Important, page 1</td>
</tr>
<tr>
<td></td>
<td>SNMP get requests to be truncated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resolved CSCub09512—Added a “Before You Begin” section to the procedure</td>
<td>Creating VNEs Using the Network</td>
</tr>
<tr>
<td></td>
<td>for using the Network Discovery feature to add VNEs. The new section</td>
<td>Discovery Feature, page 23</td>
</tr>
<tr>
<td></td>
<td>instructs users to make sure that the gateway running the discovery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>process can reach the target devices using the management protocols</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(SNMP and Telnet/SSH).</td>
<td></td>
</tr>
<tr>
<td>July 18, 2012</td>
<td>Updated the lists of settings required to configure syslogs for Cisco</td>
<td>Syslogs—Required</td>
</tr>
<tr>
<td></td>
<td>IOS XR.</td>
<td>Device Settings, page 13</td>
</tr>
<tr>
<td>June 13, 2012</td>
<td>Initial release.</td>
<td></td>
</tr>
</tbody>
</table>

Organization of This Guide

This guide includes the following chapters and appendixes:

<table>
<thead>
<tr>
<th>Chapter/Appendix</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 1: Introduction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Getting Started with Prime Network</td>
<td>Describes the basic steps for deploying Prime Network, using the Prime Network Administration GUI client, and using Prime Network with Cisco Prime Central.</td>
</tr>
<tr>
<td>Chapter/Appendix</td>
<td>Title</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Part 2: Basic Gateway and Unit Administration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Basic Gateway Server Administration Tasks</td>
<td>Explains how to perform basic gateway administration tasks, such as viewing gateway properties, starting and stopping the gateway server, and creating a message that is displayed whenever users log into the gateway or GUI clients.</td>
</tr>
<tr>
<td>3</td>
<td>Basic Unit Server Administration Tasks</td>
<td>Explains how to administer units, check their status, and view their properties.</td>
</tr>
<tr>
<td>4</td>
<td>Basic AVM and VNE Administration Tasks</td>
<td>Explains how to administer AVMs and check their status, including using the AVM auto-add and load balancing mechanisms. Also provides some procedures for performing basic VNE administration tasks.</td>
</tr>
<tr>
<td>5</td>
<td>Licensing</td>
<td>Types of licenses supported by Prime Network, how to install and manage licenses, and how to generate a license report.</td>
</tr>
<tr>
<td>6</td>
<td>Configuring Event Notifications</td>
<td>Explains how to configure event notification services that forward event and ticket information to OSSs. Events you can forward include nonactionable events (events that cannot be parsed, including events from unmanaged devices).</td>
</tr>
<tr>
<td>7</td>
<td>Managing User Security: Roles and Scopes</td>
<td>Explains how Prime Network manages user authentication and authorization using role-based access control that control user access, and device scopes that control device access. Describes managing users using external authentication, and how to manage user accounts and passwords.</td>
</tr>
<tr>
<td>8</td>
<td>Backup and Restore</td>
<td>Describes the Prime Network backup and restore procedures (without an embedded database).</td>
</tr>
<tr>
<td><strong>Part 3: Advanced Gateway and Unit Administration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Advanced Administration for the Prime Network Gateway and Units</td>
<td>Describes advanced tasks, such as working with firewalls, restarting AVMs in a gradual manner, and how to get diagnostic information using the Prime Network Monitoring tool. Also describes the Automatic Overload Prevention mechanism, how to change the gateway IP address, and how to manage gateway open sessions.</td>
</tr>
<tr>
<td>10</td>
<td>Archiving and Purging Data</td>
<td>Explains how Prime Network archives and purges data to maintain system stability.</td>
</tr>
<tr>
<td>11</td>
<td>Working With an Embedded Database</td>
<td>Explains how to use Prime Network to manage an embedded database, including backing up and restoring an embedded database.</td>
</tr>
<tr>
<td>12</td>
<td>Workflow Administration Tasks</td>
<td>Explains how to manage workflows and templates (aborting, deleting, and so forth).</td>
</tr>
<tr>
<td>13</td>
<td>System Security</td>
<td>Describes the security features used by Prime Network to secure communication between Prime Network components.</td>
</tr>
<tr>
<td>14</td>
<td>Managing the Event Collector (AVM 100)</td>
<td>Describes Prime Network Event Collector, the role the EC plays in event flows, and how to configure single and multiple Event Collectors (AVM 100s).</td>
</tr>
<tr>
<td>15</td>
<td>Utility Scripts</td>
<td>Describes utility scripts available for use with Prime Network, including scripts for bulk VNE additions, changing passwords, and running commands on all units.</td>
</tr>
<tr>
<td>16</td>
<td>Unit Server High Availability and AVM Protection</td>
<td>Describes unit server high availability and AVM protection (watchdog protocol) options.</td>
</tr>
<tr>
<td>Chapter/Appendix</td>
<td>Title</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>17</td>
<td>Using Veritas Gateway Server High Availability</td>
<td>Describes the gateway server high availability and disaster recovery solution that uses Veritas software.</td>
</tr>
<tr>
<td>18</td>
<td>Using RHCS/ADG Gateway Server High Availability</td>
<td>Describes the gateway server high availability and disaster recovery solution that uses Red Hat Cluster Suite (RHCS) and Oracle Active Data Guard (ADG).</td>
</tr>
<tr>
<td></td>
<td><strong>Part 4: Basic VNE Administration</strong></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>VNE Administration: VNE Lifecycle and Creating VNEs</td>
<td>Explains how device reachability is reflected in VNE status, how to choose a VNE scheme, creating VNEs and viewing their properties, and controlling the VNE lifecycle. Also describes the VNE staggering mechanism for controlling concurrent VNE Telnet logins.</td>
</tr>
<tr>
<td>20</td>
<td>Troubleshooting VNE Modeling</td>
<td>Describes VNE communication and investigation states and how to troubleshoot problems that are indicated by state changes.</td>
</tr>
<tr>
<td>21</td>
<td>VNE Updates</td>
<td>Explains how to obtain and install VNE updates (new device driver packages).</td>
</tr>
<tr>
<td></td>
<td><strong>Part 5: Advanced VNE Administration</strong></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Customizing VNE Polling</td>
<td>Describes the polling mechanisms: reduced polling, adaptive polling groups, smooth polling, and smart polling. Also describes how to address high CPU usage problems.</td>
</tr>
<tr>
<td>23</td>
<td>Unmanaged Network Segments (Cloud VNEs) and Dynamic/Static Links</td>
<td>Explains how to create a Cloud VNE to work with unmanaged network segments, and how to add and remove topological (static) links.</td>
</tr>
<tr>
<td>24</td>
<td>Device Reachability</td>
<td>Explains how to get details about protocol communication for a VNE, and what communication policies are and how to change them. Describes how Prime Network determines protocol reachability and how it can be customized. Provides troubleshooting steps for VNE connectivity problems.</td>
</tr>
<tr>
<td>25</td>
<td>VNE Collectors and Command Priorities</td>
<td>Describes VNE collectors, how VNE collectors execute the commands required to build a model of a device, and how to customize the order in which the commands are executed.</td>
</tr>
<tr>
<td>26</td>
<td>VNE Persistency Mechanism</td>
<td>Describes the VNE persistency mechanism, including alarm, instrumentation, and topology persistency.</td>
</tr>
<tr>
<td></td>
<td><strong>Part 6: Appendixes</strong></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Device Configuration Tasks for VNE Creation</td>
<td>Lists the device configuration tasks that are required for proper VNE modeling and guidelines for choosing a VNE scheme.</td>
</tr>
<tr>
<td>B</td>
<td>Prime Network Log Files</td>
<td>List the logs generated by Prime Network and provides information about logging mechanism default behavior and how to change it.</td>
</tr>
<tr>
<td>C</td>
<td>Working with the Registry</td>
<td>Describes the golden source registry and how to edit it.</td>
</tr>
</tbody>
</table>
Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

**Tip**

Means *the following information will help you solve a problem.*

**Caution**

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation

**Note**

We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

For all the related documentation for Cisco Prime Network 3.9, see the *Prime Network 3.9 Documentation Overview*.

The Cisco Prime Network Technology Center is an online resource for additional downloadable Prime Network support content, including help for integration developers who use Prime Network application programming interfaces (APIs). The website provides information, guidance, and examples to help you integrate your applications with Prime Network. It also provides a platform for you to
interact with subject matter experts. To view the information on the Prime Network Technology Center website, you must have a Cisco.com account with partner level access, or you must be a Prime Network licensee. You can access the Cisco Prime Network Technology Center at: http://developer.cisco.com/web/prime-network/home.

**Obtaining Documentation and Submitting a Service Request**

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
PART 1

Introduction
CHAPTER 1

Getting Started with Prime Network

These topics provide some basic steps for getting started with Prime Network, such as how to set up the system and the basic parts of the Prime Network Administration GUI client.

- Basic Steps for Deploying Prime Network, page 1-1
- Launching the Prime Network Administration GUI Client, page 1-4
- Using Prime Network with Cisco Prime Central, page 1-4
- Parts of the Prime Network Administration Window, page 1-6
- Working with Prime Network Tables, page 1-36

For information on how to download and install the GUI clients, see the Cisco Prime Network 3.9 Installation Guide.

Note
A Prime Network base license must be registered and activated within 120 days of installation or upgrade. If there are no valid license files on the gateway server, Prime Network acts as an evaluation version. This means that it has full functionality for 120 days after installation, and then it expires and UI connections will be disallowed.

Basic Steps for Deploying Prime Network

This topic provides the basic steps you must perform in order to properly deploy Prime Network. For more specific deployment information and recommendations, such as supported configurations and system sizing, contact your Cisco account representative.

Note
A Prime Network base license must be registered and activated within 120 days of installation or upgrade. If there are no valid license files on the gateway server, Prime Network acts as an evaluation version. This means that it has full functionality for 120 days after installation, and then it expires and UI connections will be disallowed.

1. Prepare a deployment plan. You must decide on the following:
   - Whether you want to implement gateway server high availability.
   - The number of Prime Network unit servers to be deployed and the number of AVMs for each server.
Basic Steps for Deploying Prime Network

1. Plan for Prime Network deployment:
   - The number and types of VNEs to be managed.
   - The number of protection groups there are going to be and how Prime Network units are going to be organized into protection groups (clusters) for unit server high availability, based on the device type, geographical location, importance of device, and number of devices.
   
   **Note**
   The planning of protection groups in the deployment plan is only applicable when unit server high availability is enabled. For more information, see Unit Server High Availability and AVM Protection, page 16-1
   
   - If you will use unit server high availability, the number of standby Prime Network units that are going to be deployed.
   - How Prime Network units, standby units, and protection groups are going to be deployed and allocated.
   - The number of network scopes that are required and the policies they will employ.
   - The number of users to be defined.

2. Set up and manage Prime Network servers:
   a. Add Prime Network units. Transport links are created automatically between the unit and its associated gateway in a star topology or between two units. See Viewing Unit Properties, page 3-2. In addition, you can configure units for high availability and assign the units to protection groups. Units can be designated as standby during the installation process, and assigned to protection groups (optional). For more information, see Unit Server High Availability and AVM Protection, page 16-1
   
   b. Create and launch AVMs. This includes deciding where AVM 100 (Event Collector) should run. See Basic AVM and VNE Administration Tasks, page 4-1, and Managing the Event Collector (AVM 100), page 14-1
   
   c. Create and assign VNEs. (The Prime Network auto-add mechanism can assign them the units and AVMs in your system.)

3. Concurrently with the previous step, change the default setup of Prime Network units by customizing protection groups (clusters) and then assigning units to these groups. For more information, see Unit Server High Availability and AVM Protection, page 16-1


6. (Optional) Configure event notifications to forward events to OSSs. See Configuring Event Notifications, page 6-1.

7. (Optional) Manage and run workflows in runtime using the Workflow Engine windows. See Workflow Administration Tasks, page 12-1


10. Customize how long fault information and reports are saved. See Archiving and Purging Data, page 10-4.

11. (Optional) Create a message of the day that users will see whenever they log in to a Prime Network client. See Creating a GUI Client Banner Message, page 2-5.

12. If you are using EMS functionality only and your network has more than 1,000 VNEs, you must disable the discovery processes for all topology and services. If you do not, Prime Network will not be able to support a medium-to-large EMS setup. Disable the processes using the following procedure.

To disable the discovery for all topology and services:

**Step 1** Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39), and change to the Main directory by entering the following command:

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

**Step 2** Enter the following commands to disable the topology and service discovery processes and reduce memory consumption:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/mvm/services/plugin/VtpSnapshotProviderPlugin/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/mvm/services/plugin/EfdPlugin/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/mvm/services/plugin/XconnectDiscoveryPlugin/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/mvm/services/plugin/NetworkVlanDiscoveryPlugin/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/mvm/services/plugin/VmplsSnapshotProviderPlugin/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/mvm/services/plugin/VmplsDiscoveryPlugin/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/mvm/services/plugin/VlanSnapshotProviderPlugin/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/mvm/services/plugin/MartiniSnapshotProviderPlugin/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/mvm/services/plugin/PseudowireDiscoveryPlugin/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/agentdefaults/da/amsi/topology/common/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/agentdefaults/da/amsi/topology/tunnel/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/agentdefaults/da/amsi/topology/cloud/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/agentdefaults/da/amsi/topology/ethernet/enable false
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/agentdefaults/da/amsi/topology/vrf/enable false
```

**Step 3** Restart Prime Network:

```
# networkctl restart
```
Launching the Prime Network Administration GUI Client

**Note**
If Prime Network is installed with Cisco Prime Central, logging in is done from the Cisco Prime Portal by choosing **Assure > Prime Network > Administration**. If a user tries to log into a Prime Network standalone or Webstart client, they will be redirected to the Cisco Prime Portal. For more information about using Prime Network with Cisco Prime Central, see the **Cisco Prime Central 1.0 User Guide**.

Prime Network Administration is password-protected to ensure security and is available only to users with administrator privileges. If a user does not log into any of the GUI clients for a specified period of time (the default is one month), the user account is locked. Unlocking accounts and specifying the lockout time period is described in **Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22**.

When you log out, any changes that were made are automatically saved, including changes to VNEs. However, for some changes that are made to AVMs and VNEs, you must restart the AVMs or VNEs for your changes to be applied; those requirements are noted with the relevant procedures. You can do this before logging out or when you log back in.

Instructions for downloading and installing clients are provided in the **Cisco Prime Network 3.9 Installation Guide**. To launch the Administration GUI client, use one of the following:

- **Start > Programs > Cisco Prime Network > Prime Network Administration** to launch the full standalone client. You will have to enter the gateway IP address in addition to your credentials.
- **Start > Programs > Cisco Prime Network > gateway-ip > Prime Network Administration** to launch the Webstart client. You will have to enter your credentials.

Using Prime Network with Cisco Prime Central

Prime Network can be installed as a standalone product or with Cisco Prime Central. When installed with Cisco Prime Central, you can launch Prime Network GUI clients from the Cisco Prime Portal. Cross-launch to and from other suite applications is also supported. The applications share a common inventory.

The Cisco Prime Portal uses a single sign-on (SSO) mechanism so that users need not reauthenticate with each GUI client. All session management features are controlled by the portal (such as client timeouts). If a user tries to log into a standalone GUI client, the user will be redirected to the portal login. The only exception is the emergency user, who will still be allowed to log into a standalone GUI client.

These Prime Network features are disabled in suite mode because they are controlled at the suite level:

- All of the Security Settings that are available from the Global Settings branch (configuring the user authentication method, password rules, and client inactivity lockout period)
- Adding, deleting, and changing user accounts (including user passwords)
- Licensing

Prime Network sends the suite regular information about Prime Network server health (ping, CPU usage, and memory usage). At hourly intervals, Prime Network checks the suite for any changes that should be reflected in Prime Network.
Keep these operational items in mind when using Prime Network with Cisco Prime Central:

- When you create new VNEs, use the device SYSNAME as the VNE name. This allows other suite applications to recognize the device. Also, do not use None or All as the SYSNAME, because those names have internal meaning to Cisco Prime Central.

- If you migrate from standalone to suite mode, all user security roles are migrated to the suite, but device scopes are not migrated. After the migration is complete, you must create user accounts in Cisco Prime Central, using the same username that were used in standalone Prime Network. Cisco Prime Central will advise you that the user already existed in Prime Network and will retrieve the user properties and apply them to the new Cisco Prime Central user.

- If the Cisco Prime Performance Manager application is also installed, the Prime Network Event Collector will receive threshold crossing alarm (TCA) events from Prime Performance Manager components and do the following:
  - Save TCA events in the Event Archive.
  - Forward TCA events to appropriate VNEs. The events are currently not parsed by the VNE. They will be identified as generic traps and will be dropped. If desired, you can forward them to an Event Notification Service (see Configuring an Event Notification Service, page 6-3).

No special configuration is required.

Prime Network also receives EPM-MIB traps from the network. By default Prime Network receives EPM-MIB traps from any source in the network. If desired, you can configure Prime Network to only process EPM-MIB traps arriving from a specific Prime Performance Manager server. The instructions for doing this are provided on the Cisco Developer Network at http://developer.cisco.com/web/prime-network/home.
Parts of the Prime Network Administration Window

Figure 1-1 identifies the parts of the Prime Network Administration window.

Figure 1-1  Prime Network Administration Window
Chapter 1      Getting Started with Prime Network

Parts of the Prime Network Administration Window

1. Menu bar, with main menu choices
2. Toolbar, with content that depends on your current selection
3. Navigation area, where you pick items from a navigation tree to perform actions on the items (see Navigation Pane, page 1-7)
4. Content area, with content that depends on your current selection (see Content Area and Tables, page 1-8)
5. Shortcut menu, with content that depends on your current selection
6. Status bar, which displays the memory usage of the application process, and connection status

Dragging the window borders adjusts the size of each area.

Navigation Pane

The navigation pane displays a tree-and-branch representation of the Prime Network Administration folders. The branches can be expanded and collapsed to display and hide information as needed.

The following table lists the Prime Network Administration branches and identifies the tasks associated with each.

<table>
<thead>
<tr>
<th>Branch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All Servers</strong></td>
<td>Manage the Prime Network gateway and units, including AVMs and VNEs. The All Servers windows include:</td>
</tr>
<tr>
<td></td>
<td>• Gateway and Units Windows, page 1-11</td>
</tr>
<tr>
<td></td>
<td>• AVMs Windows, page 1-14</td>
</tr>
<tr>
<td></td>
<td>For more information, see All Servers Windows, page 1-9.</td>
</tr>
<tr>
<td><strong>Event</strong></td>
<td>Manage and configure event notifications. For more information, see Event Notification Window, page 1-16.</td>
</tr>
<tr>
<td><strong>Notification</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Global</strong></td>
<td>Manage system-wide settings. The Global Settings windows include:</td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>• Automatic AVM Management Window, page 1-18</td>
</tr>
<tr>
<td></td>
<td>• Event Management Settings Window, page 1-19</td>
</tr>
<tr>
<td></td>
<td>• License Report Window, page 1-21</td>
</tr>
<tr>
<td></td>
<td>• Message of the Day Window, page 1-22</td>
</tr>
<tr>
<td></td>
<td>• Polling Groups Window, page 1-23</td>
</tr>
<tr>
<td></td>
<td>• Protection Groups Window, page 1-24</td>
</tr>
<tr>
<td></td>
<td>• Report Settings Window, page 1-25</td>
</tr>
<tr>
<td></td>
<td>• Security Settings Window, page 1-26 (which includes authentication method, password, and user account settings)</td>
</tr>
<tr>
<td></td>
<td>For more information, see Global Settings Windows, page 1-17.</td>
</tr>
<tr>
<td><strong>Scopes</strong></td>
<td>Group a collection of managed network elements so users can view and manage network elements based on their specified role. For more information, Scopes Window, page 1-29.</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>Manage topology-related parameters, namely, the static links you can create between devices. For more information, see Topology Window, page 1-31</td>
</tr>
</tbody>
</table>
Parts of the Prime Network Administration Window

Click an item in the navigation tree to view information relating to the selection in the content area. Right-click an item in the navigation tree to open a shortcut menu to perform various functions.

### Note

The menus and toolbar displayed in the Prime Network Administration window are context sensitive; the options vary depending on your selection in the navigation pane and content area.

**Content Area and Tables**

The content area displays Prime Network Administration information that is related to the item selected in the navigation pane. The content area is divided into the following two parts:

- **Upper pane**—Displays the properties of the element that is selected in the navigation pane.
- **Lower pane**—Displays the element’s nested children in table format.

**Note**

Use the Ctrl key to select multiple rows in a table.

For more details about how to filter and manipulate table data, see Table Toolbar Options, page 1-36 and Filtering Table Contents, page 1-38.

**Menus**

All main menus in Prime Network Administration windows contain the following menu options. Additional options are also displayed, depending on the selection in the navigation tree.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File</strong></td>
<td></td>
</tr>
<tr>
<td>Exit</td>
<td>Exits Prime Network Administration.</td>
</tr>
<tr>
<td><strong>Tools</strong></td>
<td></td>
</tr>
<tr>
<td>Change User Password</td>
<td>Changes a user’s password; takes effect the next time they log into the GUI client. This allows individual users to change their own passwords. (Administrators can change passwords from the Users branch.)</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This choice is disabled if Prime Network is installed with Cisco Prime Central.</td>
</tr>
</tbody>
</table>
| Device Proxy Options| Creates a connection route between a GUI client and a device when they are separated by a firewall. Complete instructions are provided in Managed Devices Behind Firewalls, page 9-2.
Chapter 1  

Getting Started with Prime Network  

Parts of the Prime Network Administration Window  

These topics provide detailed descriptions of the information displayed in the Prime Network Administration window for each of the following:  

- All Servers Windows, page 1-9  
- Event Notification Window, page 1-16  
- Global Settings Windows, page 1-17  
- Scopes Window, page 1-29  
- Topology Window, page 1-31  
- Users Window, page 1-32  
- Workflow Engine Windows, page 1-33  

### All Servers Windows  

Prime Network Administration maintains a list of all servers defined in the system. The All Servers functions are used to add and remove unit servers and AVMs that reside on the gateway (or unit).  

The All Servers window contains the following:  

- Gateway and Units Windows, page 1-11  
- AVMs Windows, page 1-14  

You can expand this branch to view a list of the gateways, units, and AVMs. Each gateway, unit, and AVM has its own sub-window. These windows used to manage information relating to the AVMs and VNEs contained in the units.  

Note  

AVMs and VNEs reside on a unit as a common configuration, but they can also reside on a gateway.
Figure 1-2 shows an example of the Prime Network Administration window with All Servers selected. Note that the content area contains information about all servers in the system.

**Figure 1-2       All Servers Window**

Any changes that are made to the All Servers windows are automatically saved and immediately registered in Prime Network.

The top portion of the window summarizes the number of units in the system (the gateway is also considered a unit in this example). The following describes the columns displayed in the All Servers table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of gateway or unit.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the gateway or unit as defined in Prime Network Administration.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the gateway or unit: Up, Down, Unreachable, or Disconnected.</td>
</tr>
<tr>
<td>Up Since</td>
<td>The date and time when the gateway or unit was last loaded.</td>
</tr>
<tr>
<td>Physical Memory</td>
<td>The total physical memory on the gateway or unit (both free and in use).</td>
</tr>
<tr>
<td>Memory/Up AVMs</td>
<td>The total physical memory apportioned to Up AVMs on the unit or gateway (both user-created and reserved AVMs). This figure does not reflect the memory is in use by AVMs (that figure is represented by Allocated Memory Up AVMs, which you can view by right-clicking a gateway or unit and selecting <strong>Properties</strong>). It includes the additional 35% memory the operating system adds to the AVM size when the AVM is created. (See How Prime Network Allocates Memory to AVMs, page 4-2). The total memory being used by the AVMs in the gateway or unit.</td>
</tr>
</tbody>
</table>
Chapter 1      Getting Started with Prime Network

Parts of the Prime Network Administration Window

The following shows the All Servers toolbar options.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory/All AVMs</td>
<td>The total physical memory apportioned to all AVMs on the unit or gateway (both user-created and reserved AVMs), 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, which you can view by right-clicking a gateway or unit and selecting Properties). This total includes the additional 35% memory the operating system adds to the AVM size when the AVM is created. (See How Prime Network Allocates Memory to AVMs, page 4-2).</td>
</tr>
<tr>
<td>Protection Group</td>
<td>The protection group to which the unit is allocated (for unit server high availability).</td>
</tr>
<tr>
<td>AVM HA</td>
<td>Indicates whether AVM protection is enabled (true) on the gateway. AVM protection monitors the AVM processes and restarts them in case of failure. This should always be enabled.</td>
</tr>
<tr>
<td>Enable Unit Protection</td>
<td>(Units only) If checked, the unit is enabled for unit server high availability.</td>
</tr>
<tr>
<td></td>
<td>Note  This information is only available from the Unit properties dialog (right-click the unit and choose Properties).</td>
</tr>
</tbody>
</table>

The following shows the All Servers toolbar options.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="New" /></td>
<td>Creates a new VNE. If All Servers is selected, Prime Network will choose the appropriate unit and AVM. If you a specific gateway is selected, Prime Network will choose the appropriate AVM.</td>
</tr>
<tr>
<td><img src="image" alt="Search" /></td>
<td>Searches for AVMs and VNEs in the system (if All Servers is selected) or the gateway (if a gateway server is selected). The entity that is searched depends on what is selected in the navigation pane.</td>
</tr>
</tbody>
</table>

For more information about managing Prime Network servers, see Basic Unit Server Administration Tasks, page 3-1

Gateway and Units Windows

The Gateway and Unit windows list information about all gateways and units, enabling you to manage information relating to the AVMs and VNEs on a selected unit or gateway.
Figure 1-3 shows an example of the Prime Network Administration window with a specific gateway server selected.

**Figure 1-3 Gateway Window (Listing AVMs)**

Any changes that are made to the Gateway or Unit windows are automatically saved and immediately registered in Prime Network.

To list the information about a specific unit, choose the unit, as shown in Figure 1-4.

**Figure 1-4 Unit Window (Listing AVMs)**
To list all units in the system, choose All Servers and click the Units tab as shown in Figure 1-5. Note that the gateway server is also considered a unit server, since it can also serve that purpose.

**Figure 1-5  All Units Tab (from All Servers)**

The upper portion of the window provides general information about the selection. The following describes the columns that are displayed in the lower portion of the window, which lists the AVMs that are installed on the gateway or unit.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The name of the AVM as defined in Prime Network. It is unique to the AVM; for example, AVM 18.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the AVM: Starting Up, Up, Shutting Down, Down, or Unreachable.</td>
</tr>
<tr>
<td>Up Since</td>
<td>The date and time that the unit was last started.</td>
</tr>
<tr>
<td>Allocated Memory</td>
<td>The total physical memory being used by the AVM.</td>
</tr>
<tr>
<td>Total Memory Assigned</td>
<td>The total physical memory apportioned to the AVM. This figure does not reflect the memory is in use (that figure is represented by Allocated Memory). It includes the additional 35% memory the operating system adds to the AVM size when the AVM is created. (See How Prime Network Allocates Memory to AVMs, page 4-2).</td>
</tr>
<tr>
<td>Key</td>
<td>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 that is used depends on how you add the AVMs.</td>
</tr>
<tr>
<td>Auto-added AVMs</td>
<td>AVM ID (unit-ip)</td>
</tr>
<tr>
<td>Manually created AVMs</td>
<td>AVMID_nnn (where nnn is a unique designator assigned by Prime Network)</td>
</tr>
<tr>
<td>Enable Unit Protection</td>
<td>(Units only) If checked, the unit is enabled for unit server high availability.</td>
</tr>
</tbody>
</table>

**Note**  This information is only available from the Unit properties dialog (right-click the unit and choose Properties).
The following shows the toolbar options for the Gateway and Unit windows.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="New..." /></td>
<td>Creates a new VNE on the selected gateway or unit.</td>
</tr>
<tr>
<td><img src="image" alt="New..." /></td>
<td>Creates a new AVM on the selected gateway or unit.</td>
</tr>
<tr>
<td><img src="image" alt="Properties" /></td>
<td>Displays the selected gateway or unit properties and status.</td>
</tr>
<tr>
<td><img src="image" alt="Trash" /></td>
<td>(Units only) Deletes the selected unit.</td>
</tr>
<tr>
<td><img src="image" alt="Unlock" /></td>
<td>(Units only) Disconnects the selected unit.</td>
</tr>
<tr>
<td><img src="image" alt="Unlock" /></td>
<td>(Units only) Connects the selected unit.</td>
</tr>
<tr>
<td><img src="image" alt="Search" /></td>
<td>Searches for AVMs or VNEs in the gateway server or unit.</td>
</tr>
</tbody>
</table>

For more information managing the gateway and units, see Chapter 3, “Basic Unit Server Administration Tasks.”

**AVMs Windows**

You can view and manage AVMs and VNEs from the AVMs window. To list all AVMs or VNEs in the system, choose All Servers and click the AVMs or VNEs tab, as shown in Figure 1-6.

**Figure 1-6  All AVMs Tab (Listing AVMs)**
Figure 1-7 shows an example of the Prime Network Administration window with an AVM selected.

Figure 1-7   AVM Window (Listing VNEs)

![AVM Window (Listing VNEs)](image)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>The unique key of the VNE.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the device as defined in Prime Network Administration.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the VNE: Starting Up, Up, Shutting Down, Down, or Unreachable.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Indicates whether the VNE is (true) or is not (false) in maintenance mode.</td>
</tr>
<tr>
<td>Up Since</td>
<td>The date and time that the VNE was last started.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Indicates whether SNMP is enabled (true) or disabled (false) on the VNE.</td>
</tr>
<tr>
<td>Telnet</td>
<td>Indicates whether Telnet is enabled (true) or disabled (false) on the VNE.</td>
</tr>
<tr>
<td>Element Class</td>
<td>Detects the VNE category, such as Auto Detect, Generic SNMP, Cloud, or ICMP.</td>
</tr>
<tr>
<td>Element Type</td>
<td>The device type (manufacturer name), such as Cisco 7204.</td>
</tr>
<tr>
<td>Polling Group</td>
<td>The name of the customized polling group. The entry in this column is blank if the polling group is an instance.</td>
</tr>
<tr>
<td>Unit</td>
<td>The name of the parent unit.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the VNE device driver that the VNE is currently using.</td>
</tr>
<tr>
<td>Device Package Name</td>
<td>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.</td>
</tr>
<tr>
<td>Driver File Name</td>
<td>VNE device driver that is currently being used by the VNE.</td>
</tr>
</tbody>
</table>

Note: No VNEs are displayed when a reserved AVM is selected. Reserved AVMs are AVMs 1-100.
The following shows the AVM toolbar options. Different options are displayed depending on what is selected (an AVM or a VNE).

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="New..." /></td>
<td>Creates a new VNE in the selected AVM. You cannot create new VNEs on reserved AVMs (AVMs 0-100).</td>
</tr>
<tr>
<td><img src="image" alt="Properties" /></td>
<td>Displays the properties of the selected AVM or VNE.</td>
</tr>
<tr>
<td><img src="image" alt="Trash Can" /></td>
<td>Deletes the selected AVM or VNE.</td>
</tr>
<tr>
<td><img src="image" alt="Play" /></td>
<td>Starts the selected AVM or VNE.</td>
</tr>
<tr>
<td><img src="image" alt="Stop" /></td>
<td>Stops the selected AVM or VNE.</td>
</tr>
<tr>
<td><img src="image" alt="Maintenance" /></td>
<td>(VNEs only) Moves the selected VNE to maintenance mode.</td>
</tr>
<tr>
<td><img src="image" alt="Search" /></td>
<td>Searches for VNEs in the AVM. The AVM that is searched depends on what is selected in the navigation pane.</td>
</tr>
<tr>
<td><img src="image" alt="AVM Load Balancing" /></td>
<td>(AVMs only) Triggers the AVM load balancing feature. See Reducing AVM Loads and Checking AVM Status, page 4-11.</td>
</tr>
</tbody>
</table>

For more information, see Basic AVM and VNE Administration Tasks, page 4-1 and VNE Administration: VNE Lifecycle and Creating VNEs, page 19-1

### Event Notification Window

The Event Notification window allows you to create, modify, and delete custom event notification services. Figure 1-8 shows an example of the Prime Network Administration window with Event Notification selected.

Figure 1-8   Event Notification Window
The following describes the columns that are displayed in the Event Notification table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User-defined name for the notification service.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the notification service.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Destination port to which Prime Network is sending received events. Port 162 is used by default.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Destination IP address to which Prime Network is sending received events. Note: Events will only be forwarded if the Prime Network gateway server can communicate with the destination.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Transport protocol, either UDP (default) or TCP.</td>
</tr>
<tr>
<td>Notification Count</td>
<td>Number of notifications sent by this service.</td>
</tr>
</tbody>
</table>

The following shows the Event Notification toolbar options.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Opens the New Event Notification Service dialog box, enabling you to define a new event notification service for the current client station.</td>
</tr>
<tr>
<td></td>
<td>Displays the properties of the selected event notification service.</td>
</tr>
<tr>
<td></td>
<td>Starts the selected notification service.</td>
</tr>
<tr>
<td></td>
<td>Stops the selected notification service.</td>
</tr>
<tr>
<td></td>
<td>Deletes the selected event notification service from the system.</td>
</tr>
</tbody>
</table>

For information on managing event notifications, see Configuring Event Notifications, page 6-1

**Global Settings Windows**

The Global Settings windows control system-wide settings, such as polling and protection groups. Any changes that are made to the settings affect the configuration throughout the system.

The Global Settings windows include the following:

- Automatic AVM Management Window, page 1-18
- Event Management Settings Window, page 1-19
- Message of the Day Window, page 1-22
- Polling Groups Window, page 1-23
- Protection Groups Window, page 1-24
- Report Settings Window, page 1-25
- Security Settings Window, page 1-26
Automatic AVM Management Window

The Automatic AVM Management window allows you to control the size and memory thresholds for user-created AVMs that are added as part of the AVM auto-add feature. These settings do not apply to reserved AVMs. Figure 1-9 shows an example of the Prime Network Administration window with the Automatic AVM Management window selected.

Figure 1-9 Automatic AVM Management Window

The following describes the columns that are displayed in the Automatic AVM Management table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default AVM Size</td>
<td>The memory size to be used for auto-added AVMs. The default is 1500 MB.</td>
</tr>
<tr>
<td>Unit Reserved Memory</td>
<td>The percentage of memory that a unit should keep in reserve for auto-added</td>
</tr>
<tr>
<td></td>
<td>AVMs. If a unit exceeds its reserved memory, Prime Network will not add</td>
</tr>
<tr>
<td></td>
<td>auto-added AVMs to the unit. The default unit reserved memory is 90%.</td>
</tr>
<tr>
<td>Warning Threshold</td>
<td>The threshold at which, when surpassed, Prime Network will signal that an</td>
</tr>
<tr>
<td></td>
<td>AVM is approaching a load balancing issue (for an example, see Figure 4-5</td>
</tr>
<tr>
<td></td>
<td>on page 4-11).</td>
</tr>
</tbody>
</table>

For information on using the Prime Network AVM load balancing feature, see Reducing AVM Loads and Checking AVM Status, page 4-11.
Event Management Settings Window

The Event Management Settings page lets you specify how long Prime Network should archive and delete (purge) information in the Fault Database and Event Archive. This feature is enabled by default and removes events when they are 14 days old. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

The Fault Database and Event Archive tables are described in Prime Network Database Schemas, page 10-1.

Figure 1-10 shows an example of the Prime Network Administration window with the Event Management Settings selected.

Figure 1-10  Event Management Settings Window

The following describes the items in the Event Management Settings window content area.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault Database</td>
<td>For data saved in the Fault Database, specifies when to create time-based partitions and when to delete archived data.</td>
</tr>
<tr>
<td>Event Archive</td>
<td>For raw events saved in the Event Archive, specifies when to create time-based partitions and when to delete archived data.</td>
</tr>
</tbody>
</table>
Chapter 1  Getting Started with Prime Network

Parts of the Prime Network Administration Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Event Viewer</td>
<td>Number of hours after which network and provisioning events are removed from the inventory event viewer in Prime Network Vision. The default is 6 hours. These settings are overridden if a user makes local changes to their Prime Network Vision GUI client (using <strong>Tools &gt; Options</strong> in their client).</td>
</tr>
<tr>
<td>Auto-Clear Tickets</td>
<td>System clears the tickets that are older than a predefined time and severity. For more information on setting auto-clear of tickets, see <strong>Auto-Clearing of Tickets</strong>, page 10-10.</td>
</tr>
</tbody>
</table>

For more information about the Event Management Settings and other data purging mechanisms, see **Archiving and Purging Data**, page 10-4.

**Job Manager Settings Window**

The Job Manager Settings window enables you to specify how long Prime Network should save job runs. **Figure 1-11** shows an example of the Prime Network Administration window with Job Manager Settings selected.

**Figure 1-11  Job Manager Settings Window**

![Job Manager Settings Window](image)

The Job Manager Purge Settings specifies how long to save reports and the maximum number of job runs that can be stored.

For more information about Job Manager Purge Settings, see **Automatic Purging of Old Jobs**, page 10-9.
License Report Window

The License Report window provides information about the basic license that is being used by the system. Figure 1-12 shows an example of the Prime Network Administration window with the License Report window selected.

Figure 1-12 License Report Window

The following describes the items in the License Report content area and table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>License Report generation time</td>
</tr>
<tr>
<td>Basic License</td>
<td>Production, Lab, or Unlicensed Evaluation.</td>
</tr>
<tr>
<td>Operating Mode</td>
<td>Backend designation denoting the type of management Prime Network is</td>
</tr>
<tr>
<td></td>
<td>performing: ELM (foundation and element management), NAS (network and service</td>
</tr>
<tr>
<td></td>
<td>monitoring), or ACT (service activation).</td>
</tr>
<tr>
<td>Evaluation Days</td>
<td>For Unlicensed Evaluation, the number of days remaining (out of 120)</td>
</tr>
<tr>
<td>Remaining</td>
<td></td>
</tr>
</tbody>
</table>

For more information about using the License Report window, see Viewing the License Report, page 5-5.
Message of the Day Window

The Message of the Day window enables you to define a message that is displayed when a user logs into any of the client applications. Figure 1-13 shows an example of the Prime Network Administration window with the Message of the Day selected.

Figure 1-13 Message of the Day Window

The following describes the items in the Message of the Day content area.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The title for the message. By default, the title “Terms of Use” is displayed.</td>
</tr>
<tr>
<td>Message</td>
<td>A free text message for the user. The message supports HTML format.</td>
</tr>
<tr>
<td></td>
<td>By default, Prime Network will insert <strong>Abort</strong> and <strong>Continue</strong> choices after the message. The user will have to click <strong>Continue</strong> or they will not be allowed to log in.</td>
</tr>
</tbody>
</table>

For an example and more information about using the Message of the Day window, see Creating a GUI Client Banner Message, page 2-5.
Polling Groups Window

The Polling Groups window enables you to manage device polling intervals by specifying the intervals you want, creating a group with those intervals, and then assigning VNEs to use that polling group. Figure 1-14 shows an example of the Prime Network Administration window with Polling Groups selected. Prime Network comes with two polling groups already created, named default and slow.

**Figure 1-14   Polling Groups Window**

The following describes the columns that are displayed in the Polling Groups table. The **default** and **slow** groups are created by Prime Network and cannot be edited or deleted.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Group</td>
<td>The polling group name defined by the user.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the polling group.</td>
</tr>
</tbody>
</table>

*Note*  Any changes that are made in the Polling Groups window are automatically saved and immediately registered in Prime Network.
The following table shows the Polling Groups toolbar options.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![New]</td>
<td>Creates a new polling group.</td>
</tr>
<tr>
<td>![Properties]</td>
<td>Displays the properties of the selected polling group.</td>
</tr>
<tr>
<td>![Delete]</td>
<td>Deletes the selected polling group.</td>
</tr>
</tbody>
</table>

*Note* The default polling group must not be deleted.

For information on how to create and manage polling groups, see [VNE Polling Groups and Slow Polling](#), page 22-23.

**Protection Groups Window**

By default, all units in the Prime Network fabric belong to one cluster or protection group. Prime Network comes with one default protection group, named default-pg. You can also create new protection groups and assign units to them, categorizing them to fit your needs. Figure 1-15 shows an example of the Prime Network Administration window with Protection Groups selected.

**Figure 1-15 Protection Groups Window**
The following describes the columns that are displayed in the Protection Groups table. The default-pg protection group is created by Prime Network and cannot be deleted.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The protection group name defined by the administrator.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the protection group.</td>
</tr>
</tbody>
</table>

The following table shows the Protection Groups toolbar options.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="New" /></td>
<td>Creates a new protection group.</td>
</tr>
<tr>
<td><img src="image" alt="Properties" /></td>
<td>Displays the properties of the selected protection group.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Deletes the selected protection group.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The default protection group must not be deleted.</td>
</tr>
</tbody>
</table>

For more information on creating and managing protection groups, see Unit Server High Availability and AVM Protection, page 16-1.

**Report Settings Window**

The Report Settings window enables you to specify how long Prime Network should save reports and whether users are allowed to create shared (public) reports. Figure 1-16 shows an example of the Prime Network Administration window with Report Settings selected.
### Security Settings Window

The global Security Settings window maintains system-wide user security settings and rules for user authentication, passwords, and client inactivity lockouts. Any changes that are made to the settings affect the configuration throughout the system.

**Note** The Security Settings are disabled if Prime Network is installed with Cisco Prime Central.

The global Security Settings windows include the following:

- Authentication Method Window, page 1-27
- Password Settings Window, page 1-28
- User Account Settings Window, page 1-29
Authentication Method Window

The Authentication Method window enables control of the method used to validate passwords for Prime Network users. If you use Prime Network for authentication, all passwords are validated by Prime Network and stored in the Prime Network database. If you use LDAP for authentication, all passwords are validated by the LDAP server and stored on an external LDAP server. Figure 1-17 shows an example of the Prime Network Administration window with Authentication Method selected.

Figure 1-17 Authentication Method Window

The following describes the items in the Authentication Method content area.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP URLs</td>
<td>LDAP server name and port number.</td>
</tr>
<tr>
<td>Distinguished Name Prefix</td>
<td>First part of the LDAP DN, which is used to uniquely identify users.</td>
</tr>
<tr>
<td>Distinguished Name Suffix</td>
<td>Second part of the LDAP distinguished name, which specifies the location in the directory.</td>
</tr>
<tr>
<td>Application-LDAP Protocol</td>
<td>Encryption protocol used for communication between the Prime Network gateway server and the LDAP server (simple or SSL).</td>
</tr>
</tbody>
</table>

The Test Connection button checks the connectivity between the Prime Network gateway server and the LDAP server. For more information about external authentication, see Using an External LDAP Server for Password Authentication, page 7-7.
Password Settings Window

The Password Settings window enables you to set password rules that apply to all user accounts. Figure 1-18 shows an example of the Prime Network Administration window with Password Settings selected.

![Password Settings Window](image)

The following describes the items in the Password Settings content area.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Validity Period</td>
<td>Number of days after which users must reset their password.</td>
</tr>
<tr>
<td>Number of Attempts Before Lockout</td>
<td>Number of attempts before a user’s account is disabled. (Administrators can reenable accounts as described in Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.</td>
</tr>
<tr>
<td>Password Strength</td>
<td>Password rules that are applied to all new passwords.</td>
</tr>
</tbody>
</table>

For more information about Password Settings, see Setting Global Password Rules, page 7-14.
User Account Settings Window

The User Account Settings window enables you to specify when Prime Network should disable user accounts due to account inactivity. The inactivity timer is measured in days. You can reenable the account as described in Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22. Figure 1-19 shows an example of the Prime Network Administration window with User Account Settings selected.

Figure 1-19  User Account Settings Window

The following describes the items in the User Account Settings content area.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable account if inactive for ____ days</td>
<td>Number of days of inactivity, after which the user account is disabled. (Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.)</td>
</tr>
</tbody>
</table>

For more information about User Account Settings, see Automatically Disabling Accounts for Inactive Users, page 7-15.

Scopes Window

The Scopes window lets you create groups of managed network elements and control who can view and manage those network elements. Access is controlled according to the settings for a user’s account. Prime Network comes with one default scope named All Managed Elements; all managed network
elements belong to that scope. For more information on the Scopes window, see Managing User Security: Roles and Scopes, page 7-1. Figure 1-20 shows an example of the Prime Network Administration window with Scopes selected.

**Figure 1-20  Scopes Window**

Each row in the table displays the name of a scope as defined in Prime Network Administration. The following shows the Scopes toolbar options.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="New" /></td>
<td>Creates a new scope. See Creating and Managing Scopes, page 7-16.</td>
</tr>
<tr>
<td><img src="icon" alt="Properties" /></td>
<td>Displays the properties of the selected scope.</td>
</tr>
<tr>
<td><img src="icon" alt="Delete" /></td>
<td>Deletes the selected scope.</td>
</tr>
</tbody>
</table>

For more information about scopes, see Device Scopes, page 7-3.
**Topology Window**

The Topology window enables you to define static links between two network elements to supplement or override existing autodiscovered topology. Figure 1-21 shows an example of the Prime Network Administration window with Topology selected.

![Topology Window](image)

The Topology window displays all static links defined in the system, including the A side and Z side of the link.

The following shows the Topology toolbar options.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="New Link" /></td>
<td>Opens the New Link dialog box, enabling you to create a link between two devices. See Creating and Deleting Static Links, page 23-8.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Deletes the selected static link.</td>
</tr>
</tbody>
</table>

For more information about the Topology window and links, see Unmanaged Network Segments (Cloud VNEs) and Dynamic/Static Links, page 23-1
Parts of the Prime Network Administration Window

Chapter 1  Getting Started with Prime Network

Users Window

The Users window enables you to define and manage user accounts. For more information about the Users window, see Chapter 7, “Managing User Security: Roles and Scopes.”

Note  If Prime Network is installed with Cisco Prime Central, you can view user properties but you cannot add or change them.

Figure 1-22 shows an example of the Prime Network Administration window with Users selected.

Figure 1-22     Users Window

The following describes the columns that are displayed in the Users table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The unique username defined for the current client station.</td>
</tr>
<tr>
<td>Full User Name</td>
<td>(Optional) full username.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the user.</td>
</tr>
<tr>
<td>Default Permission</td>
<td>The default permission of the user, such as Viewer or Administrator. For example, a user with the default permission Viewer can view maps and the Device List.</td>
</tr>
<tr>
<td>Note</td>
<td>The default permission applies only at an application level; that is, it applies to all activities that are related to GUI functionality and not the activities related to devices. See Managing User Security: Roles and Scopes, page 7-1</td>
</tr>
<tr>
<td>Last Login</td>
<td>The date and time that the user last logged in.</td>
</tr>
<tr>
<td>External</td>
<td>Indicates whether an external authentication server is used for account and password verification. See External Authentication, page 7-2.</td>
</tr>
<tr>
<td>Emergency</td>
<td>Indicates that a user is designated as an emergency user for the external authentication server, in case the external server goes down. See External Authentication, page 7-2.</td>
</tr>
</tbody>
</table>
The following table shows the Users toolbar options.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="New User Icon" /></td>
<td>Opens the New User dialog box, enabling you to define a new user for the current client station.</td>
</tr>
<tr>
<td><img src="image" alt="Properties Icon" /></td>
<td>Displays the properties of the selected user.</td>
</tr>
</tbody>
</table>
| ![Trash Can Icon](image) | Deletes the selected username from the system.  
**Note** The user root cannot be deleted. |

For information on managing users, see Managing User Security: Roles and Scopes, page 7-1

**Workflow Engine Windows**

The Workflow Engine windows enable you to view and delete workflow templates and perform Administration tasks on workflows. The templates are used by the Workflow Editor (which is based on LiquidBPM by Autonomy, Inc.). The Workflow Engine windows include the following:

- **Templates**—Displays a list of the deployed workflow templates and enables you to view the properties of the workflow template. For more information, see Templates Window, page 1-34.
- **Workflows**—Displays a list of the running or completed workflows and enables you to view their output and alter their current status. See Workflows Window, page 1-35.
Templates Window

The Templates window enables you to view deployed workflow templates, view template properties, and delete a template.

Figure 1-23 shows an example of the Prime Network Administration window with Templates selected.

Figure 1-23   Workflow Templates Window

The table displays the names of the workflow templates, as defined using the Cisco Workflow Editor. The following shows the Templates toolbar option.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Trash Can]</td>
<td>Deletes the selected workflow template.</td>
</tr>
</tbody>
</table>

For more information about workflows, see:
- Workflow Administration Tasks, page 12-1
- Cisco Prime Network 3.9 Customization User Guide
**Workflows Window**

The Workflows window enables you to search and view the status of all workflows in the system, view workflow properties and output, and delete a workflow. *Figure 1-24* shows an example of the Prime Network Administration window with Workflows selected.

*Figure 1-24 Workflows Window*

![Workflows Window](image)

The following describes the columns that are displayed in the Workflows table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow ID</td>
<td>Unique identifier for the workflow (assigned by Prime Network).</td>
</tr>
<tr>
<td>Template Name</td>
<td>Name of the template used by this workflow. (All Prime Network Activation</td>
</tr>
<tr>
<td></td>
<td>templates are indicated by the prefix NSA_.)</td>
</tr>
<tr>
<td>Template Display Name</td>
<td>Name as displayed in Prime Network.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the workflow.</td>
</tr>
<tr>
<td>Execution Time</td>
<td>When the workflow was started.</td>
</tr>
<tr>
<td>User</td>
<td>User that executed the workflow.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Devices affected by the workflow. This data is gathered from workflows that</td>
</tr>
<tr>
<td></td>
<td>contain any DeviceName* attributes.</td>
</tr>
<tr>
<td>Device IP</td>
<td>IP address of devices affected by the workflow. This data is gathered from</td>
</tr>
<tr>
<td></td>
<td>workflows that contain any DeviceIP* or IPAddress* attributes.</td>
</tr>
<tr>
<td>Information</td>
<td>Informational data supplied when the workflow was created. This data is</td>
</tr>
<tr>
<td></td>
<td>gathered from workflows that contain any <em>Info</em> attributes.</td>
</tr>
<tr>
<td>Workflow ID</td>
<td>Unique identifier for the workflow (assigned by Prime Network).</td>
</tr>
</tbody>
</table>

For more information about workflows, see:

- [Workflow Administration Tasks](#), page 12-1
- [Cisco Prime Network 3.9 Customization User Guide](#)
Working with Prime Network Tables

RPrime Network uses tables to display different types of information. The following topics describe how to work with Prime Network tables so that you can view the information that you want and, optionally, save the information to a file:

- Table Toolbar Options, page 1-36
- Finding Text in a Table, page 1-37
- Sorting a Table, page 1-37
- Filtering Table Contents, page 1-38
- Viewing Selected Rows, page 1-40
- Exporting Tables to a File, page 1-41

To view all text in a table cell, you can do either of the following:

- Click the red triangle in the cell to automatically expand the cell to the size of the cell’s contents.
- Hover your mouse cursor over the cell.

Table Toolbar Options

The following table describes the options available in table toolbars.

<table>
<thead>
<tr>
<th>Option</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Find" /></td>
<td>Find</td>
<td>Searches the current table for the string you enter. For more information, see Finding Text in a Table, page 1-37.</td>
</tr>
<tr>
<td><img src="image" alt="Export to CSV" /></td>
<td>Export to CSV</td>
<td>Exports the information displayed in the table, or selected portions, to a CSV file. For more information, see Exporting Tables to a File, page 1-41.</td>
</tr>
<tr>
<td><img src="image" alt="Sort Table Values" /></td>
<td>Sort Table Values</td>
<td>Sorts the information displayed in the table by the criteria you specify. For more information, see Sorting a Table, page 1-37.</td>
</tr>
<tr>
<td><img src="image" alt="Filter" /></td>
<td>Filter</td>
<td>Filters the information displayed in the table by the criteria you specify. For more information, see Filtering Table Contents, page 1-38.</td>
</tr>
<tr>
<td><img src="image" alt="Clear Filter" /></td>
<td>Clear Filter</td>
<td>Clears the existing filter.</td>
</tr>
<tr>
<td><img src="image" alt="Show All Rows" /></td>
<td>Show All Rows</td>
<td>Displays all table rows that meet the current filtering criteria.</td>
</tr>
<tr>
<td><img src="image" alt="Show Only Selected Rows" /></td>
<td>Show Only Selected Rows</td>
<td>Displays only the rows that you select. For more information, see Viewing Selected Rows, page 1-40.</td>
</tr>
</tbody>
</table>
Using Keyboard Shortcuts in Tables

Table 1-1 lists the keyboard shortcuts that you can use when working with tables.

<table>
<thead>
<tr>
<th>Keyboard Shortcut</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl + A</td>
<td>Selects all the rows in the table.</td>
</tr>
<tr>
<td>Ctrl + Space</td>
<td>Deselects all the rows in the table.</td>
</tr>
<tr>
<td>Enter</td>
<td>On a selected row, opens the default action.</td>
</tr>
<tr>
<td>Arrow Navigation Keys</td>
<td>Navigates up and down in the rows.</td>
</tr>
<tr>
<td>Ctrl + Up/Down</td>
<td>Keeps the selected row and moves up or down.</td>
</tr>
<tr>
<td>Ctrl + Up/Down + Space</td>
<td>Keeps the selected row and moves up or down. The space selects the required row.</td>
</tr>
<tr>
<td>Shift + Up/Down</td>
<td>Keeps the selected row and selects all the rows that are above or below it.</td>
</tr>
<tr>
<td>Shift + F10</td>
<td>Opens the right-click menu.</td>
</tr>
<tr>
<td>F3</td>
<td>Finds next.</td>
</tr>
<tr>
<td>Shift + F3</td>
<td>Finds previous.</td>
</tr>
</tbody>
</table>

Finding Text in a Table

Prime Network enables you to search for information about a specific entry in a table by entering search criteria, such as a partial IP address.

To find text in a table:

**Step 1**  In the Find field on the toolbar, enter the search criterion for the entity that you want to find and press Enter.

**Step 2**  Press F3 to continue searching the table or press Ctrl + F to return to the Find field.

Sorting a Table

Prime Network enables you to sort a table in the following ways:

- According to a column, by clicking the required column heading.
- In ascending or descending order, by clicking a column heading.
- By clicking **Sort Table Values** in the toolbar and specifying sort criteria.

A triangle next in the column heading indicates the sort order:

- ![ Ascending Order ] indicates the column is sorted in ascending order.
- ![ Descending Order ] indicates the column is sorted in descending order.
To sort a table using the Sort Table Values option:

**Step 1** In the table toolbar, click **Sort Table Values**. The Sort dialog box is displayed.

**Figure 1-25  Sort Dialog Box**

In the Sort Operation field, specify the frequency of the sort operation:

- **Only Once**—Sorts the information in the table only once according to the specified criteria.
- **Continuously/Repeatedly**—Sorts the information in the table continuously according to the specified criteria.

If you select this option, the icon is displayed next to the selected column heading.

**Step 3** In the Sort By field, specify the first sort criterion:

a. In the first drop-down list, choose the column to use for the first sort criterion.

b. In the second drop-down list, choose **Ascending** or **Descending** to indicate the sort order.

**Step 4** If needed, click to add another sort criterion.

**Step 5** Adjust the sort criteria as needed:

- To add additional criteria, click .
- To remove a criterion, click .

**Step 6** Click **OK** to sort the table using the specified criteria.

---

**Filtering Table Contents**

You can view only those items that are of interest to you by filtering a table’s contents. This feature can be extremely helpful when working with tables that contain many entries.

**Note**

If you load a table with many entries, (for example, thousands of entries), it can take a while for the complete table to load. The filtering options in the table toolbar are unavailable until the table has completely loaded.
The following changes in the GUI indicate that a filter has been applied:

- The Filter button is slightly shaded.
- The Clear Filter button is active.
- The filter details are displayed:
  - In the status line below the table.
  - When you hover the mouse cursor over the Filter button.

To define a filter:

**Step 1**
In the toolbar above the table, click **Filter**. The Filter dialog box is displayed as shown in Figure 1-26.

*Figure 1-26  Table Filter Dialog Box*

**Step 2**
In the Match drop-down list, choose the rule for including items that meet the specified criteria:

- All—All of the following criteria are to be met.
- Any—Any of the following criteria are to be met.

**Step 3**
For each criterion, specify the following information:

a. In the first drop-down list, choose the primary match category. The drop-down list contains all columns in the current table.

b. In the second drop-down list, choose the rule to use for this criterion. The options are:
   - Contains
   - Does not contain
   - Equals
   - Does not equal
   - Greater than
   - Less than

c. The third field either lists the available values or allows you to enter text:
   - If a drop-down list is displayed, choose the required entry.
   - If an entry field is displayed, enter a string or regular expression for the criterion.
   Any entry that is not a regular expression is treated as a string.
Tip

You can use the “Greater than” or “Less than” rule with a string for filtering. For example, if you want to include all interfaces above Ethernet0/0/3, you can select **Greater than** and enter the string **Ethernet0/0/3** to view interfaces Ethernet0/0/4, Ethernet0/0/5, and so on.

**Step 4**  
Click [ ] to add another criterion for this filter.

**Step 5**  
Add additional criteria as required. To remove a criterion, click [ ].

**Step 6**  
When you have specified all criteria for the filter, click **OK**.

The table data is displayed using the defined filter.

**Step 7**  
To clear a filter, click **Clear Filter** in the table toolbar.

The table is refreshed and all entries are displayed.

The following tables have additional filtering capabilities (for more information, see the *Cisco Prime Network 3.9 User Guide*):

- Prime Network Vision ticket pane.
- Links view in the content pane.

### Viewing Selected Rows

Prime Network enables you to select a line or a specific set of lines, and display them in the table. The lines that you do not select are hidden from view.

You can use this feature with the filtering mechanism to view the specific entries that you need. You can either select specific rows and then apply a filter, or you can filter the table’s contents and then select specific rows to view.

If you apply a filter, the details of the filter are displayed below the table. For example, if you apply a filter that specifies all elements with names containing ME are to be displayed, the following appears in the table status line:

**Filter:** Name Contains ME

The status bar below the table also displays the:

- Number of the selected row, if a row is selected.
- Number of rows selected, if any.
- Total number of rows currently displayed in the table.

For example, if you select line four in a table with six rows, the following information is displayed:

**Line 4 (1/6 Selected)**

If no rows are selected, the value for the line defaults to 0, such as:

**Line 0 (Size 6)**
To view selected rows:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select the appropriate line or lines in the table using standard Windows mouse or keystroke operations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click <strong>Show Only Selected Rows</strong>.</td>
</tr>
<tr>
<td></td>
<td>The table displays the selected rows, and the Show All Rows option becomes active.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Show All Rows</strong> to view all rows in the table.</td>
</tr>
</tbody>
</table>

### Exporting Tables to a File

Prime Network enables you to export the currently displayed data from a table. You can either select specific rows to export, or clear all selections in the table to export the entire table. The data can then be imported and viewed at a later stage.

To export a table to a file:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Press <strong>Ctrl + Space</strong> to clear any existing selection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Identify the content you want to export:</td>
</tr>
<tr>
<td></td>
<td>• To export specific rows, select the required rows.</td>
</tr>
<tr>
<td></td>
<td>• To export the entire table, ensure that nothing is selected.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the table toolbar, click <strong>Export to CSV</strong>. The Export Table to File dialog box is displayed.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Navigate to the directory where you want to save the table.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the File name field, enter a name for the file.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Save</strong>. The content specified in <strong>Step 2</strong> is saved in the specified file and directory.</td>
</tr>
</tbody>
</table>
PART 2

Basic Gateway and Unit Administration
Basic Gateway Server Administration Tasks

The following topics describe the basic administration tasks you can perform to verify the health of the Prime Network gateway server, and how to stop the server and all system components:

- Overview of the Prime Network Gateway, page 2-1
- Viewing Gateway Properties in Prime Network Administration, page 2-2
- Starting and Stopping the Gateway and Checking AVM Status, page 2-3
- Creating a GUI Client Banner Message, page 2-5

Additional gateway administration tasks are described in Advanced Administration for the Prime Network Gateway and Units, page 9-1.

Overview of the Prime Network Gateway

The Prime Network gateway enforces access control and security for all connections and manages client sessions. It maintains a repository of 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 that is not directly contained in the network (such as information on VPNs and subscribers) and display it to northbound applications.

The default installation directory for Prime Network is /export/home/network user. In general, the Prime Network installation directory is referenced in user documentation by the variable NETWORKHOME.

When Prime Network is installed, a operating system account for the Prime Network application is created. This user account is called network user; an example of network user is network39. Based on the value for network user:

- Prime Network is installed by default in /export/home/network user. If at installation time, network user is defined as network39, and Prime Network is installed using the default settings, the Prime Network installation directory would be /export/home/network39.

- The NETWORKHOME environment variable is set to this Prime Network installation directory. Continuing with this example would result in the following:

  # echo $ANAHOME
  /export/home/network39
To connect to a gateway using Prime Network Administration (or any of the other GUI clients), you must first install the client software on your client machine. Installing the gateway and client software is described in the *Cisco Prime Network 3.9 Installation Guide*, along with other basic setup information. You can also connect to the gateway and check its status using `networkctl`; see Starting and Stopping the Gateway and Checking A VM Status, page 2-3.

As a best practice, use GMT (with 0 offset) on the gateway server.

### Viewing Gateway Properties in Prime Network Administration

When you right-click a gateway and select **Properties**, Prime Network displays the gateway properties, as shown in Figure 2-1. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

#### Figure 2-1 Gateway Status

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of gateway.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the gateway as defined in Prime Network Administration.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the gateway.</td>
</tr>
<tr>
<td>Up Since</td>
<td>The date and time when the gateway was last loaded.</td>
</tr>
</tbody>
</table>
When you select a specific gateway in the navigation tree, the GUI client displays all of the AVMs in the gateway including whether the AVM memory consumption is normal. That display is described in Viewing AVM Properties, page 4-6.

To stop or restart the gateway, use the `networkctl` command. The log for the gateway process is stored in `NETWORKHOME/Main/logs/11.out`.

### Starting and Stopping the Gateway and Checking AVM Status

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Memory</td>
<td>The total physical memory on the gateway (both free and in use).</td>
</tr>
<tr>
<td>Physical Memory Available</td>
<td>Of the total physical memory on the gateway, amount of memory that has not been assigned to any AVMs.</td>
</tr>
<tr>
<td>Total Memory Assigned All AVMs</td>
<td>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 How Prime Network Allocates Memory to AVMs, page 4-2).</td>
</tr>
<tr>
<td>Total Memory Assigned Up AVMs</td>
<td>The total physical memory apportioned to Up AVMs on the gateway (both user-created and reserved AVMs). This figure does not reflect the memory 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 How Prime Network Allocates Memory to AVMs, page 4-2).</td>
</tr>
<tr>
<td>Allocated Memory Up AVMs</td>
<td>The total physical memory being used by Up AVMs on the gateway (both user-created and reserved AVMs).</td>
</tr>
<tr>
<td>AVM HA</td>
<td>Indicates whether AVM protection is enabled (true) on the gateway. AVM protection monitors the AVM processes and restarts them in case of failure. This should always be enabled.</td>
</tr>
<tr>
<td>Enable Unit Protection</td>
<td>Indicates that the gateway is using unit server high availability; this cannot be disabled on the gateway.</td>
</tr>
</tbody>
</table>

When you select a specific gateway in the navigation tree, the GUI client displays all of the AVMs in the gateway including whether the AVM memory consumption is normal. That display is described in Viewing AVM Properties, page 4-6.

To stop or restart the gateway, use the `networkctl` command. The log for the gateway process is stored in `NETWORKHOME/Main/logs/11.out`.

### Starting and Stopping the Gateway and Checking AVM Status

**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 stop and restart the gateway, all Prime Network components are stopped and restarted. The gateway server and units can be stopped and restarted using the `networkctl` command. If you would rather start AVMs in a gradual manner (rather than having them automatically restart), you can use the GUI to do so, but you must perform (see Restarting Prime Network In a Gradual Manner, page 9-5).
You can use the `networkctl` command to check the Prime Network version that is running on the gateway, start and stop the gateway and all component processes (including AVMs you created), or just perform a general check of the system status.

**Note**
When you restart the gateway, all VNEs that were in maintenance mode will be moved to the Down state.

The `networkctl` command is located in `NETWORKHOME/Main`. It takes the following options:

```
networkctl [ start | stop | status | restart ]
```

<table>
<thead>
<tr>
<th>Options/Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>start</code></td>
<td>Starts the gateway process. With no options, this command starts the gateway and all component processes.</td>
</tr>
<tr>
<td><code>stop</code></td>
<td>Stops the gateway process. With no options, this command stops the gateway and all component processes. If AVM protection (watchdog protocol) is enabled, Prime Network will try to restart the process after a few minutes. If you do not want the process to be restarted, stop the AVM using the GUI; see Changing AVM Status (Start or Stop), page 4-12.</td>
</tr>
<tr>
<td><code>status</code></td>
<td>Displays the status of the gateway processes.</td>
</tr>
<tr>
<td><code>restart</code></td>
<td>Stops and starts the gateway processes. With no options, this command stops and restarts the gateway and all component processes.</td>
</tr>
</tbody>
</table>

When you run the `networkctl` command, the first few lines will display the Prime Network version you are running, as in the following example:

```
.-= Welcome to sjcn-sysm, running Cisco Prime Network gateway (v3.9.0) =-.
```

You must be logged in as `network user` to use this command. (*network user* is the operating system account for the Prime Network application, created when Prime Network is installed; an example of `network user` is `network39`.) In the following example, the user has created AVM 751 and AVM 851.

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

```
.-= Welcome to sjcn-sysm, running Cisco Prime Network gateway (v3.9.0) =-.
```

```
+ Checking for services integrity:
  - Checking if host's time server is up and running                  [OK]
  - Checking if webserver daemon is up and running                   [OK]
  - Checking if secured connectivity daemon is up and running        [OK]
  - Checking if license server is up and running                     [OK]
  - Checking Prime Network Web Server Status                         [UP]
+ Detected AVM99 is up, checking AVMs
  - Checking for AVM19's status                                     [DISABLED]
  - Checking for AVM76's status                                     [OK 0/129]
  - Checking for AVM66's status                                     [OK 6/232]
  - Checking for AVM11's status                                     [OK 0/987]
  - Checking for AVM851's status                                    [OK 29/10618]
  - Checking for AVM83's status                                     [OK 0/108]
  - Checking for AVM751's status                                    [OK 0/16410]
  - Checking for AVM55's status                                     [DISABLED]
  - Checking for AVM100's status                                    [OK 0/69]
```
Chapter 2  Basic Gateway Server Administration Tasks

Creating a GUI Client Banner Message

Prime Network Administration enables you to define a Message of the Day, or banner, that is displayed when a user logs into any client application. The user must accept the message before logging in. If the user does not accept the message, the user cannot log in. The message supports HTML format. Figure 2-2 provides an example.

Figure 2-2  Message of the Day Example

The message can be changed as required. However, only one message is applied at a time.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

networkctl could display any of the following status indicators:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Service or AVM is up and running.</td>
</tr>
<tr>
<td>DOWN</td>
<td>Service or AVM is down.</td>
</tr>
<tr>
<td>LOADED</td>
<td>Service is down, but the system is trying to start (load) it.</td>
</tr>
<tr>
<td>EVAL</td>
<td>License service is running with an evaluation license.</td>
</tr>
<tr>
<td>DISABLED</td>
<td>AVM has been stopped.</td>
</tr>
</tbody>
</table>

- Checking for AVM0's status [OK 0/178]
- Checking for AVM25's status [OK 0/488]
- Checking for AVM35's status [OK 0/118]
- Checking for AVM82's status [DISABLED]
- Checking for AVM78's status [OK 0/111]
- Checking for AVM84's status [OK 0/72]
Creating a GUI Client Banner Message

Adding or Changing a Message

To add or change a message of the day:

---

**Step 1** Choose **Global Settings > Message of the Day**. The Title and Message fields appear in the content area.

**Step 2** In the Title field, enter a title for the message.

**Step 3** In the Message field, enter the text that is to appear when users log in.

**Note** Abort and Continue buttons are displayed in the message dialog box by default, so the message must be related to these actions. For example, “Do you accept the terms of use in the Product License Agreement? Click **Continue** to proceed or click **Abort** to cancel.”

**Step 4** Click **Save**. A confirmation message is displayed.

**Step 5** Click **OK**. The message is displayed when a user logs into any client application.

---

Removing a Message

To remove a message of the day:

---

**Step 1** Choose **Global Settings > Message of the Day**.

**Step 2** Delete the text in the Message field.

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

**Step 4** Click **OK**. The message no longer appears when a user logs into a client application.

---

For information about the main menu that is displayed in the Prime Network window, see **Message of the Day Window, page 1-22**.
Basic Unit Server Administration Tasks

These topics describe the basic administration tasks for Prime Network units:

- Overview of Prime Network Units, page 3-1
- Viewing Unit Properties, page 3-2
- Starting or Restarting a Unit and Checking AVM Status (networkctl), page 3-4
- Connecting and Disconnecting a Prime Network Unit, page 3-4
- Deleting a Prime Network Unit, page 3-5

See these topics for additional unit administration tasks:

- Advanced Administration for the Prime Network Gateway and Units, page 9-1
- Unit Server High Availability and AVM Protection, page 16-1

Overview of Prime Network Units

The interconnected fabric of units comprises the lowest level of the Prime Network architecture. Each unit manages a group of network elements. Units host the autonomous VNEs. This creates a fabric of interconnected VNEs which can intercommunicate with other VNEs (regardless of which unit they are running on).

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. The switchover to the redundant standby unit does not result in any loss of information in the system because all information is autodiscovered from the network, and no persistent storage synchronization is required. Units can only be designated as standby during the installation process.

For more information on unit server high availability, see Unit Server High Availability and AVM Protection, page 16-1.

Note

The Prime Network system is usually configured with the unit server high availability mechanism enabled.
Viewing Unit Properties

When you right-click a unit and select **Properties**, Prime Network displays the unit properties, as shown in **Figure 3-1**. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

**Figure 3-1  Viewing the Properties All Unit Servers**

![Figure 3-1 Viewing the Properties All Unit Servers](image)

**Table 3-1  Unit Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the unit server.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the unit server. Units behind firewalls or NAT devices will have an IP address of <strong>0.0.0.</strong>. This is an artificial IP address used by the gateway server.</td>
</tr>
</tbody>
</table>
### Table 3-1 Unit Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the unit: Up, Down, Unreachable, Disconnected.</td>
</tr>
<tr>
<td>Up</td>
<td>The unit process is reachable, was loaded, and has started.</td>
</tr>
<tr>
<td>Down</td>
<td>The unit is reachable, but was stopped. This is the status when a <code>networkctl stop</code> command is issued. The unit is both operationally and administratively down.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>The unit cannot be reached by the gateway, so it cannot be managed.</td>
</tr>
<tr>
<td>Disconnected</td>
<td>The unit was disconnected from the gateway (normally a temporary measure to address a problem).</td>
</tr>
<tr>
<td>Up Since</td>
<td>The date and time that the unit was last started.</td>
</tr>
<tr>
<td>Physical Memory Available</td>
<td>The total physical memory on the unit (both free and in use).</td>
</tr>
<tr>
<td>Total Memory Assigned All AVMs</td>
<td>The total physical memory <em>apportioned to all AVMs</em> (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 How Prime Network Allocates Memory to AVMs, page 4-2).</td>
</tr>
<tr>
<td>Total Memory Assigned Up AVMs</td>
<td>The total physical memory <em>apportioned to Up AVMs</em> (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 How Prime Network Allocates Memory to AVMs, page 4-2).</td>
</tr>
<tr>
<td>Allocated Memory Up AVMs</td>
<td>The total physical memory being used by Up AVMs (both user-created and reserved AVMs).</td>
</tr>
<tr>
<td>Protection Group</td>
<td>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.</td>
</tr>
<tr>
<td>AVM HA</td>
<td>Indicates whether AVM protection is enabled (true) on the unit. AVM protection monitors the AVM processes and restarts them in case of failure. This should always be enabled.</td>
</tr>
</tbody>
</table>

When you select a specific unit in the navigation tree, the GUI client displays all of the AVMs in the unit including whether the AVM memory consumption is normal. That display is described in Viewing AVM Properties, page 4-6.

**Note** How to add a unit is described in the *Cisco Prime Network 3.9 Installation Guide.*
Starting or Restarting a Unit and Checking AVM Status (networkctl)

You can use the `networkctl` command to check the status of all unit processes (including AVMs you created). Restarting a unit stops all AVM and VNE processes on that unit and restarts them. Given that the system saves part of its information within the process memory, restarting a unit causes some of the information to disappear. Therefore, it takes as long as the longest full polling cycle for the system to recover all information that was stored in the process memory prior to the restart. Data that was saved in persistent storage before restarting is available immediately.

Keep these items in mind when restarting a unit:

- Restarting a machine can cause some of the VNEs running on the machine to be reported as unreachable. This is due to handshake protocols with the unit that fail due to the unavailability of the VNEs.
- Restarting a machine stops all active queries, flows, and transactions that are currently being run within the VNEs that run on the restarted Prime Network unit.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To start or restart a unit:

1. Log into the unit server as `network user` (where `network user` is the operating system account for the Prime Network application, created when Prime Network is installed; an example of `network user` is `network39`).
2. Change to the Main directory:
   ```bash
   # cd $ANAHOME/Main
   ```
3. Enter the following, substituting `start` or `restart` for option:
   ```bash
   # 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 Reducing AVM Loads and Checking AVM Status, page 4-11.

Connecting and Disconnecting a Prime Network Unit

Disconnecting a unit allows you to temporarily stop unit-gateway communication. This provides a temporary state during which you can fix the unit problem without having to completely reconfigure the unit when you are done. For example, if a unit’s Ethernet card went down and the unit became 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.

If you disconnect a unit that is part of a protection group, this will not trigger starting the standby unit; the high availability will be temporarily disabled on the active unit that is being disconnected. You cannot disconnect a 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.

Before You Begin

If the Event Collector (AVM 100) was enabled on the unit, you must enable an Event Collector on another unit. Otherwise the system will drop events.

1. Configure devices to forward events to the new Event Collector.
2. Enable AVM 100 on another unit, as described in Enabling a New Event Collector on a Unit, page 14-12.

To disconnect or reconnect a unit:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Prime Network Administration window, select All Servers.</td>
</tr>
<tr>
<td>2</td>
<td>Right-click the unit and choose Disconnect. (To connect, choose Connect.)</td>
</tr>
<tr>
<td>3</td>
<td>If the unit is running, a warning will be displayed that says</td>
</tr>
<tr>
<td>4</td>
<td>Confirm your choice. You can now delete the unit as described in Deleting a Prime Network Unit, page 3-5.</td>
</tr>
</tbody>
</table>

Deleting a Prime Network Unit

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

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

Before You Begin

Delete all the VNEs and unreserved AVMs before deleting a unit; see Moving and Deleting AVMs, page 4-13. The reserved AVMs cannot be deleted.

Use this procedure to remove a unit:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Prime Network Administration window, select All Servers.</td>
</tr>
<tr>
<td>2</td>
<td>Right-click the unit that you want to remove, then choose Delete. A warning message is displayed.</td>
</tr>
<tr>
<td>3</td>
<td>Click Yes to proceed or No to cancel the operation. A confirmation message is displayed.</td>
</tr>
<tr>
<td>4</td>
<td>Click OK. The unit is deleted and is no longer displayed in the navigation pane and content area.</td>
</tr>
</tbody>
</table>
These topics describe the basic management tasks that you can perform on Prime Network AVMs and VNEs:

- Overview of AVMs, page 4-2
- Understanding AVM Status, page 4-5
- Viewing AVM Properties, page 4-6
- Adding AVMs, page 4-8
- Reducing AVM Loads and Checking AVM Status, page 4-11
- Changing AVM Status (Start or Stop), page 4-12
- Moving and Deleting AVMs, page 4-13
- Viewing VNE Status, page 4-14
- Moving VNEs to a Different AVM, page 4-16
- Deleting a VNE, page 4-16

See these topics for information on advanced AVM and VNE administration:

- VNE Administration: VNE Lifecycle and Creating VNEs, page 19-1
- Troubleshooting VNE Modeling, page 20-1
- VNE Updates, page 21-1
- Unit Server High Availability and AVM Protection, page 16-1
Overview of AVMs

These topics provide a general introduction to AVMs and how to administer them:

- What Are AVMs?, page 4-2
- How Prime Network Allocates Memory to AVMs, page 4-2
- Reserved AVMs, page 4-3
- Automatic AVM Management: Auto-Add and Memory Load Balancing, page 4-4

What Are AVMs?

AVMs are Java processes that have dedicated memory. AVMs provide the necessary support for executing and monitoring multiple VNEs in a distributed manner. These AVMs are further distributed among the unit servers in the system.

Some AVMs are reserved, which means they are used by the system; other AVMs are user-created, which means they are used to host VNEs. Prime Network contains a watchdog protocol process that monitors the AVMs, and restarts them if they have stopped. This is called AVM protection. For information on how this protocol works, see Managing the Watchdog Protocol (AVM Protection), page 16-10.

Every AVM has its own log in NETWORKHOME/Main/logs.

When you add an AVM, use a number (AVM-ID) that is unique to the unit and between 101-999. 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 3.9 Installation Guide.)

How Prime Network Allocates Memory to AVMs

The amount of memory that is assigned to AVMs depends on whether you use auto-add or create them manually. Regardless of the method you use, 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 4-1 illustrates the defaults for auto-added and manually created AVMs.

<table>
<thead>
<tr>
<th>Method</th>
<th>Memory Assigned to AVM (Default)</th>
<th>Total Physical Memory Assigned to AVM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-add AVMs</td>
<td>1500 MB</td>
<td>2025 MB</td>
</tr>
<tr>
<td>Manually add AVMs</td>
<td>256 M</td>
<td>345 MB</td>
</tr>
</tbody>
</table>

You can adjust the default memory that is assigned to AVMs as follows:

- For auto-added AVMs, by changing the setting in Global Settings > Automatic AVM Management.
- For manually added AVMs when you create the AVM (by editing the Allocated Memory field).
Aggregated totals for all AVMs is provided at the unit level; see Viewing Unit Properties, page 3-2.

**Reserved AVMs**

Reserved AVMs are created by Prime Network and cannot be edited or deleted. Some reserved AVMs are only installed on the gateway; others are installed on both the gateway and units.

Table 4-2 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 4-2 Reserved AVMs**

<table>
<thead>
<tr>
<th>AVM #</th>
<th>Purpose</th>
<th>Is installed on...</th>
<th>Can be checked using...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>GW</td>
<td>Unit</td>
</tr>
<tr>
<td>AVM 0</td>
<td>High Availability/Switch AVM—Enables communication between the unit and other units, as well as the gateway. See Unit Server High Availability and AVM Protection, page 16-1.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AVM 11</td>
<td>Gateway AVM—Manages the gateway server and other processes running on it. See Basic Gateway Server Administration Tasks, page 2-1.</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>AVM 25</td>
<td>Fault Agent AVM—Processes event information (in each unit), including updates and new correlation information, and generates new tickets when required. See Managing the Event Collector (AVM 100), page 14-1.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AVM 35</td>
<td>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.)</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>AVM 66</td>
<td>Workflow engine AVM—Defines rules and dependencies to activate business and network processes. See Workflow Administration Tasks, page 12-1.</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>AVM 76</td>
<td>Job scheduler AVM/.</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>AVM 77</td>
<td>Reserved for use by Prime Network Change and Configuration Management (when installed).</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>AVM 78</td>
<td>VNE topology AVM—Distributes topology information among VNEs.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AVM 83</td>
<td>TFTP Server—Reserved for use by Prime Network Change and Configuration Management (when installed) if using TFTP.</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>AVM 84</td>
<td>Reports AVM—Manages the reporting framework.</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>AVM 99</td>
<td>Management AVM—Manages the unit and the other AVMs running on the unit (or gateway, if there are no separate units). See Basic Unit Server Administration Tasks, page 3-1.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AVM 100</td>
<td>Event Collector AVM—Listens for and receives traps and syslog notifications from devices, and forwards them to corresponding VNEs. See Managing the Event Collector (AVM 100), page 14-1.</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Overview of AVMs

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 can 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 4-1.

Figure 4-1  AVM Auto-Add

In addition, 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. Prime Network signals when an AVM exceeds its memory capacity by changing the AVM icon to red. (You can also check the memory consumption of all AVMs in a unit by selecting the unit in the GUI client.) 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 confirm or reject the move. (The Reduce Load option is only made available to AVMs when they contain at least one VNE.)

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.

1. You can also check AVM status using the system health and diagnostics tool; see Obtaining Diagnostic Information Using Graphs, page 9-6.
Understanding AVM Status

AVM status describes the condition of the AVM process on the unit or gateway. AVM status is determined by a combination of the AVM’s administrative and operational modes:

- **AVM administrative mode** indicates whether or not Prime Network should recognize or ignore administration instructions sent to the AVM. This mode is entirely user-directed. You can control this mode from the All Servers branch. See Changing AVM Status (Start or Stop), page 4-12.

- **AVM operational mode** describes the health and condition of the AVM process on the gateway (for example, whether the gateway can reach the AVM).

The AVM Admin and Oper modes are not displayed in Prime Network Administration; they are implicit in the overall status. Only the overall AVM status is displayed in the GUI.

Table 4-3 describes how the combination of AVM administrative and operational modes determine the overall AVM status.

<table>
<thead>
<tr>
<th>AVM Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Up</td>
<td>When a <strong>Start</strong> (command) option is issued.</td>
</tr>
<tr>
<td>Up</td>
<td>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.</td>
</tr>
<tr>
<td>Shutting Down</td>
<td>When a <strong>Stop</strong> (command) option is issued and, while the command is being run, some processes are still running, the status of the AVM is Shutting Down.</td>
</tr>
<tr>
<td>Down</td>
<td>The AVM process is reachable, but was stopped. This is the status when a <strong>Stop</strong> (command) is issued. The AVM is both operationally and administratively down.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>The AVM process cannot be reached by the gateway, so the AVM cannot be managed.</td>
</tr>
<tr>
<td>Disconnected</td>
<td>The AVM is on a unit that was disconnected from the gateway (the unit has a Disconnected status).</td>
</tr>
</tbody>
</table>

When moving an AVM, its status has a bearing on whether the process is automatically reloaded. If its status is Up, it is reloaded; if its status is down, it is not reloaded. For more information about moving AVMs, see Moving and Deleting AVMs, page 4-13.

Viewing AVM Properties, page 4-6, shows how you can check the status of AVMs. You can also get AVM diagnostic information using the system health and diagnostics tool; see Obtaining Diagnostic Information Using Graphs, page 9-6.
CHAPTER 4  BASIC AVM AND VNE ADMINISTRATION TASKS

VIEWING AVM PROPERTIES

When you select a gateway server or unit in the navigation tree, Prime Network displays all of its member AVMs. This includes system AVMs and user-created AVMs. For example, in Figure 4-3, the gateway server has ten system and user-created AVMs.

**Figure 4-2**  Listing all AVMs in a Unit or Server

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 4-3, the entire system has 10 user-created AVMs.

**Figure 4-3**  Listing all User-Created AVMs in Prime Network
The fields in the AVM table are described in Table 4-4. To see which fields are editable, right-click an AVM and select properties (refer to Table 4-5).

Table 4-4  AVM Properties in AVMs List

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>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.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the unit: Up, Down, Unreachable, Disconnected. To find out how long the AVM has been Up, check the AVMs table, which is displayed when you select the parent unit or gateway server.</td>
</tr>
<tr>
<td></td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Unreachable</td>
</tr>
<tr>
<td></td>
<td>Disconnected</td>
</tr>
<tr>
<td>Unit IP</td>
<td>IP address of the parent unit server. Units behind firewalls or NAT devices will have an IP address of <code>0.0.0.#</code>. This is an artificial IP address used by the gateway server.</td>
</tr>
<tr>
<td>Allocated Memory</td>
<td>The total physical memory being used by the AVM. This field is editable but changing it requires an AVM restart to apply the change.</td>
</tr>
<tr>
<td>Total Memory</td>
<td>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.)</td>
</tr>
<tr>
<td>Assigned</td>
<td>Key</td>
</tr>
<tr>
<td>Memory Consumption</td>
<td>Indicates whether the AVM has surpassed its warning memory consumption warning threshold. Supported values are:</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Normal</td>
</tr>
<tr>
<td></td>
<td>High</td>
</tr>
</tbody>
</table>

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

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 the GUI client. Prime Network can choose the most appropriate unit for you, or you can specify the one you want to use. Alternatively, you can use the manual procedure, which is described in Adding AVMs Manually, page 4-9.

Adding AVMs Using Auto-Add

Use this procedure to configure the default settings for all auto-added AVMs, and then create a group of auto-added AVMs on a unit. If you need deployment information and recommendations, such as AVM memory requirements, contact your Cisco account representative.

Before You Begin
Make sure AVM 0 and AVM 99 are running on the unit.

**Step 1** Configure the default values for all auto-added AVMs.

**Note** These settings are only applied to auto-added AVMs. They are not applied to AVMs that are configured manually.

- Select Global Settings > Automatic AVM Management.

---

Table 4-5  AVM Properties Shown When You Right-Click an AVM

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit Data</td>
<td>IP Address The IP address of the parent unit.</td>
</tr>
<tr>
<td></td>
<td>Available Memory The amount of memory that is currently available on the parent unit (note time stamp).</td>
</tr>
<tr>
<td></td>
<td>Allocated Memory The amount of memory that is being used by the AVM.</td>
</tr>
<tr>
<td></td>
<td>Enable AVM Protection If the check box is checked, AVM protection (the watchdog protocol) is enabled. For more information, see Managing the Watchdog Protocol (AVM Protection), page 16-10.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>This field is editable.</td>
</tr>
</tbody>
</table>
b. In the AVM Sizing field, configure the following.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default AVM Size</td>
<td>The memory size to be used for auto-added AVMs. The default is 1500 MB.</td>
</tr>
<tr>
<td>Unit Reserved Memory</td>
<td>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%.</td>
</tr>
</tbody>
</table>

c. Click **Apply**.

**Step 2**
Right-click the desired unit and choose **Auto Add AVMs**. Prime Network will automatically add eight AVMs to the unit and start the AVMs. Figure 4-4 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 4-4 Unit Listing Auto-Added AVMs

You can edit the key, allocated memory, or AVM protection setting by right-clicking the AVM, choosing **Properties**, and making your changes. The changes will require an AVM restart to take effect.

---

Adding AVMs Manually

To manually create an AVM:

**Step 1** Expand the All Servers branch and select the required entity.

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>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_*** + 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 3.9 Installation Guide.)</td>
</tr>
<tr>
<td>Key</td>
<td>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 AVMID_***, where *** is an designator assigned by Prime Network for tracking purposes.</td>
</tr>
<tr>
<td>Allocated Memory</td>
<td>The maximum memory that can be used by the AVM, in megabytes. The default is 256. If you need deployment information and recommendations, such as AVM memory requirements, contact your Cisco account representative. <strong>Note</strong> When you create an AVM manually rather than using auto-add, the default AVM size is <em>not</em> determined by the setting specified in Global Settings &gt; Automatic AVM Management. That setting is only applied to auto-added AVMs.</td>
</tr>
<tr>
<td>Activate on Creation</td>
<td>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 unchecked, and the newly created AVM has an administrative status of Down.</td>
</tr>
<tr>
<td>Enable AVM Protection</td>
<td>By default this check box is checked, enabling the watchdog protocol on the AVM. For more information, see Managing the Watchdog Protocol (AVM Protection), page 16-10. <strong>Note</strong> It is highly recommended that you do not disable this option. If you change the option when the AVM is up, you must disable and re-enable the AVM for the change to take effect.</td>
</tr>
</tbody>
</table>

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

Creating a new AVM results in Prime Network providing the registry information of the new AVM in the specified unit. The AVM can now host VNEs.
Reducing AVM Loads and Checking AVM Status

The automatic AVM monitoring (load balancing) function signals you when AVMs are reaching their memory capacity so that you can move VNEs to different AVMs and ensure system stability. The AVM memory capacity threshold is controlled from the Automatic AVM Management window in Global Settings. It affects user-created AVMs across the system.

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 4-5.

![AVM Memory Consumption Indicator in Units Windows](image)

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 (if the AVM is up and contains at least one VNE).

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Triggers the load balancing mechanism for the selected user-created AVM.</td>
</tr>
</tbody>
</table>

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, you should consider manually moving VNEs or adding new AVMs.
To configure the memory threshold for all user-created AVMs in the system (the point at which Prime Network flag a problem as shown in Figure 4-5, 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 4-5 on page 4-11.

*Note* This setting controls the load balancing function for all user-created AVMs in the system.

If you want more diagnostic information, Prime Network provides a web-based diagnostics tool that provides information about AVMs, such as Java heap, dropped messages, CPU usage, and so forth. This data is provided in the form of graphs so you can quickly identify problems.

**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. (The web-based tool uses the username admin; the password is configured by the network-conf script during installation.)

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

**Step 3** Click the hyperlink for the gateway or unit that contains the AVMs in which you are interested. (The gateway is always 127.0.0.1; units are represented by their IP address.) This launches a display of information for each AVM on the gateway or unit.

- The first row displays *aggregated AVM information for the unit*. The rows that follow displays information about *one AVM* (units listed before the gateway).
- Each *column* displays *one graph type*.

For information on the graph types and how to interpret them, see *Obtaining Diagnostic Information Using Graphs*, page 9-6.

### Changing AVM Status (Start or Stop)

You can use the Prime Network Administration GUI to start or stop an AVM.

- **Start**—The AVM will move through a status of Starting Up to Up. When the AVM is Up, its process is running and it is reachable.

- **Stop**—The AVM will move through a status of Shutting Down to Down. This also stops all the VNEs in the AVM. Any 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 *Reducing AVM Loads and Checking AVM Status*, page 4-11.
Chapter 4  Basic AVM and VNE Administration Tasks

Moving and Deleting AVMs

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.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To start or stop an AVM:

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

**Step 2**
Start or stop the AVM in one of the following ways:

- Right-click the AVM, then choose Actions > **Start** or Actions > **Stop**.
- In the toolbar, click **Start** or **Stop**.

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

**Note**
When the AVM status is displayed as Down, the status remains Down and no reload occurs.

Moving and Deleting AVMs

You can *move* an AVM from one unit to another unit. You can also move groups of AVMs to the same unit in one operation. AVMs 0-100 are reserved and cannot be moved.

**Note**
If an AVM's parent unit is down, you must disconnect the unit before moving the AVMs. See Connecting and Disconnecting a Prime Network Unit, page 3-4.

After the move is completed, the AVM 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 its 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 Persistency Overview, page 26-1.

When you *delete* a running AVM, the AVM is stopped before being removed. This procedure deletes the AVM registry information in the specified unit. If any VNEs are running on the AVM, an error message is displayed, and you cannot delete the AVM. For more information, see Deleting a VNE, page 4-16. You cannot delete reserved AVMs (see Overview of AVMs, page 4-2).

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.
Moving an AVM

To move an AVM:

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

The Move To dialog box appears, displaying a tree-and-branch representation of the selected Prime Network server and its units, excluding the unit in which the AVM is currently located. The highest level of the navigation tree displays the Prime Network server. The branches can be expanded and collapsed to display and hide information.

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 Moving VNEs to a Different AVM, page 4-16.

Moving an AVM

Use the following procedure to delete an AVM.

Before You Begin
Remove all VNEs from the AVM, or the deletion will fail. See Deleting a VNE, page 4-16.

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.

Viewing VNE Status

VNE status indicates the administrative condition of the VNE: Starting Up, Up, Shutting Down, Down. If the gateway server cannot communicate with the VNE, the VNE status will be Unreachable.
(Remember that this is the status of the entity that models the device, not the device itself. The device may still be processing network traffic; it is just not connecting to Prime Network.) This information is displayed in Prime Network Administration when you select an AVM (see Figure 4-6).
Starting and stopping VNEs is entirely user-directed, as explained in Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-44. Table 4-6 lists the possible VNE status values that you may see in a table of VNEs.

Table 4-6  VNE Status

<table>
<thead>
<tr>
<th>VNE Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Up</td>
<td>A <strong>Start</strong> (command) option was issued.</td>
</tr>
<tr>
<td>Up</td>
<td>The VNE process is reachable, was loaded, and has started. This is the status when a <strong>Start</strong> command is issued (or when you create a VNE and choose <strong>Start</strong> as its initial status), and no problems are encountered (such as an overloaded server).</td>
</tr>
<tr>
<td>Shutting Down</td>
<td>A <strong>Stop</strong> (command) option was issued and, while the command is being run, some processes are still running, the status of the VNE is Shutting Down.</td>
</tr>
</tbody>
</table>
| 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 was moved.  
                         - The AVM was restarted or moved.  
                         - The unit was disconnected or was switched to a standby server.  
                         - 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 Adding VNEs, page 19-11.) |
| Disconnected   | The VNE is on a unit that was disconnected from the gateway (the unit has a Disconnected status). |
Moving VNEs to a Different AVM

When you move a VNE to a different AVM, the moved VNE are unloaded. The status of the VNEs is maintained after they are reloaded, except for VNEs that were in maintenance mode; those VNEs will be moved to Down (and the Maintenance indicator in the AVMs window will display false). You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

Note When you move a VNE to another AVM, the VNE alarm persistency information is saved. Persistency information is data that is stored for later use. For information on the VNE persistency mechanism, see Persistency Overview, page 26-1.

To move one or more VNEs:

1. Expand the All Servers branch, and select the required AVM in the navigation tree. The VNEs are displayed in the content area.
2. Select one or more VNEs using the mouse or keyboard, then right-click one of the selected VNEs.
3. Choose Move VNEs from the shortcut menu. The Move To dialog box is displayed.
   The Move To dialog box displays a tree-and-branch representation of the selected Prime Network server, its units, and AVMs, excluding the AVM in which the VNE is currently located. The highest level of the navigation tree displays the Prime Network server. The branches can be expanded and collapsed to display and hide information.
4. In the Move To dialog box, browse to and select the AVM where you want to move the VNEs.
5. Click OK. The VNE is moved to its new location, and now appears beneath the selected AVM in the VNEs Properties table.

Note You can verify that the VNE has been moved by selecting the appropriate AVM in the navigation tree and viewing the moved VNE in the VNEs Properties table.

Note The VNE that is moved is automatically unloaded and reloaded if its status was Up before the move (because its status is maintained).

Deleting a VNE

When you delete a running VNE from a unit and AVM, the VNE is stopped and all VNE references are deleted from the system and Golden Source. This includes the registry information of the VNE in the specified unit. A VNE that has been removed no longer appears in any future system reports.

Note VNE information is deleted only if the VNE is Up when you perform the delete operation. If after deleting a VNE you are still seeing tickets and alarms related to the VNE, you should remove the VNE information manually, as described in the procedure that follows.
When you delete a VNE, you also delete all Layer 3 VPN site and virtual router business element data associated with the VNE. You can delete business elements separately by using Prime Network Vision. For more information about deleting business elements using Prime Network Vision, see the *Cisco Prime Network 3.9 User Guide*. Since all VNE information is deleted, adding the VNE again requires you to reenter all VNE information.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

Note

A VNE that has static links configured cannot be deleted without first removing all static links configured for the VNE. Dynamic links are automatically removed.

To delete a VNE:

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

Step 2
Right-click the required VNE in the VNEs Properties table, then choose Delete. A confirmation prompt is displayed.

Step 3
Click Yes to delete the VNE or No to retain the VNE. If you click Yes, a dialog box appears, asking if you want to delete all Layer 3 VPN business element data for the VNE from Prime Network.

Step 4
Do one of the following:

- Click Yes to remove all Layer 3 VPN site and virtual router business element data from Prime Network. This option removes all VPN business elements associated with the selected VNE from Prime Network. Prime Network updates the VPN topology views in Prime Network Vision accordingly by removing the deleted business elements.

- Click No to retain the Layer 3 VPN site and virtual router business element data in Prime Network. This option retains the VPN business element associated with the selected VNE in Prime Network. Prime Network updates the VPN topology views in Prime Network Vision; the orphaned business elements are identified by a white X on a red background ( ). To remove these orphaned business elements, delete them manually in Prime Network Vision.

- Click Cancel to exit the procedure without deleting the VNE and its Layer 3 VPN site and virtual router business element data.

Step 5
If the VNE was not running when you deleted it from Prime Network, manually delete any remaining VNE data. Otherwise Prime Network may generate tickets and alarms related to that VNE, and they will never clear.

Remove the following files, where avm-id is the AVM hosting the VNE, and vne-ip is the IP address of the VNE that was removed. (Note that you should remove all files and directories in the instrumentor-persistency directory.)

```
$ANAHOME/unit/avm-id/persistency/alarm/vne-ip.per
$ANAHOME/unit/avm-id/persistency/event/vne-ip.per
$ANAHOME/unit/avm-id/instrumentor-persistency/vne-ip/*
```
Licensing

The following topics describe the Prime Network licensing mechanism and how to view a basic license report:

- Licensing Overview, page 5-1
- Licensing for Upgrades from Cisco ANA 3.6.x and 3.7.x, page 5-2
- Licensing and Gateway Server High Availability, page 5-2
- Obtaining a License File, page 5-3
- Installing and Updating a License File, page 5-4
- Viewing the License Report, page 5-5
- Troubleshooting Licensing Issues, page 5-5

Note

A Prime Network base license must be registered and activated within 120 days of installation or upgrade. If there are no valid license files on the gateway server, Prime Network acts as an evaluation version. This means that it has full functionality for 120 days after installation, and then it expires and UI connections will be disallowed.

Licensing Overview

Prime Network provides a mechanism for managing, validating, and enforcing basic licenses. Licenses are encrypted files that are stored on the gateway server. The gateway server keeps track of the licenses by communicating with the FlexNet license validation server, which is provided with the Prime Network image.

All purchased Prime Network basic licenses must be registered and activated by installing the license file on the Prime Network server.

If a user logs into a GUI client and Prime Network detects a license violation, a warning message is displayed, as illustrated in Figure 5-1.
Licensing for Upgrades from Cisco ANA 3.6.x and 3.7.x

If you are upgrading from Cisco ANA 3.6.x or Cisco ANA 3.7.x, keep the following in mind:

- Upgrade from Cisco ANA 3.7.x: If you are upgrading from a registered version of Cisco ANA 3.7, no new license files are required. To check whether you have a valid license file installed on the Prime Network gateway server, see Viewing the License Report, page 5-5.
- Upgrade from Cisco ANA 3.6.x: A new license file is required because there is no automatic transfer of licenses from Cisco ANA 3.6.x. Contact your Cisco account representative or send an e-mail to ask-ana-licensing@cisco.com to get a new license file, and install it on the Prime Network 3.7 gateway server within 120 days of the upgrade.

Licensing and Gateway Server High Availability

If you using gateway server high availability, you must do the following:

1. Purchase two base kit licenses.
2. Contact your Cisco account manager and ask them to manually generate the licenses for the additional gateway server(s). (Because users receive only one Product Activation Key (PAK), they can only generate one license file.)
3. Place a copy of all gateway server license files in the license directory NETWORKHOME/Main/ha/licenses on an active gateway. This directory is part of the Prime Network partition that is shared (local redundancy) or replicated (geographical redundancy) between servers in the gateway server high availability solution.
If you add new licenses, you must copy them to this directory on the active gateway. After installing new license files, the license server should be restarted using the resetLicenses.pl script (see Installing and Updating a License File, page 5-4).

**Note**
All gateway licenses should be copied to \texttt{NETWORKHOME/Main/ha/licenses} on the active gateway.

## Obtaining a License File

Prime Network software must be registered via Cisco.com in order to obtain a license file (*.lic). The license file will be sent to you by e-mail and must be installed on the Prime Network gateway server. See Installing and Updating a License File, page 5-4.

A Product Authorization Key (PAK number) is used for identification purposes when you register the software to request a license file. The PAK number is an automatically generated identification key that represents the specific software and hardware covered by the license. You will find the PAK number at the bottom of the Software License Claim Certificate supplied with the Prime Network package. An example PAK number is ANA-3X-JAB-XXXXXX. Each PAK number is unique and can be registered only once.

**Note**
If you cannot find the PAK number, contact your Cisco account representative or send an e-mail to ask-ana-licensing@cisco.com for assistance.

To obtain the license file:

### Step 1
Go to the licensing web page at \texttt{http://www.cisco.com/go/license} and enter your Cisco.com user credentials to enter the Product License Registration process. If you are not a registered Cisco.com user, create an account and log in.

### Step 2
Enter the PAK number that appears in the Software License Claim Certificate you received with your Prime Network package and click \texttt{Submit}.

### Step 3
Enter the hostname and host ID of the Prime Network gateway server.

**Note**
- If you do not know the host ID, log into the Prime Network gateway server and enter the command \texttt{hostid}.
- For linux, the license file should be generated with both hostname and MAC address.

### Step 4
Fill in the rest of the requested information, including your e-mail address, and submit the request.

Your license file and user information will be sent within 1 hour to the e-mail address you specified. If you do not receive an e-mail within 1 hour, contact your Cisco account representative or send an e-mail to ask-ana-licensing@cisco.com for assistance.

**Caution**
Do not edit the contents of the .lic file in any way. The contents of the file are signed and must remain intact.
Installing and Updating a License File

When you receive the license file, install it as described in Installing and Updating a License File, page 5-4.

### Installing and Updating a License File

When you receive the license file (*.lic) after registering the software, you must install it on the Prime Network gateway server within 120 days after installation. The license file is held and managed by the FlexNet license validation server, which is provided with the Prime Network image.

You can also use this procedure to update an existing license, or install additional licenses.

When Prime Network is installed, the FLEXNET_HOME environment variable is set to NETWORKHOME/utils/operating-system/FlexNet. Table 5-1 lists the contents used by the licensing framework.

---

**Note**

If you are using gateway server high availability, be sure to install new licenses in the correct directory as listed in Table 5-1. If you do not copy licenses into the correct directory, the license server will not start.

---

<table>
<thead>
<tr>
<th>Directory Contents</th>
<th>Directory Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlexNet binaries and Cisco daemon</td>
<td>$FLEXNET_HOME/bin</td>
</tr>
<tr>
<td>FlexNet and liccontrol logs</td>
<td>$FLEXNET_HOME/logs</td>
</tr>
<tr>
<td>License file storage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For gateways in a gateway server high availability environment</td>
</tr>
<tr>
<td></td>
<td>All other configurations</td>
</tr>
</tbody>
</table>

Use the following procedure to install and update license files. These procedures can be performed at any time.

**Step 1**  
Log into the Prime Network gateway as **network user**. (**network user** is the operating system account for the Prime Network application, created when Prime Network is installed; for example, **network39**.)

**Step 2**  
For all licenses:

a. Copy the license file to the $FLEXNET_HOME/licenses directory.

b. Enter the following command to make sure that the file is detected:

```
# liccontrol reread
```

**Step 3**  
If you are using gateway server high availability environment, copy all licenses to an additional location so it can be accessed by all gateways in the environment.
a. Copy all server license files to the NETWORKHOME/Main/ha/licenses directory on the active gateway. This directory is part of the Prime Network partition that is shared (local redundancy) or replicated (geographical redundancy) between servers in the gateway server high availability solution.

b. On the active gateway, enter the following commands to make sure that the files are detected. (You only need to do this once.)

```
# liccontrol stop
# perl $ANAHOME/Main/ha/resetLicenses.pl
# liccontrol start
```

## Viewing the License Report

The License Report window provides basic license information, such as whether the installation is running a Production or Lab license. It is displayed when you choose Global Settings > License Report. The following information is displayed in the License Report window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>License Report generation time</td>
</tr>
<tr>
<td>Basic License</td>
<td>Production, Lab, or Unlicensed Evaluation.</td>
</tr>
<tr>
<td>Operating Mode</td>
<td>Backend designation denoting the type of management Prime Network is performing: ELM (foundation and element management), NAS (network and service monitoring), or ACT (service activation).</td>
</tr>
<tr>
<td>Evaluation Days Remaining</td>
<td>For Unlicensed Evaluation, the number of days remaining (out of 120)</td>
</tr>
</tbody>
</table>

## Troubleshooting Licensing Issues

If you encounter any issues with Prime Network licenses, contact your Cisco account representative or send an e-mail to ask-ana-licensing@cisco.com for assistance.

At any time you can check license compliance by generating a License Report; see Viewing the License Report, page 5-5. You can also check the license log files at $FLEXNET_HOME/logs.

These topics provide additional troubleshooting information:

- License Violation Messages, page 5-6
- Stopping and Starting the License Server, page 5-6
License Violation Messages

To detect licensing issues, you can check for license-related System events in Prime Network Events. Prime Network generates warning events for license violations. The events are logged in the database and are visible from the System tab in Prime Network Events. System events are generated in the following scenarios.

<table>
<thead>
<tr>
<th>License Violation Message</th>
<th>Details/Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>You are using an Prime Network without a license. The evaluation period is expired.</td>
<td>When the evaluation license expires, client connections are disallowed.</td>
</tr>
<tr>
<td>You are using an Prime Network evaluation license which expires in x days</td>
<td></td>
</tr>
<tr>
<td>The installation of Prime Network is compliant only for LAB usage and cannot be used in production network.</td>
<td>Informational message; no action required.</td>
</tr>
</tbody>
</table>

Stopping and Starting the License Server

Whenever you run the `networkctl status` command on the gateway, Prime Network provides information about component processes using the following format:

```
Checking if license server is up and running     [ status ]
```

The status information may be any of the following:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>A license file was found and the license server is up and running.</td>
</tr>
<tr>
<td>LOADED</td>
<td>The license server is starting. If it remains LOADED and does not change to OK, there might be a problem with the license file. Contact your Cisco account representative or send an e-mail to <a href="mailto:ask-ana-licensing@cisco.com">ask-ana-licensing@cisco.com</a>.</td>
</tr>
<tr>
<td>NO LICENSE</td>
<td>No license file exists; the license server is not started.</td>
</tr>
<tr>
<td>ERROR</td>
<td>A problem occurred while starting the license server.</td>
</tr>
</tbody>
</table>

To manage the license server, use the `liccontrol` command (for example, when installing new license files):

```
liccontrol [start | restart | reread ]
```

The `liccontrol reread` detects new licenses; that is, it reads them and activates them. If you run `liccontrol start` and there are no license files installed, the license server will not start.
Configuring Event Notifications

These topics describe the Prime Network Event Notification Service, and how to manage these services:

- What Is the Event Notification Service?, page 6-1
- Viewing and Managing Existing Notification Services, page 6-2
- Configuring an Event Notification Service, page 6-3

For information on how Prime Network respond to incoming raw events from devices, see Managing the Event Collector (AVM 100), page 14-1.

What Is the Event Notification Service?

The Event Notification Service (ENS) is a service that takes events received from devices and system events generated by Prime Network, and forwards them to OSSs. You can create notifications for:

- Network events (syslogs, traps, and service events), including events from unmanaged devices
- Non-network events, such as system, security, and provisioning
- Actionable events (with correlation), and non-actionable (generic) events
- Tickets and ticket updates

Figure 6-1 illustrates how Prime Network responds to incoming event notifications from devices. The complete flow illustrated in this figure is described in Overview of the Event Collector and Event Processing, page 14-1. The Event Notification Service resides in the Fault Manager. Any events sent to the Fault Manager can be forwarded to external OSS applications using the Event Notification Service.

Note

Figure 6-1 illustrates the logical flow of events through Prime Network. The actual network communication is subject to the transport configuration between the gateway server and units.
The ENS can also forward non-actionable events, which are events coming from unmanaged devices and events that the VNE cannot parse. These are also called generic events. These non-actionable events are normalized into the CISCO-EPM-NOTIFICATION-MIB trap format and are forwarded to OSS applications. (To enable event forwarding from unmanaged devices, see the Cisco Prime Network Integration Developer Guide.)

The following topics describe how to create event notifications using the GUI. (You can also create notification using the Prime Network API, as described in the Cisco Prime Network Integration Developer Guide, which is provided on the Prime Network Developer Network.)

**Viewing and Managing Existing Notification Services**

To view existing event notification services, select Event Notifications in Prime Network Administration. You must have Administrator privileges to use this function in Cisco Prime Network Administration. The content area is populated and lists all existing services. The last column lists the total number of notifications that have been sent by each service. See Figure 6-2 for an example.
Configuring an Event Notification Service

This procedure explains how to create a new notification service. You can also use this procedure to edit an existing notification service. You must have Administrator privileges to use this function in Cisco Prime Network Administration. The notification service can be forwarded as a trap or by e-mail.

To create a new event notification service, or edit an existing service:

**Step 1** Right-click Event Notification and select **New Event Notification Service**. (To edit an existing service, right-click or double-click the service in Prime Network Administration, and select **Properties**.)

**Step 2** Configure the main characteristics of the new service in the New Notification Service dialog box and click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User-defined name for the new notification service.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the new notification service.</td>
</tr>
<tr>
<td>Forward Events</td>
<td>Defines how the Prime Network forwards event notifications. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• As Traps</td>
</tr>
<tr>
<td></td>
<td>• By E-mail</td>
</tr>
</tbody>
</table>

Depending on your selection, you must configure the Trap Notifications Settings or E-mail Notifications Settings.
## Configuring an Event Notification Service

### Trap Notification Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IP</td>
<td>IP address of the destination to which Prime Network will forward the received events.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Events will only be forwarded if the Prime Network gateway server can communicate with the destination.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of the destination to which Prime Network will forward the received events. Port 162 is used by default.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Transport protocol, either UDP (default) or TCP. (For configured notifications, if there is a TCP connection issue, a System event is generated.)</td>
</tr>
<tr>
<td>Community String</td>
<td>SNMP community string used for sending the SNMP notifications (public, by default).</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>SNMP version, either SNMPv1 (default) or SNMPv2.</td>
</tr>
</tbody>
</table>

### E-mail Notification Settings

1. The e-mail notifications set here are generated every five seconds. In case of multiple event notification, all of the notifications are forwarded as one e-mail. The Subject field of this e-mail displays the number of notifications within the e-mail.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server</td>
<td>The FQDN or the IP address of the e-mail server.</td>
</tr>
<tr>
<td>From Address</td>
<td>The e-mail address of the sender.</td>
</tr>
<tr>
<td>To Address(es)</td>
<td>The e-mail address of the recipient. You can enter multiple e-mail addresses separated by a comma or a semi-colon.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="mailto:bob@abc.com">bob@abc.com</a>, <a href="mailto:anne@abc.com">anne@abc.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:bob@abc.com">bob@abc.com</a>; <a href="mailto:anne@abc.com">anne@abc.com</a></td>
</tr>
<tr>
<td>Subject</td>
<td>The subject of the e-mail.</td>
</tr>
</tbody>
</table>
Choose the specific events from the Available Items list. The Available Items list displays the available event types. When you choose an event type, its subtypes are displayed in the Included Events list. For example, selecting the service event type **CPU Utilization exceeded upper threshold** includes the event subtype **CPU utilization is less than lower threshold**.

### Step 3

Choose the type and severity of the tickets or events that you want to include in the notifications and click **Next**. For optimal performance, choose only the events in which you are interested.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Network Events         | Forward or notify network events of the selected type (Syslogs, Traps, Service).  
  *Excluding* a network event means you will *not* receive the following:  
  - Any notifications of the event, including its clearing event.  
  - Any notifications of tickets with that event type as its root cause.  
  For more granular choices of the selected network events,  
  1. Check a type of network events check box and click **Select Types**.  
  2. Choose the events to be included. When you choose an event, it includes its clearing event. For example:  
  To include generic syslogs, click **Syslog** and click **Select Types** to select **Generic syslog**, as shown in **Figure 6-3**.  
  | Note | If the **New Tickets** field is selected along with the **Network Events** field, the event of the selected type and the ticket whose root cause is of the selected event type is forwarded. |
| New Tickets            | Notifications are created on new tickets. If the Ticket's severity changes, a notification is sent only if the **Ticket Updates** field is checked  
  | Note | Select the specific severity property if you want only the severity updates. |
| Non-Network Events     | Include Non-Network Events (System, Security, Provisioning) in the notifications if they are of the chosen type.  
  *Excluding* a non-network event means you will *not* receive any notifications of the event, including its clearing event.  
  For more granular choices of the selected non-network events,  
  1. Check a type of non-network events check box and click **Select Types**.  
  2. Choose the non-network events to be included. When you choose an event, it includes its clearing event. For example:  
  To include HA replication failure, click **System** and click **Select Types** to select **HA replication failure**, as shown in **Figure 6-3**.  
| Ticket Updates         | Sends notification only when the selected ticket property change. Click **Select Properties** to select the ticket properties for the notification.  
| Severity               | Include tickets/events in the notifications if they are of the chosen severity.  

Choose the specific events from the Available Items list. The Available Items list displays the available event types. When you choose an event type, its subtypes are displayed in the Included Events list. For example, selecting the service event type **CPU Utilization exceeded upper threshold** includes the event subtype **CPU utilization is less than lower threshold**.
Figure 6-3  Selecting a Generic Syslog Event for an Event Notification Service

When you add an event from the Available Items list, Prime Network automatically includes all of its subtype events (which are listed under Included Events).
Step 4  In the Source Selection dialog box, specify the source of the events to be included or excluded from the event notification service by selecting managed network elements or specifying the IP addresses.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include all Sources</td>
<td>Receive notifications from all the event sources. This option is selected by default.</td>
</tr>
<tr>
<td>Include all managed network elements</td>
<td>Receive notifications from all the managed network elements. This also includes the notification from the new managed elements added after the subscription is created.</td>
</tr>
<tr>
<td>Include specific managed network elements/IP address</td>
<td>Receive notifications from specified managed network elements or IP address. Do the following:</td>
</tr>
<tr>
<td></td>
<td>• To select a specific managed network element from an existing list, select Add &gt; Managed Network Element.</td>
</tr>
<tr>
<td></td>
<td>• To select a specific IP address, select Add &gt; IP Address to enter one or more IP addresses.</td>
</tr>
</tbody>
</table>

Note  Enter multiple IP addresses as a comma-separated list.

Note  Make sure to add these IP addresses to the list of unmanaged devices sending notifications to the Event Collector (AVM 100); see the Cisco Prime Network Integration Developer Guide for instructions on how to do this.

<table>
<thead>
<tr>
<th>Exclude the following managed elements /IP address</th>
<th>Exclude the notifications from the specified managed elements or IP address. Do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• To exclude a specific managed network element from an existing list, select Add &gt; Managed Network Element.</td>
</tr>
<tr>
<td></td>
<td>• To exclude a specific IP address, select Add &gt; IP Address.</td>
</tr>
</tbody>
</table>

Step 5  Click Finish to create the notification service. A status message is displayed and, if successful, the new service will appear in Prime Network Administration.
Managing User Security: Roles and Scopes

These topics describe how Prime Network implements a two-dimensional security engine combining a role-based security mechanism with scopes (groups of network elements) that are granted to users. In addition, it describes managing users in the Prime Network platform, including defining users and passwords.

- Overview of User Authentication and Authorization, page 7-1
- Managing Global Security Settings, page 7-7
- Creating and Managing Scopes, page 7-16
- Managing User Accounts and Controlling User Access, page 7-19
- Deleting a Prime Network User Account, page 7-24
- Changing a User’s Prime Network Password, page 7-24

Overview of User Authentication and Authorization

Note

User authentication by Prime Network is disabled if Prime Network is installed with Cisco Prime Central.

Prime Network uses a combination of methods to manage user authentication and authorization:

- **User authentication** can be managed locally by Prime Network or externally by an LDAP application. Either method can be used to validate user accounts and passwords, thus controlling who can log in to Prime Network. If you use Prime Network, user information and passwords are stored in the Prime Network database. If you use an external LDAP application, passwords are stored on the external LDAP server. See External Authentication, page 7-2.

- **User authorization** is managed through a combination of user access roles and scopes:
  - User access roles control the actions a user can perform in the Prime Network GUI clients. When a user’s account is created, the user is assigned an access role that determines the user’s default permissions. For more information, see Prime Network User Roles, page 7-2.
  - Scopes are groups of network elements that are created by administrators. Once a scope is created, you can assign it to users. A user’s default permissions determine the actions the user can perform on the network elements in the scope. These actions are referred to as the user’s security level on that scope. If desired, you can assign the user a more strict user access role for a scope. For more information, see Device Scopes, page 7-3.
Prime Network determines whether a user is authorized to perform a task as follows:

- For GUI-based tasks (tasks that do not affect devices), authorization is based on the default permission that is assigned to the user’s account.
- For device-based tasks (tasks that do affect devices), authorization is based on the device scope assigned to the user’s account—that is, whether the device is in the user’s assigned scopes and whether the user meets the minimum security level for that scope.

User authorization information (roles and scopes) is always stored in the Prime Network database. The external LDAP server, if used, only stores passwords.

**External Authentication**

External authentication means that user authentication and passwords are validated by an external application, rather than by Prime Network. When Prime Network performs the authentication, Prime Network validates users by checking information that is saved in the Prime Network database. If you use an LDAP application, the information is validated by the external LDAP server.

If Prime Network is using external authentication and cannot communicate with the LDAP server, the only user permitted to log back into Prime Network is root. This is because root is also an emergency user, and is validated only by Prime Network. The root user can then log into Prime Network, change the authentication method to local, and edit user accounts so that those users can subsequently log in.

Prime Network uses LDAP version 3.

---

User authentication by Prime Network is disabled if Prime Network is installed with Cisco Prime Central. However, the emergency user will still be allowed to log into Prime Network.

If you want to use external authentication, you must do the following:

- Perform the necessary installation prerequisites. See the *Cisco Prime Network 3.9 Installation Guide*.
- Configure Prime Network so that it can communicate with the LDAP server. See Configuring Prime Network to Communicate with the External LDAP Server, page 7-10.

If you are switching from external authentication to Prime Network authentication, you can import the user information from the LDAP server into Prime Network. That procedure is described in the Importing Users from the LDAP Server to Prime Network, page 7-13.

**Prime Network User Roles**

User roles control the actions a user is authorized to perform in Prime Network. Prime Network provides five predefined security access roles that you can grant to users to enable system functions (see Table 7-1).
Users with higher user roles can perform all the actions for which lower roles are authorized. For example, the Configurator is authorized to perform all the actions that the Viewer, Operator and OperatorPlus can perform.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewer</td>
<td>Views the network, links, events, and inventory. Has read-only access to the network and to nonprivileged system functions.</td>
</tr>
<tr>
<td>Operator</td>
<td>Performs most day-to-day business operations such as managing alarms, working with existing maps, viewing network-related information, and managing business attachments.</td>
</tr>
<tr>
<td>OperatorPlus</td>
<td>Manages tickets and the alarm lifecycle.</td>
</tr>
<tr>
<td>Configurator</td>
<td>Performs tasks and tests related to configuration and activation of services, through Command Builder, Configuration Archive, NEIM, and activation commands.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Manages the Prime Network system and its security using the Prime Network Administration GUI.</td>
</tr>
</tbody>
</table>

Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

Device scopes are groups of managed NEs. Users can only access devices when a device scope has been assigned to their account. In this way, you can control the devices a user can access. Furthermore, you can designate a security level (user access role) within each scope that controls the actions users can perform on those NEs. (The GUI-based operations (that do not affect devices) are controlled by the user’s default permissions.)
Overview of User Authentication and Authorization

Prime Network provides a predefined scope called All Managed Elements, which cannot be edited. It has these characteristics:

- The scope includes all network elements (as the name implies).
- This scope is automatically assigned to user accounts with Administrator privileges when the accounts are newly created. This is done by default. If necessary, you can edit the scope to have less privileges, or even delete it completely, which would give the Administrator full access to all GUI functions that do not affect devices.
- The scope can be assigned to non-Administrator user accounts, but with lower privileges. For example, for an account with OperatorPlus privileges, you could assign the All Managed Devices scope to the account, but the highest available security level would be Configurator.

Whenever the All Managed Elements scope is assigned to an Administrator—either when the Administrator account is created or after increasing a user’s privileges to Administrator role—the scope has a unique (and recognizable) security level called Special. The Special security level is equivalent to the Administrator security level and grants the Administrator user complete access to the network devices.

Note that a device scope can override a GUI user access role. Here is an example:

1. John has the Operator user access role (his default permission) for GUI operations.
2. John has the Configurator role for the device scope CE-SJ.

John can perform Configurator operations on any devices in the device scope CE-SJ, even though his default permission is the Operator user access role.

Table 7-2 describes the actions a user can perform in the GUI clients or in a scope, based on each user access role.

---

Note

Users with higher user roles can perform all the actions for which lower roles are authorized. For example, the Configurator is authorized to perform all the actions that the Viewer, Operator, and OperatorPlus can perform.
### Table 7-2 Scope and GUI Functions Permitted According to User Access Roles

<table>
<thead>
<tr>
<th>User Access Role</th>
<th>GUI-Based Actions Permitted to Users with This Role</th>
<th>Device Based (Scope) Actions Permitted to Users with This Role</th>
</tr>
</thead>
</table>
| Administrator    | Administrators are the only users that can perform actions in Prime Network Administration, which means managing:  
- Gateways, units, AVMs, VNEs.  
- Event notifications  
- Global settings: Database segments, event management settings, polling groups, protection groups, service disclaimers, report settings, and security settings (including user authentication method and password rules).  
- Device scopes.  
- User accounts.  
- Static topology links.  
- Workflow templates and workflows.  
Perform all event management actions in Prime Network Events.  
Perform all monitoring tasks in Prime Network Vision.  
- Launch PathTracer. | All |
| Configurator     | Advanced tools:  
- Ping and Telnet an NE directly from the client.  
- Prime Network Command Builder. | Advanced tools:  
- Enable and disable port alarms.  
- Deploy workflows (that have BQL tasks).  
Activation services:  
- Add and publish activation commands on managed NE (regardless of whether the NE is inside or outside the Configurator’s scope).  
Display network information:  
- Include path tool traffic, rates, drops, or any dynamic data. |
| OperatorPlus     | Maps:  
- Create new maps and add NEs.  
- Edit, delete, and rename maps.  
- Save maps.  
- Find, select, and filter links. | Display network information:  
- Refresh port information from NE. |
| Operator         | Maps: Group and ungroup aggregations  
- Create and delete business tags. | Display network information:  
- Include path tool traffic, rates, drops, or any dynamic data. |
Overview of User Authentication and Authorization

These guides provide detailed lists about the roles that are required to use these Prime Network functions:

- *Cisco Prime Network 3.9 User Guide* for Vision, Events, PathTracer
- *Cisco Prime Network 3.9 Change and Configuration Management User Guide* for Prime Network Change and Configuration Management

### Steps for Setting Up Users and Scopes

Note

These features are disabled if Prime Network is installed with Cisco Prime Central. If a user tries to log into Prime Network, they will be redirected to the suite login page. The only exception is the Prime Network emergency user, who will still be allowed to log into standalone Prime Network.

Follow these steps to set up user accounts and device scopes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>See:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure external authentication if you want to use an external LDAP server to store passwords and authenticate users.</td>
<td>Using an External LDAP Server for Password Authentication, page 7-7</td>
</tr>
<tr>
<td>2</td>
<td>Set up the global password and security rules.</td>
<td>Managing Global Security Settings, page 7-7</td>
</tr>
</tbody>
</table>
Managing Global Security Settings

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

The global Security Settings control the following:

- **Using an External LDAP Server for Password Authentication, page 7-7** — This topic explains how external authentication works, prerequisites and how to use the Authentication Method window, how to import a list of users, and how to change from external to local authentication.

- **Setting Global Password Rules, page 7-14** — The global Password Settings window allows you to specify password strength, the number of allowed password retries, and how often users should change their passwords. These rules are applied to all users.

- **Automatically Disabling Accounts for Inactive Users, page 7-15** — The User Account settings specifies when user accounts should be disabled due to inactivity.

Using an External LDAP Server for Password Authentication

Note These features are disabled if Prime Network is installed with Cisco Prime Central.

The following topics describe how you can use an external LDAP server to perform user authentication. By default, Prime Network users internal authentication, which means passwords are stored in and verified against the data that is stored in the Prime Network database. If you want to use external authentication, these topics will guide you through the process.

- **How Does External Authentication Work?, page 7-8**
- **Prerequisites for Using LDAP, page 7-9**
- **Configuring Prime Network to Communicate with the External LDAP Server, page 7-10**
- **Importing Users from the LDAP Server to Prime Network, page 7-13**
- **Changing from External to Local Authentication, page 7-14**
How Does External Authentication Work?

These features are disabled if Prime Network is installed with Cisco Prime Central.

User authentication can be managed locally by Prime Network or externally by a Lightweight Directory Access Protocol (LDAP) application. If you use an external authentication, user information is checked against what is stored in the external LDAP server (instead of the Prime Network database). The external authentication server only stores login and password information; information pertaining to user roles and scopes is stored in the Prime Network database.

As illustrated in Figure 7-1, when a user logs in to the GUI client, the gateway server contacts the LDAP server to authenticate the user. If the user is successfully authenticated, the LDAP server sends a confirmation to the gateway server, and the gateway server allows the user to log in to Prime Network. From that point on, the user can perform functions and access network elements as specified by their roles and scopes (see Overview of User Authentication and Authorization, page 7-1).

The root user is the emergency user. The LDAP emergency user is validated only by Prime Network. Consequently, if the LDAP server goes down, root can log back into Prime Network.

If Prime Network is installed with Cisco Prime Central, the emergency user will still be allowed to log into Prime Network.
Prerequisites for Using LDAP

These features are disabled if Prime Network is installed with Cisco Prime Central.

You must meet the following prerequisites before you can configure Prime Network to use LDAP:

- The LDAP server must be reachable from the Prime Network server, including port 389 for nonencrypted communication, 636 for encrypted communication.
- The LDAP server must support LDAPv3 protocol.
- For encrypted communication, a certificate must be installed on the Prime Network server. See Installing the LDAP Certificate on the Prime Network Gateway Server, page 7-10.

Configuring a Secure Connection with the Windows Server 2003 Active Directory

To manage users in the Active Directory from Java, the connection to the server must be secure. Follow these procedures to make the server connection secure.

If you are using Secure Socket Layer (SSL) for encryption between the Prime Network server and the LDAP server, the Windows server must be a domain controller installed with an Enterprise Certificate Authority. To guarantee a secure connection, you must request and install the appropriate certificate.

To obtain the certificate from the LDAP server and place it on the gateway:

Step 1 Use Router Discovery Protocol (RDP) to log into the remote LDAP server.
Step 2 Choose Start > Programs > Administrative Tools > Domain Controller Security Policy.
Step 3 In the left pane, choose Security Settings > Public Key Policies > Automatic Certificate Request Settings.
Step 4 Right-click the right pane and choose New > Automatic Certificate Request.
Step 5 Click Next.
Step 6 Choose Domain Controller and click Next.
Step 7 Click Finish.
Step 8 Restart the server.
Step 9 After the server restarts, enter the following command on the command line:

```
# netstat -na
```

The SSL port 636 should be active; for example:

```
TCP 0.0.0.0:636 0.0.0.0:0 LISTENING
```
Installing the LDAP Certificate on the Prime Network Gateway Server

Prime Network requires a certificate to open a context with the LDAP server. To import the certificate into the system .truststore file, complete the following steps:

**Step 1** Download the certificate from the relevant LDAP workstation:

a. From the client workstation, go to http://ldaphost/certsrv, where ldaphost is the fully qualified domain name or IP address of the LDAP server.

b. For blade LDAP, enter the service provider username and password.

c. Click **Download a CA certificate, certificate chain, or CRL**.

d. Choose **Previous cmpdc** in the **CA certificate** option.

e. Click **Download CA certificate**.

f. Save the certnew.cer file on the workstation. You can rename the file as CA.LDAP-IP-address.cer.

**Step 2** Log into your workstation.

**Step 3** Go to ~/Main/resourcebundle/com/sheer and copy the .cer file to that directory.

**Step 4** Enter the following command on the command line:

```bash
# keytool -import -alias LDAPID -file CA.LDAP-IP-address.cer -keystore .truststore
```

**Note** Use the password in the security.properties file in this directory. Be sure to use a unique ID to set a unique alias.

**Step 5** Enter the following command to check your LDAP certificates on the system .truststore file:

```bash
# keytool -list -keystore .truststore
```

Configuring Prime Network to Communicate with the External LDAP Server

**Note** These features are disabled if Prime Network is installed with Cisco Prime Central.

Use this procedure to configure the Prime Network gateway server to communicate with the LDAP server, and to test the connection after it is configured. You can configure a primary and secondary LDAP server. This procedure uses LDAP terminology, such as distinguished name (DN), common name (CN), and domain component (DC). An LDAP distinguished name uniquely identifies a user in the LDAP database, similar to a full filename but in reverse order. CNs and DCs are attributes of the domain name.

**Before You Begin**

Make sure you have performed the required prerequisites that are described in the *Cisco Prime Network 3.9 Installation Guide*:

- The LDAP server is correctly configured.
- You know the port number needed for the SSL or simple encryption protocol. These are normally 636 for SSL and 389 for simple.
If you select SSL for the Application-LDAP Protocol, the SSL certificate must be installed on the Prime Network gateway.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To configure the Prime Network gateway server to communicate with the LDAP server:

1. Choose **Global Settings > Security > Authentication Method**.
2. Click **LDAP Authentication** to activate the LDAP Settings area.
3. Complete the LDAP settings. The settings include specifying LDAP schema attributes, such as CN (common name) and DC (domain component).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP URL</td>
<td>LDAP server name and port number, in the following format:</td>
</tr>
<tr>
<td></td>
<td><code>ldap://host.company.com:port</code></td>
</tr>
<tr>
<td></td>
<td>where:</td>
</tr>
<tr>
<td></td>
<td>- <code>host.company.com</code>—Fully qualified domain name or IP address of the LDAP server, followed by the final two fields of the Distinguished Name Suffix (company.com, described below</td>
</tr>
<tr>
<td></td>
<td>- <code>port</code>—Network port of the LDAP server. The LDAP server port number is normally 389 for simple encryption and 636 for SSL encryption.</td>
</tr>
<tr>
<td></td>
<td>To specify a primary and secondary LDAP server, use the following format:</td>
</tr>
<tr>
<td></td>
<td><code>ldap://host1.company.com:port1 ldap://host2.company.com:port2</code></td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td><code>ldap://ldapsj.acme.com:636 ldap://ldapsfo.acme.com:636</code></td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>First part of the LDAP DN, which is used to uniquely identify users. Enter the information exactly as shown:</td>
</tr>
<tr>
<td>Prefix</td>
<td>CN</td>
</tr>
<tr>
<td></td>
<td>(The actual format is <code>CN=Value</code>, which specifies the common name for specific users. <code>=Value</code> will be automatically populated with Prime Network usernames.)</td>
</tr>
</tbody>
</table>
Managing Global Security Settings

Step 4
Click **Test Connection** to test the connection between the gateway server and the LDAP server.

Step 5
Click **Apply**.

Step 6
Restart the gateway for your changes to take effect. See **Starting and Stopping the Gateway and Checking AVM Status, page 2-3**.

You can now manage user passwords using the external LDAP server.

---

**Table 7-3 LDAP Authentication Method Settings (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distinguished Name</td>
<td>Second part of the LDAP distinguished name, which specifies the location in the directory:</td>
</tr>
<tr>
<td>Suffix</td>
<td>,CN=Users,DC=LDAP_server,DC=company,DC=com</td>
</tr>
<tr>
<td></td>
<td>where:</td>
</tr>
<tr>
<td></td>
<td>• ,CN=Users—Common name for the type of user; enter <strong>Users</strong>. For example:</td>
</tr>
<tr>
<td></td>
<td>,DC=Users</td>
</tr>
<tr>
<td></td>
<td>• ,DC=LDAP_server—Domain component that specifies the fully qualified domain name or IP address of the Prime Network server. For example:</td>
</tr>
<tr>
<td></td>
<td>,DC=ldapsj</td>
</tr>
<tr>
<td></td>
<td>• ,DC=company—Beginning of the domain name. For example:</td>
</tr>
<tr>
<td></td>
<td>,DC=acme</td>
</tr>
<tr>
<td></td>
<td>• ,DC=com—End of the domain name; enter <strong>com</strong>. For example:</td>
</tr>
<tr>
<td></td>
<td>,DC=com</td>
</tr>
<tr>
<td></td>
<td>The form should:</td>
</tr>
<tr>
<td></td>
<td>• Begin with a comma.</td>
</tr>
<tr>
<td></td>
<td>• End without any ending symbols or punctuation.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>,CN=Users,DC=ldapsj,DC=cisco,DC=com</td>
</tr>
<tr>
<td>Application-LDAP</td>
<td>Encryption protocol used for communication between the Prime Network gateway server and the LDAP server.</td>
</tr>
<tr>
<td>Protocol</td>
<td><strong>Note</strong> The encryption protocol used must be configured on both the Prime Network gateway server and the LDAP server.</td>
</tr>
<tr>
<td></td>
<td>The supported protocols are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>SIMPLE</strong>—Encrypt using LDAP. Uses port 389 by default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SSL</strong>—Encrypt using SSL. Uses port 636 by default. The SSL certificate must be installed on the Prime Network gateway (see the <strong>Cisco Prime Network 3.9 Installation Guide</strong>).</td>
</tr>
</tbody>
</table>
Importing Users from the LDAP Server to Prime Network

**Note**
These features are disabled if Prime Network is installed with Cisco Prime Central.

You can perform a bulk import of users from the LDAP Data Interchange Format (LDIF) file. The Prime Network `import_users_from_LDIF_file.pl` command has the following attributes:

- LDIF filename.
- Prime Network role—Administrator, Configurator, Operator, OperatorPlus, and Viewer (the default).
- username—Attribute name as it appears in the LDIF file. The username can appear in the LDIF file as username only, or in the format `username@domain`. In both cases, after the import, the Prime Network user is the name only (without the `@domain` suffix).
- user description—Attribute name as it appears in the LDIF file.
- user full name—Attribute name as it appears in the LDIF file.

The LDIF file has the following constraints:

- For each user, the username attribute is mandatory. The description and full name are optional.
- All other attributes are ignored.
- The LDIF file should reside in the gateway workstation under the `~/.Main` directory.

For example, for a Windows LDAP server, enter the following command to produce a valid LDIF file:

```
# ldiffde -l description,displayName,userPrincipalName -f desired-filename -r objectClass=user
```

The `import_users_from_LDIF_file.pl` command has the following syntax:

```
import_users_from_LDIF_file.pl ldif-filename [roleName] username-attribute-name user-desc-attribute-name full-name-attribute-name
```

**Example LDIF File and Import Command**

This example uses an LDIF file named users.LDF, with the following contents:

```
dn: CN=xxx,CN=Users,DC=ldapsj,DC=com
changetype: add
displayName: xxx
userPrincipalName: xxx@acme.com

dn: CN=yyyy,CN=Users,DC=ldapsj,DC=com
changetype: add
displayName: yyyy
userPrincipalName: yyy@acme.com

dn: CN=zzz,CN=Users,DC=ldapsj,DC=com
changetype: add
description: description
displayName: zzz
userPrincipalName: zzz@acme.com
```

This corresponding Prime Network command is as follows:

```
# cd $ANAHOME/Main/scripts
# import_users_from_LDIF_file.pl users.LDF userPrincipalName description displayName
```
This example would create three users with a Viewer role.

**Note**

All imported users are created with non-Prime Network authentication permissions (LDAP authentication). If the username already exists in Prime Network, the new user is not created.

### Changing from External to Local Authentication

**Note**

The Authentication Method feature is disabled if Prime Network is installed with Cisco Prime Central. However, the emergency user will still be allowed to log into Prime Network.

If Prime Network is using external authentication and cannot communicate with the LDAP server, the only user permitted to log back into Prime Network is root. This is because root is the emergency user, and is validated only by Prime Network. The root user can then log into Prime Network, change the authentication method to local, and edit user accounts so that those users can subsequently log in. For information on editing user accounts, see Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To change from external to local authentication, follow this procedure:

**Step 1** Choose Global Settings > Security > Authentication Method.

**Step 2** Click Prime Network Authentication to activate local authentication.

**Step 3** Click Apply.

**Step 4** Restart the gateway for your changes to take effect. See Starting and Stopping the Gateway and Checking AVM Status, page 2-3.

**Step 5** Reconfigure user accounts accordingly (see Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22).

### Setting Global Password Rules

**Note**

The Password Settings feature is disabled if Prime Network is installed with Cisco Prime Central.

You can set password rules that will apply to all new user accounts and to existing accounts when users change their passwords. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.
To set up or change global password rules:

---

**Step 1** Choose **Global Settings > Security Settings > Password Settings.** The Title and Message fields appear in the content area.

**Step 2** Configure the general settings in the General area:
- Password Validity Period—Number of days after which users must change their password.
- Number of Attempts Before Lockout—Choose a value from 3 to 7, or Unlimited. If a user is locked out, they cannot log back in until an administrator reenables their account (see Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22).

**Step 3** Check the check boxes for the password strength settings you want to apply to all users by default:
- Number of previous passwords that cannot be repeated (1 to 15)
- Number of character types required in password (0 or 3)
- Whether repeated characters can be used consecutively
- Whether usernames can appear in passwords
- Words that cannot appear in any passwords (comma-separated list)

**Step 4** Click **Apply** to immediately apply your settings.

After you click **Apply**, the password settings are applied to all new user accounts. You can restore the Prime Network default settings at any time by clicking **Restore and Apply**.

For information about the main menu that is displayed in the Prime Network window, see **Password Settings Window, page 1-28**.

### Automatically Disabling Accounts for Inactive Users

**Note**
The User Account Settings feature is disabled if Prime Network is installed with Cisco Prime Central.

You can configure Prime Network to disable a user account when a user has not logged in for a specified period of days. By default, this period is 30 days.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To change this setting:

**Step 1** Choose **Global Settings > Security Settings > User Account Settings.**

**Step 2** Enter the number of days after which the accounts will be disabled.

**Step 3** Click **Apply** to immediately apply your settings.

After you click **Apply**, the password settings are applied to all new user accounts. You can restore the Prime Network default settings at any time by clicking **Restore and Apply**.
You can reenable a user account as described in Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

For information about the main menu that is displayed in the Prime Network window, see User Account Settings Window, page 1-29.

Creating and Managing Scopes

Note

Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

Prime Network Administration enables you to group specific managed network elements so that users can view and manage those network elements based on their user role or permission.

After a scope is created, it can be assigned to a user. Multiple scopes can be assigned to a single user and a single scope can be assigned to multiple users. When the scope is assigned to a user, you must provide the user with security access roles that define the user’s role within the assigned scope. See Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

These topics explain how to manage scopes:

- Creating Device Scopes in Prime Network, page 7-16
- Viewing and Editing Existing Device Scopes, page 7-18
- Deleting a Device Scope from Prime Network, page 7-18

Creating Device Scopes in Prime Network

Note

Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

A scope is a group of devices. Users cannot perform any devices until you create a scope and apply it to their user account.

Note

By default, users can only view links if both endpoints are in this scope. If you want to change this setting so that only one link endpoint is required, see Viewing Links in Device Scopes, page 7-17.

To create a scope:

Step 1 Right-click Scopes and choose New Scope to open the New Scope dialog box.

Step 2 In the Scope field, enter a name for the scope.
Step 3  Add devices to the scope by selecting them from the Available Devices list and moving them to the Selected Devices list.

Note  You can select multiple devices by using the Ctrl key.

Step 4  Click OK. The scope is saved and is displayed in the content area.

Step 5  If you want a user to be allowed

Note that the scope does not have a default security level. When you add the scope to a user’s account, you specify their security role on the scope at that time. This allows you to provide different security levels for different users.

**Viewing Links in Device Scopes**

By default, a user can view a link in Prime Network Vision only if both link endpoints are in the user’s device scope. If you want to make links viewable if only one endpoint is in a user’s scope, you must edit the registry as follows. Changes are applied to all device scopes in the system.

Step 1  Log into the gateway as `network user` (where `network user` is the operating system account for the Prime Network application, created when Prime Network is installed; an example of `network user` is `network39`), and change to the `NETWORKHOME/Main` directory:

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

Step 2  To check the current setting, run the following command (which is one line):

```bash
# ./runRegTool.sh -gs 127.0.0.1 get 0.0.0.0 "site/mmvm/services/securitymanager/linkoid-by-any-side"
```

A return of false means it is set to the default; that is, both links must be in a user’s scope to be viewable.

Step 3  To change the setting so that only one link endpoint is required, run the following command (which is one line):

```bash
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/mmvm/services/securitymanager/linkoid-by-any-side" true
```

Step 4  When the gateway server returns a success message, restart it.
Creating and Managing Scopes

Chapter 7      Managing User Security: Roles and Scopes

Viewing and Editing Existing Device Scopes

Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

To view the properties of an existing scope, simply right-click the scope and select Properties.

When editing a scope, keep the following mind:

- You can add or delete devices from an existing scope. The changes will be applied to all user accounts that have access to that scope.
- You cannot change the name of an existing scope.
- You can change the security level on a device scope, but not from the Scopes window. You must edit the user account in the Users window. See Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

To edit a scope by adding or deleting devices:

- **Step 1**: Select Scopes to populate the list of existing scopes.
- **Step 2**: Right-click a scope and choose Properties.
- **Step 3**: Modify the scope device list by selecting them from the Available Devices list and moving them to the Selected Devices list.

  *Note* You can select multiple devices by using the Ctrl key.

- **Step 4**: Click OK. The scope is updated and is displayed in the content area.

Deleting a Device Scope from Prime Network

Device scopes are disabled if Prime Network is installed with Cisco Prime Central.

When a scope is deleted, it is deleted from all users who have the assigned scope.

To delete a scope:

- **Step 1**: Select Scopes in the navigation pane.
- **Step 2**: Right-click the scope you want to remove, then choose Delete.

  *Note* You can select multiple scopes by using the Ctrl key.

The scope is deleted and is removed from the content area.
Managing User Accounts and Controlling User Access

These features are disabled if Prime Network is installed with Cisco Prime Central. If a user tries to log into Prime Network, they will be redirected to the suite login page. The only exception is the Prime Network emergency user, who will still be allowed to log into standalone Prime Network. If you migrate from standalone to working with Cisco Prime Central, you must create the Cisco Prime Central users using the Cisco Prime Portal portal, even if the users already existed in standalone mode. (Cisco Prime Central will advise you that the user already existed in Prime Network and will retrieve the user properties and apply them to the new Cisco Prime Central user.)

The Users windows enable you to define and manage user accounts. This includes managing general user information as well as security access rights and forced login changes, as required. You can also monitor a user’s last login time. See the following topics for more information:

- Creating a New User Account and Viewing User Properties, page 7-19
- Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22
- Controlling User Access to Maps (Maps Tab), page 7-23

Creating a New User Account and Viewing User Properties

These features are disabled if Prime Network is installed with Cisco Prime Central. If a user tries to log into Prime Network, they will be redirected to the suite login page. The only exception is the Prime Network emergency user, who will still be allowed to log into standalone Prime Network. If you migrate from standalone to working with Cisco Prime Central, you must create the Cisco Prime Central users using the Cisco Prime Portal portal, even if the users already existed in standalone mode. (Cisco Prime Central will advise you that the user already existed in Prime Network and will retrieve the user properties and apply them to the new Cisco Prime Central user.)

The following procedure describes how to define a user account. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

**Step 1**  
Right-click **Users** and choose **New User** to open the New User dialog box.

**Step 2**  
Enter the general information about the user in the General Settings area. For existing users, click the General tab to display this information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter the new user’s name to be used for logging in.</td>
</tr>
<tr>
<td>Full Name</td>
<td>(Optional) Enter the full name of the user.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a free text description of the user.</td>
</tr>
</tbody>
</table>
Step 3 Click **Next** and configure the GUI client and device authorization settings for the user. For existing users, click the Authorization tab to display these settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Role</td>
<td>Select the role that will control the actions the user can perform in the Prime Network, such as which functions they can use in the GUI clients. Click <strong>Read More</strong> for a description of the roles; you can also get more information from Prime Network User Roles, page 7-2. For information on the special All Managed Elements scope, see Device Scopes, page 7-3.</td>
</tr>
<tr>
<td>Device Security</td>
<td>Select scopes and apply the security levels to them that will control the actions the user can perform on devices. You can apply different security levels for different scopes. If you do not apply a security level to a scope, it defaults to the Viewer level. <strong>Note</strong> Users will not see any devices in the GUI client unless a device scope is assigned to their account. Use the following buttons to manage scopes. Note that the edit and remove buttons only affect the scopes assigned to this user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong>—Add a scope to this user account from the list of available scopes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong>—Edit the security level for a scope <strong>assigned to this user</strong>. (This edit function only changes the user's scope security level; it does not change the scope device list. That must be done from the Scopes drawer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove</strong>—Deletes a scope <strong>from this user’s account</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>New Scope</strong>—Creates a new scope and adds it to the list of available scopes <strong>for all users</strong>. See Creating Device Scopes in Prime Network, page 7-16. Changes that you apply to a scope will be applied to all users that have access to that scope.</td>
</tr>
</tbody>
</table>
**Step 4**  Click **Next** and enter the account settings for the user. For existing users, click the Account tab to display these settings. (If you are creating a new account, you can also click **Finish** to accept the default account settings. The default settings are provided in the following.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
</table>
| Enable Account                | Enables and disabled the user account. You can manually lock or unlock a user’s account at any time. A user whose account is locked cannot log into the system until you reenable their account. The user account is automatically locked if:  
  - The number of logins defined is exceeded (see the Limit Connections field in the following).  
  - The user account is not active for a certain number of days, as configured in the Global Settings branch (see **Automatically Disabling Accounts for Inactive Users**, page 7-15); by default, this period is 30 days. | Enabled. |
| Force Password Change at Next Login | Check this check box to force the user to change their user password when they next log in. This field is disabled if the gateway server is using external LDAP authentication.                                                                                      | Enabled. |
| Limit Connections:           | The maximum number of Prime Network client sessions that the user can be running at any one time. This includes all client types including BQL sessions and workflow invocations. Leaving this field blank means the user can have *unlimited* connections.  
  **Note** The workflow mechanism requires 3 connections. If you set this value to lower than 3, users will not be able to access the workflow mechanism. | 10 connections |
| Force Password Change After ___ Days | Forces the user to change their password after a specific number of days. Uncheck this check box to allow the user to retain their current password indefinitely. This field is disabled if the gateway server is using external LDAP authentication. | Controlled by Global Settings; see **Setting Global Password Rules**, page 7-14. |

**Step 5**  Click **Finish**, and Prime Network creates the account. After the confirmation message is displayed, click **Close** to close the dialog box. The new account is displayed in the Users table.
Viewing, Changing, and Disabling User Accounts and Device Scope Access

**Note**

These features are disabled if Prime Network is installed with Cisco Prime Central.

Administrators can view, edit, or disable an individual user’s account settings.

To change global settings such as password rules and inactivity periods, see Managing Global Security Settings, page 7-7. The global settings control settings for all users.

**Step 1**
Select **Users** to populate the list of existing user accounts.

**Step 2**
Right-click a user account and choose **Properties** to open the user properties dialog box.

**Step 3**
Edit the following fields, as required (not all fields are editable).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Full Name</td>
<td>(Optional) Full name of the user.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Free text description of the user.</td>
</tr>
<tr>
<td><strong>Authorization Tab</strong></td>
<td></td>
</tr>
<tr>
<td>User Role</td>
<td>The role that will control the actions the user can perform in the Prime Network, such as which functions they can use in the GUI clients. For information on how to make changes, see Creating a New User Account and Viewing User Properties, page 7-19.</td>
</tr>
<tr>
<td>Device Security</td>
<td>Scopes and apply the security levels to them that will control the actions the user can perform on devices. For information on how to make changes, see Creating a New User Account and Viewing User Properties, page 7-19.</td>
</tr>
<tr>
<td><strong>Account Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Account</td>
<td>Enables and disabled the user account.</td>
</tr>
<tr>
<td>Force Password Change at Next Login</td>
<td>Force the user to change their user password when they next log in. This field is disabled if the gateway server is using external LDAP authentication.</td>
</tr>
<tr>
<td>Limit Connections</td>
<td>The maximum number of Prime Network client sessions that the user can be running at any one time. This includes all client types.</td>
</tr>
<tr>
<td>Force Password Change After ____ Days</td>
<td>Forces the user to change their password after a specific number of days. Uncheck this check box to allow the user to retain their current password indefinitely. This field is disabled if the gateway server is using external LDAP authentication.</td>
</tr>
</tbody>
</table>

**Step 4**
Click **Apply** to apply your changes, and click **OK** to close the Properties dialog box.
Controlling User Access to Maps (Maps Tab)

Note
These features are disabled if Prime Network is installed with Cisco Prime Central.

You can use the Maps tab to control user access to existing maps.

Note
This feature is disabled by default.

When logging into Prime Network Vision, new users do not have permission to view any existing maps; they can only access maps they create going forward. However, administrators can assign existing maps to new users by enabling this feature and manually assigning the maps.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To enable this feature:

Step 1
Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; an example of network user is network39), and change to the NETWORKHOME/Main directory:

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

Step 2
Run the following command (which is one line):

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/mvvm/services/securitymanager/map-security-enabled" true
```

Step 3
When the gateway server returns a success message, restart the gateway.

To assign maps to a user (after enabling the feature):

Step 1
Select Users in the Prime Network window.

Step 2
Right-click the required user, then choose Properties. The User Properties dialog box is displayed.

Step 3
Click the Maps tab. The Maps tab is divided into two parts:

- The left side displays a list of all available maps in the database that have not been assigned to the user.
- The right side displays all maps that have been assigned to the user and that the user can open and manage in Prime Network Vision.

Step 4
Choose a map from the list of Available Maps, then click the required button to add the map to the list of Assigned Maps to the user.

Note
You can select multiple rows by using the Ctrl key.
Deleting a Prime Network User Account

Note
This feature is disabled if Prime Network is installed with Cisco Prime Central.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

If you want to disable a user account but not delete it, see Viewing, Changing, and Disabling User Accounts and Device Scope Access, page 7-22.

To delete a user account:

Step 1 Select Users in the navigation pane.
Step 2 Right-click the account you want to remove, then choose Delete.

The account is deleted and is removed from the content area.

Changing a User’s Prime Network Password

Note
This feature is disabled if Prime Network is installed with Cisco Prime Central.

You can use Prime Network Administration to change a user’s Prime Network password at any time. Passwords must adhere to the global password rules set by the administrator (see Setting Global Password Rules, page 7-14).

The following procedures apply only if you are using Prime Network to validate users. If you are using an external LDAP application to manage passwords, you must change the passwords in the LDAP server.

There are different procedures for administrators and for users, as described in the following. The root user password can also be changed using these procedures.

Note
If you have lost the root password, you can create a new one using the procedure in Changing Passwords: bosenable, bosconfig, and bosusermanager, and root, page 15-4.
You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

**Changing Passwords—Procedure for Administrator**

Administrators can change any user’s password using the following procedure.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Users</strong> in the navigation pane.</td>
</tr>
<tr>
<td>2</td>
<td>Right-click the users account, then choose <strong>Change Password</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Enter the new password in the Password and Confirm Password fields.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>OK</strong>. A confirmation message is displayed.</td>
</tr>
<tr>
<td>5</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

**Changing Passwords—Procedure for Users**

Users can change their own passwords using the following procedure.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Tools &gt; Change User Password</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Enter the old password in the Old Password field.</td>
</tr>
<tr>
<td>3</td>
<td>Enter the new password in the New Password and Confirm Password fields.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>OK</strong>. A confirmation message is displayed.</td>
</tr>
<tr>
<td>5</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
CHAPTER 8

Backup and Restore

These topics describe how to back up and restore your data:

- Backing Up Your Data, page 8-1
- Restoring Prime Network Data, page 8-4

For information on how to back up and restore an embedded database, see Working With an Embedded Database, page 11-1.

Backing Up Your Data

The following topics explain how and when Prime Network performs backups.

Note
The procedures described in these topics do not back up the Oracle database. If you have installed an embedded database, you can follow the procedure in Backing Up an Embedded Database and Prime Network, page 11-10. Otherwise, see your Oracle documentation for instructions on how to back up the database.

- Overview of the Backup Procedure, page 8-1
- Changing the Periodic Backup Time, page 8-3
- Performing a Manual Backup, page 8-4

Overview of the Backup Procedure

The following topics provide an overview of the standard backup procedure and its default settings.

Which Files Are Backed Up

Prime Network backs up its registry data, encryption keys, and reports using the operating system cron mechanism. If you have installed an embedded database, see Backing Up an Embedded Database and Prime Network, page 11-10.

Table 8-1 lists the directories that are backed up.
Chapter 8      Backup and Restore

8-2

Table 8-1  Directories Backed Up by Prime Network

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry information</td>
<td>NETWORKHOME/Main/registry</td>
<td>Prime Network registry, which includes changes made since the installation (new soft properties, Command Builder commands, alarm customizations, and so forth)</td>
</tr>
<tr>
<td>General information</td>
<td>NETWORKHOME/Main/.encKey</td>
<td>SSH encryption key files</td>
</tr>
<tr>
<td></td>
<td>NETWORKHOME/Main/to_backup</td>
<td>Other user-specified data</td>
</tr>
<tr>
<td></td>
<td>NETWORKHOME/Main/reportfw/rptdocument</td>
<td>Prime Network reports¹</td>
</tr>
</tbody>
</table>

1. Some report data is stored in the database, so you must back up both the database and the Prime Network data to capture all report information.

How Many Backups Are Saved

By default, Prime Network saves five backups.

Where Backups Are Stored

When the backup files are created, they are stored in the directory NETWORKHOME/backup.

Note

If you reinstall the server using the install.pl script, the user network user and the content under it is deleted. This includes the default backup directory. (network user is the operating system account for the Prime Network application, created when Prime Network is installed.) In this example, network user is network39. You can change the location, but the user network user must be able to write to the location. For example, the default directory permissions are:

`(*drwx------ 2 network39 network39 512 Sep 24 02:54*)`

We recommend that you do not locate the backup directory under /tmp, since this directory is deleted whenever the server is rebooted, and the backed-up content lost.

To maximize data safety, we recommend that you copy the backed-up directory to an external storage location, such as a DVD or a disk on a different server.

When Backups Are Performed

By default, backups every 12 hours at 4:00 a.m. and 4:00 p.m, as defined in the crontab file. You can change the backup time using the procedure described in Changing the Periodic Backup Time, page 8-3.

To restore data, you must execute the restore.pl command manually.

Changing the Default Backup Directory

You can change the default backup directory by editing the registry using the runRegTool.sh script.

Note

Changes to the registry should be performed only with the support of Cisco. For more information, contact your Cisco account representative.
Chapter 8  Backup and Restore

Backing Up Your Data

Before You Begin

Make sure that network user has the necessary write permissions for the new backup directory.

Step 1  Log into the gateway as network user. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39).

Step 2  Change the directory to the Main directory:

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

Step 3  Specify the new backup directory by providing a complete pathname for new-directory:

```
  # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
  "site/mmvm/agents/integrity/backup/backupOutputFolder" new-directory
```

Changing the Periodic Backup Time

Note  Do not change the periodic backup schedule if you have installed an embedded database (see Working With an Embedded Database, page 11-1). If this is required, contact the Technical Assistance Center.

The integrity service runs regular backups, along with other integrity tests, according to the settings in the system crontab file. Registry backups are controlled according to commands in the crontab file. To change the backup time, you must edit the crontab file.

The crontab file consists of lines, where each line contain six fields:

```
  min  hour  day-of-month  month-of-year  day-of-week  command
```

The fields are separated by spaces or tabs. The first five are integer patterns that can contain the following values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>min</td>
<td>Minute in range 0-59</td>
</tr>
<tr>
<td>hour</td>
<td>Hour in range 0-23</td>
</tr>
<tr>
<td>day-of-month</td>
<td>Day in range 1-31</td>
</tr>
<tr>
<td>month-of-year</td>
<td>Month in range 1-12</td>
</tr>
<tr>
<td>day-of-week</td>
<td>Day in range 0-6 (0=Sunday).</td>
</tr>
<tr>
<td>command</td>
<td>Command</td>
</tr>
</tbody>
</table>

To specify days using only one field, set the other fields to *. For example, 0 0 * * 1 runs a command only on Mondays.

In the following example, core files are cleaned up every weekday morning at 3:15 a.m.:  

```
15 3 * * 1-5 find $HOME -name core 2>/dev/null | xargs rm -f
```
The sequence 0 0 1,15 * 1 runs a command on the first and fifteenth of each month as well as every Monday.

Use this procedure to change when Prime Network backs up its registry (this command also changes when Prime Network will run integrity tests; see Archiving and Purging Data, page 10-4).

Step 1 Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39).

Step 2 Edit the cron table as follows:

```bash
# crontab -e
```

Step 3 Make your changes to the crontab file.

Step 4 Save your changes by entering Ctrl-x, and confirm your changes by entering y.

Step 5 Restart the gateway server.

---

**Performing a Manual Backup**

This procedure explains how to perform an on-demand backup contains the information described in Table 8-1 on page 8-2. This procedure does not back up any database information. For more information, see Overview of the Backup Procedure, page 8-1.

Step 1 Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39).

Step 2 Change the directory to the Main/scripts directory:

```bash
# cd $ANAHOME/Main/scripts
```

Step 3 Start the backup:

```bash
# backup.pl backup-folder
```

**Note** It is normal for null to appear in response to this command.

---

**Restoring Prime Network Data**

The following procedure restores the Prime Network data that is backed up, as listed in Which Files Are Backed Up, page 8-1.

**Note** The procedures described in these topics do not restore the Oracle database. If you have installed an embedded database, you can follow the procedure in Restoring an Embedded Database and Prime Network, page 11-13. Otherwise, see your Oracle documentation for instructions on how to restore the database.
To restore Prime Network data from a backup:

**Step 1**  Log into the gateway as *network user* (where *network user* is the operating system account for the Prime Network application, created when Prime Network is installed; for example, *network39*).

**Step 2**  Stop the gateway server and all units:
```
# cd $ANAHOME/Main
# networkctl stop
# rall.csh networkctl stop
```

**Step 3**  From the *NETWORKHOME/Main* directory, change to the directory *NETWORKHOME/Main/scripts*:
```
# cd scripts
```

**Step 4**  Execute the restoration script:
```
# restore.pl backup-folder
```

**Step 5**  Once the restoration is successful, initialize the Prime Network gateway by running the following commands:
```
# cd Main
# networkctl restart
```
PART 3

Advanced Gateway and Unit Administration
Advanced Administration for the Prime Network Gateway and Units

The following topics explain how to perform advanced administration tasks on the Prime Network gateways and units:

- Managing Configurations with Firewalls (Device Proxy), page 9-2
- Restarting Prime Network In a Gradual Manner, page 9-5
- Obtaining Diagnostic Information Using Graphs, page 9-6
- Automatic Overload Prevention (AOP/Safe Mode), page 9-17
- Changing the IP Address of the Gateway Server, page 9-21
- Gateway Open Sessions Registry Settings, page 9-23

Additional gateway and unit administration tasks are described in these topics:

- Basic Gateway Server Administration Tasks, page 2-1
- Basic Unit Server Administration Tasks, page 3-1
- Basic AVM and VNE Administration Tasks, page 4-1
Managing Configurations with Firewalls (Device Proxy)

Servers and Units Behind Firewalls

If a gateway server is behind a firewall, you must open ports on the firewall. The gateway will need a 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 9-1.
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.
Managing Configurations with Firewalls (Device Proxy)

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 and all units 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_user_passwd [-home_dir dir] -ana_user ana_username
```
The script uses the following arguments:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| -ana_user ana_username    | Name for ana_user (also called network user in our documentation). This is the operating system account for the Prime Network application, created when Prime Network is installed. A common example of network user is `network39`.
| -new_user_password ssh_user_passwd | SSH password for ana_username. 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 admin -ana_user network39
```

*Note* If a device proxy is configured on a setup without any units, use only the `create_ssh_user.pl` script.

**Step 3** 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 username -new_user_password ssh_user_passwd
```
The script uses the argument described in **Step 2**. For example, to create a dedicated SSH tunnel for the user created in **Step 2**:
```
# ./create_ssh_tunnel.pl -ana_user network39 -new_user_password admin
```
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 9-2.
Figure 9-2   Enabling the Device Proxy Feature

Restarting 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 A VMs (A VMs 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 A VMs.

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

Disable the user-defined A VMs 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 network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; an example of network user is network39).

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 Changing AVM Status (Start or Stop), page 4-12).

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.

Obtaining Diagnostic Information Using Graphs
In addition to the basic information provided by the networkctl command (described in Starting and Stopping the Gateway and Checking AVM Status, page 2-3), Prime Network provides a web-based diagnostics tool, the Cisco Prime Network Monitoring, that conveys 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.

These topics describe how to work with the Prime Network Monitoring tool:
- Logging Into the Prime Network Monitoring Tool, page 9-7
- Overview of the Prime Network Monitoring Window, page 9-7
Logging Into the Prime Network Monitoring Tool

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 Changing Passwords: Diagnostics Tool, page 15-5). When you log in for the first time, download and install the security certificate.

**Note**
The connection to the tool is via 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 9-3 on page 9-8). You can select a sampling period by choosing from the Period drop-down list and clicking Submit.

Overview of the Prime Network Monitoring Window

Figure 9-3 shows the default page that is displayed when you first log into the Prime Network Monitoring tool; it is called the MC Loads page. The MC Loads page lists information using this page orientation:

- Each row displays information about one server (units listed before the gateway). Units are identified by their IP addresses. In Figure 9-3, 10.56.56.93 is the one unit server that is managed by the Prime Network gateway server. The gateway server is identified by 127.0.0.1 which is the gateway IP address used by the golden source registry. You can find the gateway server’s actual IP address by looking at the address in the web page (10.56.56.92).

- Each column displays one graph type. In Figure 9-3, the top left graph provides Java heap data for the unit server 10.56.56.93. Directly below that graph is the Java heap data for the gateway server (127.0.0.1). You can add or remove graphs and adjust the sampling period using the toolbar; see Figure 9-4 on page 9-9.
## Obtaining Diagnostic Information Using Graphs

### Figure 9-3  MC Loads Page—All Servers (Default)

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Current date and time on the selected server.</td>
</tr>
</tbody>
</table>
| 2      | Toolbar that controls the sampling period represented in the graphs, and the graph types that are displayed. See:  
- Toolbar Controls—MC Loads Page, page 9-9  
- Toolbar Controls—Transport Counters Page, page 9-10 |
| 3      | Web page options that control what data is displayed: MC Graphs (gateway and unit information), Transport Counters, or Status. See Other Graphs Area (MC Loads Page and Transport Counters Page), page 9-9. |
| 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. |
Other Graphs Area (MC Loads Page and Transport Counters Page)

The Other Graphs area provides hyperlinks to other graphs and web pages that are supported by the Prime Network Monitoring tool. The choices displayed depend on the current web page. The following table lists all supported diagnostics tool pages.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC Loads</td>
<td>Provides load statistics for the gateway and unit servers. Clicking on an IP address hyperlink launches a drill-down page to that server, which lists the same graphs for each AVM. See Using the MC Loads Graphs, page 9-11.</td>
</tr>
<tr>
<td>Transport Counters</td>
<td>Displays a transport switch counters page that shows incoming and outgoing traffic rates, dropped messages, and flood counts, using the same basic GUI framework as the MC Loads pages. We recommend you use the MC Loads pages because those pages provide the most useful information.</td>
</tr>
<tr>
<td>Status</td>
<td>Provides status information about the graphs service—whether the service is up for all units, and when the data was last polled. If the service is down, contact your local Cisco professional.</td>
</tr>
</tbody>
</table>

Toolbar Controls—MC Loads Page

The MC Loads page provides the toolbar control illustrated in Figure 9-4.

Figure 9-4  Toolbar Controls for MC Loads Graphs

MC loads, Thu Oct 21 18:29:46 2010

Using the drop-down list, you can add and remove the following graphs to the MC Loads pages.
Obtaining Diagnostic Information Using Graphs

Chapter 9      Advanced Administration for the Prime Network Gateway and Units

Field | Description
--- | ---
Period | Sets the period of time for the graphs on the page.
Add/Remove column | Adds or removes the following supported graphs:

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

Toolbar Controls—Transport Counters Page

The Transport Counters page shows incoming and outgoing traffic rates, dropped messages, and flood counts, using the same basic GUI framework as the MC Loads pages. The Transport Counters page provides the toolbar control illustrated in Figure 9-4.

Figure 9-5   Toolbar Controls for Transport Counter Graphs

Transport switch counters, Thu Oct 21 18:27:22 2010

Using the drop-down list, you can add and remove the following graphs to the Transport Counters page.

Field | Description
--- | ---
Period | Sets the period of time for the graphs on the page.
Add/Remove column | Adds or removes the following supported graphs for gateways, units, and AVMs.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>The number of traffic frames and traffic bytes sent and received.</td>
</tr>
<tr>
<td>Drops</td>
<td>The number of dropped frames and dropped bytes, both outgoing and incoming.</td>
</tr>
<tr>
<td>Floods</td>
<td>The number of flood frames and flood bytes generated and received.</td>
</tr>
</tbody>
</table>
Using the MC Loads Graphs

These topics describe how to use and interpret the graphs presented in the MC Loads pages:

- Understanding the Colors and Indicators, page 9-11
- Common Uses for the MC Loads Page, page 9-13
- Customizing Graphs with Address Bar Parameters, page 9-16

Understanding the Colors and Indicators

When you click an IP address from the main MC Loads page (illustrated in Figure 9-3 on page 9-8), Prime Network Monitoring displays a drill-down page for the specific server. Figure 9-6 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.
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 9-7** Grey Line Indicators in the MC Loads Graphs

Figure 9-8 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.
Common Uses for the MC Loads Page

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 an 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 sawteeth 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 sawteeth—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 sawteeth 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.
Obtaining Diagnostic Information Using Graphs

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.

Customizing Graphs with Address Bar Parameters

In addition to the toolbar options, you can customize the graphs by entering additional parameters in the browser URL field, in an HTTP GET format. Table 9-1 describes the parameters you can use, along with examples.

Table 9-1 Available Graph Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| period    | The sampling period in the following format:  
  &period=\textit{xn}  
  where \( x \) is a number, and \( n \) is the unit of time measurement: \textit{h} (hours), \textit{m} (months), \textit{d} (days), or \textit{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=\textit{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 |
When Prime Network Monitoring Data is Purged

Prime Network Monitoring history is maintained for a period of 28 days, as follows.

<table>
<thead>
<tr>
<th>Age of Data</th>
<th>How Data is Saved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 3 hours old</td>
<td>Data is saved every 15 seconds.</td>
</tr>
<tr>
<td>3-24 hours old</td>
<td>Data is diluted to a sampling rate of 300 seconds.</td>
</tr>
<tr>
<td>24 hours to 7 days</td>
<td>Data is diluted to a sampling rate of 15 minutes.</td>
</tr>
<tr>
<td>24 hours to 7 days</td>
<td>Data is diluted to a sampling rate of 15 minutes.</td>
</tr>
<tr>
<td>More than 28 days old</td>
<td>Data is discarded.</td>
</tr>
</tbody>
</table>

Automatic Overload Prevention (AOP/Safe Mode)

Prime Network uses a software mechanism called Automatic Overload Prevention (AOP) to detect and prevent system overload. The AOP service monitors the load produced by components in Prime Network. Similar components, such as those that control fault management, are grouped together into an AOP subsystem. When a subsystem’s processing load becomes heavy, the whole system moves into safe mode. Other subsystems respond by adjusting their processing in order to prevent system overload. When this happens, a System event is generated and can be viewed in Prime Network EventVision.

If the subsystem continues to be overloaded, the components will take other measures to lessen the system load (if those measures are configured). As soon as the problematic subsystem returns to a normal load, all other components revert to normal.

The AOP mechanism is currently used by the following subsystems, due to the very large amount of data they process:

- Reporting subsystem.
- Fault subsystem, which includes the Alarm Plugin, Global Event Filter Agent, Event Integrity Agent, and Ticket Agent.
Chapter 9  Advanced Administration for the Prime Network Gateway and Units

Automatic Overload Prevention (AOP/Safe Mode)

Loads and Running Levels

The AOP service maintains the following information about each component in a subsystem.

<table>
<thead>
<tr>
<th>Load Indicator</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Load</td>
<td>Current processing load. When a component’s Current Load changes, other</td>
</tr>
<tr>
<td></td>
<td>components may respond by changing their Current Loads and/or Running</td>
</tr>
<tr>
<td></td>
<td>Levels. Supported Current Loads are:</td>
</tr>
<tr>
<td></td>
<td>• NORMAL</td>
</tr>
<tr>
<td></td>
<td>• LOADx (safe mode), where x is 1-6</td>
</tr>
<tr>
<td>Running Level</td>
<td>The state in which a component is running. Running Levels can change in</td>
</tr>
<tr>
<td></td>
<td>response to Current Load and/or Running Level changes in other components.</td>
</tr>
<tr>
<td></td>
<td>Supported Running Levels are:</td>
</tr>
<tr>
<td></td>
<td>• NORMAL, also called Running Level 0.</td>
</tr>
<tr>
<td></td>
<td>• AOPx or safe mode, where x is Running Levels 1-6.</td>
</tr>
</tbody>
</table>

When a problem occurs and a component’s load increases, the following can occur, depending on your system configuration:

- The reporting subsystem disabled reports (at AOP 6, by default).
- The Alarm Plugin stops auto-clearing events (at AOP 6, by default).
- The Global Event Filter drops some syslogs and traps (it does this at all AOP levels, and at AOP 6, it drops all syslogs and traps).

To specify which events the fault subsystem drops at different running levels, see Customizing the AOP Global Event Filter, page 9-19.

Note

Dropping syslogs and traps in this context means that syslogs and traps are not correlated and forwarded to the Fault Agent (AVM 25); syslogs and traps are still sent to the Event Archive (if enabled). Also note that only syslogs and traps are dropped; service events and network events (Audit, Security, System, and Provisioning events) are never dropped by the AOP mechanism.

As soon as the load returns to normal on the problematic component, all components respond by returning to normal and the system moves out of safe mode.

Displaying Current AOP Loads and Running Levels

To display the status of all components that are using AOP:

Step 1  Open an SSH session to the Prime Network gateway server and log in as networkuser. (networkuser is the UNIX account for the Prime Network application, created when Prime Network is installed; for example, network39.)

Step 2  Enter the following:

```bash
# telnet 0 2011
Connected to 0.
Sheer BOS AVM management
AVM11#/>cd aop
```
Customizing the AOP Global Event Filter

The Event Global Filter has two flavors:

- Filtering when the system is running in NORMAL mode (Running Level 0)
- Filtering when the system is in AOP mode (Running Levels AOP 1-6)

You can define filters for Running Levels 0-5—that is, for NORMAL mode, and for AOP 1-5. At Running Level 6, all traps and syslogs are dropped so no further filtering is useful.

The filter contains a list of rules that define what events should be excluded. Events are assigned a number (1-6), corresponding to the AOP running levels. When the AOP running level is x, all events with a number equal to or lesser than x are dropped. Note that this is done after events are sent to the Event Archive (if enabled).

Use the following procedure to create a new filter. In this procedure you will specify:

- Running level at which to drop the events that match the filter.
- The event information. When matched, the event will be dropped.

To create a new filter, use this procedure. For information on the properties described in the procedure, see the Cisco Prime Network Integration Developer Guide.

### Step 1
Log into the Prime Network gateway server as networkuser. (networkuser is the UNIX account for the Prime Network application, created when Prime Network is installed; for example, network39.)

### Step 2
Add the new filter information to the registry using the following command.

```
# ./runRegTool.sh -gs 127.0.0.1 add 0.0.0.0 site/event-global-filter/runningLevelID/propertyName
```
Automatic Overload Prevention (AOP/Safe Mode)

Chapter 9      Advanced Administration for the Prime Network Gateway and Units

**propertyName** can be any of the following:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description and Supported Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeverityEnum</td>
<td>An integer that represents the severity. Supported Severity Enums are:</td>
</tr>
<tr>
<td></td>
<td>1—INFO</td>
</tr>
<tr>
<td></td>
<td>2—CLEARED</td>
</tr>
<tr>
<td></td>
<td>3—WARNING</td>
</tr>
<tr>
<td></td>
<td>4—MINOR</td>
</tr>
<tr>
<td></td>
<td>5—MAJOR</td>
</tr>
<tr>
<td></td>
<td>6—CRITICAL</td>
</tr>
<tr>
<td>Name</td>
<td>An integer that represents the alarm as defined in the alarm-types.xml registry file. For example, 1 represents “Link Down.”</td>
</tr>
<tr>
<td>State</td>
<td>Short description of the event, such as “Port down due to card down.”</td>
</tr>
<tr>
<td>DetectionType</td>
<td>An integer that represents the event protocol type. Supported Detection Types are:</td>
</tr>
<tr>
<td></td>
<td>0—Service Event</td>
</tr>
<tr>
<td></td>
<td>1—Syslog Event</td>
</tr>
<tr>
<td></td>
<td>2—V1 Trap</td>
</tr>
<tr>
<td></td>
<td>3—V2 Trap</td>
</tr>
<tr>
<td></td>
<td>4—V3 Trap</td>
</tr>
</tbody>
</table>

This command adds a SeverityEnum property value to AOP 1:

```bash
# ./runRegTool.sh -gs 127.0.0.1 add 0.0.0.0
    site/event-global-filter/runningLevel1/SeverityEnum
```

**Step 3**  
Set a value for the event property. Events will be dropped when the property has that value.

```bash
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
    site/event-global-filter/runningLevel/propertyName/propertyValue ""
```

This command sets the SeverityEnum value to 1 in the Global Event Filter:

```bash
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
    site/event-global-filter/runningLevel1/SeverityEnum/1 ""
```

To remove a filter, use this procedure.

**Step 1**  
Log into the Prime Network gateway server as networkuser. (networkuser is the UNIX account for the Prime Network application, created when Prime Network is installed; for example, network39.)

**Step 2**  
Remove the filter from the registry using the following command.

*ID* is the AOP running level at which to drop events if they match the filter criteria, and *propertyName* is the event attribute to be checked by the filter:

```bash
# ./runRegTool.sh -gs 127.0.0.1 remove 0.0.0.0
    site/event-global-filter/runningLevel/propertyName ""
```

This command removes the filter created in the previous procedure:

```bash
# ./runRegTool.sh -gs 127.0.0.1 remove 0.0.0.0
    site/event-global-filter/runningLevel1/SeverityEnum ""
```
### Changing the IP Address of the Gateway Server

If you change the gateway IP address, 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.
- Stop all applications that are running on 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 change the IP address for a gateway server:

---

**Step 1**

Change the Solaris system settings on the gateway server. We recommend that you connect to the gateway server using the console port for a secure connection.

a. Change to the `/etc` folder:
   ```
   # cd /etc
   ```

b. Edit and save the following files in the `/etc` folder:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Required Change to File</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nodename</code></td>
<td>Add new gateway hostname below the existing entry.</td>
</tr>
<tr>
<td><code>hostname.network_if_name</code></td>
<td>Add new gateway hostname and IP address below the existing entry.</td>
</tr>
<tr>
<td><code>hosts</code></td>
<td>Add new gateway hostname and IP address below the existing entry.</td>
</tr>
<tr>
<td><code>netmasks</code></td>
<td>Add new IP address and subnet mask below the existing entry.</td>
</tr>
<tr>
<td><code>defaultrouter</code></td>
<td>Add new IP address below the existing entry.</td>
</tr>
</tbody>
</table>

c. Assign the new gateway IP address to the network interface using the `ifconfig` command in the following format:

   ```
   /sbin/ifconfig interface address
   ```

   For example, to set the `bge0` interface for the new address `172.23.241.1`:

   ```
   # /sbin/ifconfig bge0 172.23.241.1
   ```

d. Verify that the new IP address is configured on the gateway by checking that the address and hostname appear in the `ipnodes` file:

   ```
   # more /etc/inet/ipnodes
   ```
You should see output similar to the following. In this example, the hostname is newserver1.

```
# Internet host table
::1     localhost
127.0.0.1 localhost
172.23.241.1 ana-newserver1 loghost ana-newserver1.
172.71.163.2 sjlab1-nismaster.cisco.com
```

**Step 2** Change the gateway IP address for the Oracle server. These files reside on the machine where the database is located.

a. Go to the Oracle folder:
   ```
   # cd $ORACLE_BASE/network/admin
   ```

b. Edit and save the following files:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Required Change to File</th>
</tr>
</thead>
<tbody>
<tr>
<td>listener.ora</td>
<td>Replaced old gateway IP address with new IP address.</td>
</tr>
<tr>
<td>tnsnames.ora</td>
<td>Replaced old gateway IP address with new IP address.</td>
</tr>
</tbody>
</table>

c. Restart the Oracle database.

**Step 3** Start the `change_gw_ip.pl` script as follows:

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

ANA GW IP Update Utility
1. Update ANA Files.
2. Quit
Press Enter to choose.
```

**Step 4** Use your keyboard arrow keys to highlight Update ANA Files and press return.

**Note** 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/network39network39/Main/registry/persistency.xml
Updated: /export/home/network39/Main/registry/ConfigurationFiles/0.0.0.0/persistency.xml
Updated: /export/home/network39/Main/registry/ConfigurationFiles/127.0.0.1/persistency.xml
Updated: /export/home/network39/Main/registry/ConfigurationFiles/avm66.xml
Updated: /export/home/network39/Main/registry/ConfigurationFiles/avm0.xml
Updated: /export/home/network39/Main/registry/ConfigurationFiles/10.56.56.111/persistency.xml
Updated: /export/home/network39/Main/registry/ConfigurationFiles/10.56.56.111/avm0.xml
Updated: /export/home/network39/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/network39/Main/registry/persistency.xml
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.

---

### Gateway Open Sessions Registry Settings

The maximum number of gateway open sessions is controlled by a setting in the registry. The registry entry and default value are provided in Table 9-2.

**Note**

We recommend that you do not exceed the value of 150 maximum open sessions. All changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxOpenSessions</td>
<td>Maximum number of sessions that may be open with the gateway (includes both GUI client and BQL sessions)</td>
<td>150</td>
</tr>
</tbody>
</table>
Archiving and Purging Data

These topics provide basic information about data purging and archiving and system stability:

- **Prime Network Database Schemas, page 10-1**, describes the schemas supported by the Prime Network database and the main tables in the Fault Database and Event Archive schemas.
- **Archiving and Purging Data, page 10-4**, describes how the Prime Network integrity service and other mechanisms maintain system stability by checking for and purging old data.

**Note**

If you have installed an embedded database, see *Working With an Embedded Database, page 11-1* for additional information on how to administer it.

Prime Network Database Schemas

A Prime Network application operating system account is created when Prime Network is installed. When the database is created, it uses this operating system account name as the default for naming the schemas. Table 10-1 lists the database schemas that are created by Prime Network. It also provides examples of what the schema names would be if `network user` was defined as `network39` at installation time. You can also create the schemas manually, using different names, as described in the *Cisco Prime Network 3.9 Installation Guide*, but the purpose of each schema remains the same.

**Note**

Prime Network stores events in the database in Greenwich Mean Time (GMT). The Prime Network clients convert events to the time zone that is configured on the client’s workstation. As a best practice, use GMT (with 0 offset) on the gateway server.
## Prime Network Database Schemas

<table>
<thead>
<tr>
<th>Default Schema Names</th>
<th>Description</th>
<th>Example Schema Name</th>
</tr>
</thead>
</table>
| **network user**     | Prime Network main schema that contains most Prime Network data. This schema also contains the Fault Database (the tables that are related to the fault application):  
  - Network event tables—NETWORKEVENT, ALARM, and TICKET tables. Each of these tables contain an active partition and an archived partition, and the archived partitions are further divided into time-based subpartitions. Data in these three tables are never deleted; they are archived, either manually or automatically. When archived, the data is moved to an archive subpartition based on the object timestamp, and the data begins aging. When the archive exceeds its history size (14 days by default), the data is deleted.  
  - Non-network event tables—SYSTEMEVENT, AUDITEVENT, SECURITYEVENT, PROVISIONINGEVENT, NEWTRAPEVENT, NEWTRAPVALUE, MONITOR. Non-network tables contain only one time-based partition. Unlike tickets, they do not have lifecycle, so once created and saved, they begin aging. Like the network events tables, when the table exceeds its history size (14 days by default), the data is deleted.  
To change the settings that control when events are purged from the Fault Database, see Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6. A special process also purges tickets when the number of tickets exceeds its threshold; see How Fault Data is Auto-Archived in the Database, page 10-9. | **network39** |
| **network user_ep**  | Prime Network Event Archive (event persistence) schema that contains the following tables:  
  - HP_SYSLOG  
  - HP_TRAP  
The **network user_ep** schema contains all raw events that are sent from devices to Prime Network. Specifically, these raw events are received by the Event Collector (on AVM 100) and persisted in the Event Archive. The data is arranged in time-based partitions. When a partition’s age exceeds its history size (14 days by default), the data is deleted. You can disable event archiving using the procedure in Disabling and Re-Enabling Event Archiving, page 14-16.  
To change the settings that control when events are purged from the Event Archive, see Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6. | **network39_ep** |
| **network user_dwe** | Prime Network Workflow Engine schema that contains all data (templates and workflows) related to the Workflow Engine. The Workflow Engine is described in Workflow Administration Tasks, page 12-1. Workflows are deleted according to the workflowEngine integrity test; see Table 10-3 on page 10-6. | **network39_dwe** |
Table 10-1  Prime Network Database Schemas (continued)

<table>
<thead>
<tr>
<th>Default Schema Names</th>
<th>Description</th>
<th>Example Schema Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>network user</strong> <em>xmp</em></td>
<td>Prime Network Change and Configuration Management schema that contains all data related to the functions of Change and Configuration Management. This feature is optionally installed with Prime Network and is described in the <em>Cisco Prime Network 3.9 Installation Guide</em>. For more information on Change and Configuration Management, see the <em>Cisco Prime Network 3.9 Change and Configuration Management User Guide</em>.</td>
<td>network39_xmp</td>
</tr>
<tr>
<td><strong>network user</strong> <em>admin</em></td>
<td>User with database administrator permissions who can run maintenance tasks—such as gathering statistics—on the other Prime Network database schemas. If this user is created with the proper permissions (as described in the installation guide), Prime Network will run a cron job called <code>every_24_hours.cmd</code> that gathers statistics on other database tables. This provides an automatic method for generating database statistics, which is recommended for better performance. For more information, see the <em>Cisco Prime Network 3.9 Installation Guide</em>.</td>
<td>network39_admin</td>
</tr>
</tbody>
</table>

Table 10-2 lists the main tables used by the `network user` schema. They are listed here to aid in troubleshooting purposes (for example, if you see any missing statistics messages in the AVM 11 log (`NETWORK_HOME/logs/11.out`), they could be referring to tables that are no longer used by Prime Network).

Table 10-2  Database Tables in the `network user` Schema

<table>
<thead>
<tr>
<th>Primary Tables (Tables with More Traffic)</th>
<th>ALARM</th>
<th>NEWTRAPEVENT</th>
<th>SECURITYEVENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUDITEVENT</td>
<td>NEWTRAPVALUE</td>
<td>SEVERITYASPECT</td>
<td></td>
</tr>
<tr>
<td>NETWORKEVENT</td>
<td>NOTIFICATION</td>
<td>SYSTEMEVENT</td>
<td></td>
</tr>
<tr>
<td>NEWAFFECTEDSNC</td>
<td>PROVISIONINGEVENT</td>
<td>TICKET</td>
<td></td>
</tr>
</tbody>
</table>
Archiving and Purging Data

The Prime Network integrity service and several other mechanisms control how long data is saved and eventually purged (deleted) from the system. For fault data, there is an extra archiving mechanism for saving and tracking older data. These mechanisms are described in the following topics:

- How Data Purging Works, page 10-5
- Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6
- Customizing Purge Settings for Reports, page 10-8
- Automatic Purging of Old Jobs, page 10-9
- How Fault Data is Auto-Archived in the Database, page 10-9

If you have installed an embedded database, see Working With an Embedded Database, page 11-1 for information on additional checks that are performed by Prime Network. Data gathered by the Prime Network Monitoring tool is purged after 28 days as described in When Prime Network Monitoring Data is Purged, page 9-17.

### Table 10-2 Database Tables in the network user Schema (continued)

<table>
<thead>
<tr>
<th>Tables with Less Traffic</th>
<th>Tables with More Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOSRESULTS</td>
<td>MAP</td>
</tr>
<tr>
<td>BOSUSER</td>
<td>MAPASPECT</td>
</tr>
<tr>
<td>BUSINESSOBJECT</td>
<td>MAPDATAASPECT</td>
</tr>
<tr>
<td>CLIENTREGISTRY</td>
<td>MARTINITUNNELPEER</td>
</tr>
<tr>
<td>CONNECTIONTP</td>
<td>NETWORKPSEUDOWIRE</td>
</tr>
<tr>
<td>CUSTOMER</td>
<td>NETWORKVLAN</td>
</tr>
<tr>
<td>EFPCROSSCONNECT</td>
<td>NOTE</td>
</tr>
<tr>
<td>ETHERNETFLOWDOMAIN</td>
<td>OIDARRAYS</td>
</tr>
<tr>
<td>ETHERNETSERVICE</td>
<td>PASSWORDHISTORYENTRY</td>
</tr>
<tr>
<td>ETHFLOWPOINT</td>
<td>PERMISSION</td>
</tr>
<tr>
<td>EVC</td>
<td>PSEUDOWIREEDGE</td>
</tr>
<tr>
<td>HIERARCHYNODE</td>
<td>PWSWITCHINGENTITY</td>
</tr>
<tr>
<td>LCA</td>
<td></td>
</tr>
</tbody>
</table>

For more information on the Event Archive and Fault Database and the flow of events through Prime Network, see Managing the Event Collector (AVM 100), page 14-1. For information on how to change database passwords, see Changing Passwords: Prime Network Database Schemas, page 15-1.
How Data Purging Works

Prime Network maintains system stability by running cron jobs to maintain the database and eliminate clutter in the system, especially fault management data. Some jobs are run every 12 hours, while others are run every hour.

Different cron jobs are run on different schedules. To check the current schedules, use this procedure.

**Step 1**
Using an SSH session, log into the Prime Network gateway as network user. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

**Step 2**
Use the following command to list the contents of the crontab file for user network user. The local/cron directories listed below are all located in NETWORKHOME.

```bash
# crontab -l
# Cisco Prime Network crontab file
# contains scheduled tasks for user prime-network
* * * * * if [ -f local/cron/every_1_minute.cmd ]; then local/cron/every_1_minute.cmd > /dev/null 2>&1; fi
* * * * * /var/adm/cisco/prime-network/scripts/keep_alive_port_watchdog.pl > /dev/null 2>&1
0 * * * * if [ -f local/cron/every_1_hour.cmd ]; then local/cron/every_1_hour.cmd > /dev/null 2>&1; fi
0 4,16 * * * if [ -f local/cron/every_12_hours.cmd ]; then local/cron/every_12_hours.cmd > /dev/null 2>&1; fi
0 23 * * * if [ -f local/cron/every_24_hours.cmd ]; then local/cron/every_24_hours.cmd > /dev/null 2>&1; fi
0,10,20,30,40,50 * * * * if [ -f local/cron/every_10_minutes.cmd ]; then local/cron/every_10_minutes.cmd > /dev/null 2>&1; fi
```

(The port watchdog script is part of the AVM protection mechanism and is described in AVM 100 and Unit Server High Availability, page 16-3.)

If desired, you can modify when the jobs run by editing the crontab file. For example, the following line in the crontab file runs the file every_12_hours.cmd at 4:00 a.m. and 4:00 p.m.:

```
0 4,16 * * * local/cron/every_12_hours.cmd > /dev/null 2>&1
```

**Table 10-3** lists the integrity service checks that run on a regular basis to ensure system stability and purge old data. Prime Network performs archives and purges fault data according to the settings described in Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6.

If you have an embedded database, additional purging checks are performed as described in Purging Data and Checking Space on an Embedded Database, page 11-7. These settings are defined in the registry unless otherwise noted.
Chapter 10      Archiving and Purging Data

Archiving and Purging Data

Customizing Archive and Purge Settings for the Fault Database and Event Archive

The Event Management Settings window controls the following settings for both the Fault Database and the Event Archive:

- When archived data is deleted (purged)
- When database partitions are split

Every hour Prime Network monitors the size of tables in the Fault Database, deleting old data and splitting the partitions. These settings are controlled using Global Settings > Event Management Settings.

All database tables contain an active partition and an archived partition. Archived partitions are further divided into time-based subpartitions. When data is archived, it is moved to an archive subpartition. The archive partitioning and data purging is controlled by the settings in this window.

**Note**

To disable saving any raw events to the Event Archive, use the procedure in Disabling and Re-Enabling Event Archiving, page 14-16.

In addition the Inventory Event Viewer settings control when network and provisioning events are removed from the inventory event display Prime Network Vision. This display is launched when a user views a device’s inventory in Prime Network Vision, thus allowing users to see network and provisioning events (and tickets) on devices within their scope. By default, network and provisioning

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>analyze</td>
<td>Generates a System event if the period between the current date and the date each database table was analyzed is larger than the analyze-Period setting. Tables are analyzed every 30 days and includes all database tables. Archiving database logs is also enabled, and Prime Network saves a maximum of 10 database logs.</td>
</tr>
<tr>
<td>backup</td>
<td>Backs up the registry, encryption keys, and crontab files. By default, backups are saved to NETWORKHOME/backup. Backups are performed every 12 hours at 4:00 a.m. and 4:00 p.m. (Registry backup settings are described in Backup and Restore, page 8-1.)</td>
</tr>
<tr>
<td>businessObject</td>
<td>Checks for invalid OIDs in business objects. If more than two invalid business tags are found, Prime Network generates an event containing the list of OIDs.</td>
</tr>
<tr>
<td>capacity</td>
<td>Checks the disk space capacity and sends alarms. Alarms are sent when the disk capacity reaches 80% and 90%.</td>
</tr>
<tr>
<td>checkDbClock</td>
<td>Ensures that database clock is synchronized with the NTP server.</td>
</tr>
<tr>
<td>mapAspect</td>
<td>Removes mapAspect OIDs which are not connected to any hierarchy.</td>
</tr>
<tr>
<td>oidArrays</td>
<td>Removes OIDs which exist in the OidArrays table, but not in a parent table.</td>
</tr>
<tr>
<td>reports</td>
<td>Deletes reports after 90 days. (This setting is controlled in the Prime Network Administration GUI client; see Customizing Purge Settings for Reports, page 10-8).</td>
</tr>
<tr>
<td>unusableIndexes</td>
<td>Checks for unusuable table indexes and, if found, rebuilds them.</td>
</tr>
<tr>
<td>workflowEngine</td>
<td>Deletes all complete workflows after 7 days. For information on Prime Network Activation workflows and when they are deleted, see the Cisco Prime Network 3.9 Customization Guide.</td>
</tr>
</tbody>
</table>
events are removed from the display after 6 hours, and no more than 15,000 events are displayed. Users can also adjust this setting from their Prime Network Vision GUI client (using Tools > Options in their client). Changes made from the client will override the settings controlled from Prime Network Administration.

**Warning** Changing these settings can result in immediate and permanent removal of fault data.

**Step 1** Select Global Settings > Event Management Settings from Prime Network Administration.

**Step 2** Make your desired changes to the following settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault Database</td>
<td>Number of days after which archived events will be deleted from each archived database partition. The default is 14.</td>
</tr>
<tr>
<td>Database partition size (in hours)</td>
<td>Number of hours after which each database partition will be split. The default is 1 hour. (For database sizing guidelines and other capacity planning information, contact your Cisco account representative.)</td>
</tr>
<tr>
<td>Event Archive</td>
<td>Number of days after which archived events will be deleted from each archived database partition. The default is 14. To disable saving any raw events to the Event Archive, set this to 0 days.</td>
</tr>
<tr>
<td>Database partition size (in hours)</td>
<td>Number of hours after which each database partition will be split. The default is 1 hour. (For database sizing guidelines and other capacity planning information, contact your Cisco account representative.)</td>
</tr>
<tr>
<td>Inventory Event Viewer</td>
<td>Number of hours after which network and provisioning events are removed from the inventory event viewer in Prime Network Vision. The default is 6 hours. These settings are overridden if a user makes local changes to their Prime Network Vision GUI client (using Tools &gt; Options in their client).</td>
</tr>
</tbody>
</table>

**Step 3** Click Apply. The changes will take effect in the next partitioning process execution (which is done once an hour).

For information about the main menu that is displayed in the Prime Network window, see Event Management Settings Window, page 1-19.
Customizing Purge Settings for Reports

You can run different types of reports from the Prime Network window using the Reports main menu. This feature is described in the Cisco Prime Network 3.9 User Guide. The Report Settings page in the Global Settings drawer controls:

- When reports should be purged. Reports are saved in a gateway file system (in an intermediate format that is rendered to HTML or PDF when viewed). By default, they are purged after 90 days. This page also shows you how much space reports are currently consuming.

- Whether users can share reports (create public reports). If a report is public, all users can view the report; public reports are not filtered according to scopes or security privileges.

The settings do not affect user permissions for report actions such as adding, deleting, canceling, and so forth. Users can still perform all actions on reports they create; they can view other reports only if the reports are public. Administrators are the only users who can perform all actions on all reports.

Note: We recommend that you use these default settings in order to reduce system clutter. Allowing report data to accumulate could affect system performance.

To set up or change global report settings:

**Step 1** Choose Global Settings > Report Settings.

**Step 2** Configure the settings that control when reports will be purged from Prime Network, using dates, size, or both.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge Report After</td>
<td>Specifies how long to save a report. The time is measured from when the report is created. If you do not check this box, Prime Network defaults to 90 days. The Prime Network integrity service runs a job every 12 hours to purge all reports that exceed this age.</td>
</tr>
<tr>
<td>Store Reports Up to</td>
<td>Specifies the maximum disk size, in MB, at which reports should be purged. When this space setting is exceeded, Prime Network deletes the oldest reports (first in, first out). Prime Network runs a purge by size check every time a new report is created or a user changes the settings on this page. This feature is disabled by default.</td>
</tr>
</tbody>
</table>

If these settings are changed to lower values, after the changes are applied, Prime Network immediately deletes all reports that exceed the thresholds.

**Step 3** Check or uncheck the Enable Shared Reports check box to specify whether users can create public reports. When a report is public, all users can view the contents; reports are not filtered according to scopes or security privileges. Changes to this setting are applied to all subsequent new reports.

- If not selected, no users will be able to create public reports. Users will only be able to view their own reports.
- If selected, users have the option to create public reports and share them with other users.

**Step 4** Click Apply to immediately apply your settings.
After you click **Apply**, the report settings are applied to all existing and new reports. You can restore the Prime Network default settings at any time by clicking **Restore** and **Apply**.

For information about the main menu that is displayed in the Prime Network window, see Report Settings Window, page 1-25.

**Automatic Purging of Old Jobs**

The retention policy for job runs can be configured using the Job Manager Settings page. Old job runs which do not comply to the configured policy will be automatically purged as per the configured policy. The default policy will not purge any job until the administrator modifies the policy.

- **Note**: We recommend that you use these default settings in order to reduce system clutter. Allowing data to accumulate could affect system performance.

To set up or change Job Manager purge settings:

1. Choose **Global Settings > Job Manager Settings**.
2. Configure the settings that control when job runs will be purged from Prime Network, using dates, size, or both.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge Job Runs After</td>
<td>Specifies how long to save a job run. The time is measured from when the job run is created.</td>
</tr>
<tr>
<td>Store Reports Up to</td>
<td>Specifies the maximum number of job runs, after which job runs should be purged. When this number is exceeded, Prime Network deletes the oldest job runs (first in, first out). Prime Network runs a purge by size check every time a new job runs is created or a user changes the settings on this page. This feature is disabled by default.</td>
</tr>
</tbody>
</table>

If these settings are changed to lower values, after the changes are applied, Prime Network immediately deletes all job runs that exceed the thresholds.

3. Click **Apply** to immediately apply your settings.

After you click **Apply**, the job manager settings are applied to all existing and new job. You can restore the Prime Network default settings at any time by clicking **Restore** and **Apply**.

For information about the main menu that is displayed in the Prime Network window, see Job Manager Settings Window, page 1-20

**How Fault Data is Auto-Archived in the Database**

The NETWORKEVENT, ALARM, and TICKET database tables—that is, the tables that contain the events, alarms, and tickets that are in the Fault Database—each contain an active partition and an archived partition. The archived partitions further divided into time-based subpartitions. The archive operation moves data to an archive subpartition. Archived data is purged after 14 days, according to the setting in Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6.
Auto-Archiving of Cleared Tickets

Prime Network automatically archives cleared tickets which have not changed in the last hour. This setting is controlled in the registry.

\[\text{Note}\] All changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

### Table 10-4  Registry Settings for Automatic Archiving of Cleared Tickets

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoArchivingTimeout</td>
<td>Remove Cleared tickets that have not changed in this period of time (in milliseconds).</td>
<td>3600000 (1 hour)</td>
</tr>
</tbody>
</table>

**Step 1** Log into the gateway as *network user* and change to the Main directory by entering the following command. (*network user* is the operating system account for the Prime Network application, created when Prime Network is installed; for example, *network39*.)

\[\text{# \ cd \ $ANAHOME/Main}\]

**Step 2** To change the autoArchivingTimeout setting to 90 minutes:

\[\text{# \ ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 \ "site/plugin/AlarmPlugin/autoArchivingTimeout" \ 5400000}\]

**Step 3** Restart AVM 11 using *networkctl*.

Auto-Clearing of Tickets

Tickets older than the specified time and severity are automatically cleared by the system. This feature is disabled by default and can be enabled by selecting Event Management Settings > Auto-Clear Tickets.

To set up auto-clear ticket settings:

**Step 1** Choose Global Settings > Event Management Settings.

**Step 2** Select the Automatically clear Tickets to automatically clear tickets older than a predefined severity and days since last modified.

**Step 3** Configure the settings that clear the tickets after the set number of days for a predefined severity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Select severity of the tickets (Critical, Major, Minor, Warning) that should be cleared.</td>
</tr>
<tr>
<td>Day since last modification</td>
<td>Clears the ticket if the ticket was not modified for the specified number of days.</td>
</tr>
</tbody>
</table>

**Step 4** Click Apply to immediately apply your settings.
After you click **Apply**, the event management settings are applied to all existing and new events. You can restore the Prime Network default settings at any time by clicking **Restore** and **Apply**.

For information about the main menu that is displayed in the Prime Network window, see Event Management Settings Window, page 1-19

**Auto-Archiving Fault Data Based on the Number of Tickets**

Prime Network checks how many tickets are saved in the Fault Database to see if they should be archived, as follows:

- When the total number of tickets in the Fault Database exceeds 12,800, it generates a System event.
- When the total number of tickets in the Fault Database exceeds 16,000, it archives tickets in groups of 400.

Table 10-5 shows the registry parameters that control this type of Fault Database purging.

### Table 10-5 Registry Settings for Purging the Fault Database Based on Number of Tickets

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ticketRedThresholdAmount</td>
<td>When the number of open tickets surpasses this amount, archive the number of tickets specified by ticketArchivingBulk.</td>
<td>16000</td>
</tr>
<tr>
<td>ticketYellowThresholdPercentage</td>
<td>When the number of open tickets surpasses this percentage of ticketRedThresholdAmount, generate a system message.</td>
<td>80</td>
</tr>
<tr>
<td>wakeUpMessageInterval</td>
<td>Interval for checking the number of open tickets (in milliseconds).</td>
<td>60000 (1 minute)</td>
</tr>
<tr>
<td>ticketArchivingBulk</td>
<td>Alarm is generated once it crosses upper threshold after this many polling cycles.</td>
<td>400</td>
</tr>
</tbody>
</table>

If you have installed an embedded database, see the additional topics in Working With an Embedded Database, page 11-1.

**Auto-Archiving Fault Data Based on the Size of Tickets**

Every five minutes, Prime Network checks the Fault Database to see if it contains any large tickets that should be archived. A ticket is considered large if it has more than 150 events associated with an alarm. Prime Network does the following:

- If a large ticket is found, it generates a System event similar to the following:

  The system contains the following XXX ticket(s) with more than 150 events per alarm. You can manually archive these tickets or the system will automatically archive them in: 15 minutes
If the user does not respond within 15 minutes, Prime Network archives the tickets.

- If the agent finds more than 1500 large tickets then it will also send a system event notifying about it.

  There are more than X excessively large tickets in the system (tickets with more than 150 events per alarm).

Table 10-6 shows the registry parameters that control this type of Fault Database purging.

Note

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

For information on the format of the `runRegTool.sh` script, see Changing Registry Settings Using `runRegTool.sh`, page C-2.

Table 10-6  Registry Settings for Purging Large Tickets From the Fault Database

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>findLargeTicketsMessageInterval</code></td>
<td>Interval for searching for large tickets (in minutes).</td>
<td>5</td>
</tr>
<tr>
<td><code>maxTicketSize</code></td>
<td>When the number of events associated with an alarm surpasses this number, consider it a large ticket and generate a System event.</td>
<td>150</td>
</tr>
<tr>
<td><code>autoRemoveTimeInterval</code></td>
<td>Interval at which to archive a large ticket (in minutes) after sending System event.</td>
<td>15</td>
</tr>
<tr>
<td><code>oversizedTicketAmountLimit</code></td>
<td>When the number of large tickets surpasses this number, generate a System event.</td>
<td>1500</td>
</tr>
</tbody>
</table>

If you have installed an embedded database, see the additional topics in Working With an Embedded Database, page 11-1.
Working With an Embedded Database

Prime Network supports configurations with an embedded database. This configuration provides full integration of the Oracle database with Prime Network and allows you to use native tools to manage and monitor your database. These topics describe how to manage, back up, and restore configurations with an embedded database:

- Managing an Embedded Database, page 11-1
- Backing Up an Embedded Database and Prime Network, page 11-10
- Restoring an Embedded Database and Prime Network, page 11-13

Managing an Embedded Database

The following topics provide information about how to monitor your database:

- Monitoring an Embedded Database and Understanding Error Messages, page 11-2, explains error messages that you may observe.
- Using the emdbctl Utility to Manage the Embedded Database, page 11-3, explains how to use emdbctl to enable automatic backups, perform manual backups, restore backups, and so forth.
- Adding Additional Storage to an Embedded Database, page 11-5, explains how to add more storage to the database.
- Purging Data and Checking Space on an Embedded Database, page 11-7, describes the additional cron jobs that Prime Network performs to delete old data and maintain system stability.

Logs are available in the following locations ($ORACLE_BASE is the operating system database user’s home directory):

- $ANAHOME/Main/logs/emdb
- $ORACLE_BASE/ana_logs
Monitoring an Embedded Database and Understanding Error Messages

Prime Network monitors the database for the errors listed in Table 11-1. If an error occurs, Prime Network:

- Sends an e-mail alert to the address that was specified when the database was installed.
- Generates a system event that you can view in Prime Network Events.

The following example shows a sample e-mail alert.

Sample E-mail Alert
Subject: Urgent: Prime Network Database Error was encountered.
From: oracle@sh-nv210-266
Message:
The following error was generated by the database:
  Database error: ORA-00942: table or view does not exist
  Source: sh-nv210-266
  Process: 3963
  Program: sqlplus@sh-nv210-266(TNS V1-V3)
  DB user: network39_ADMIN
  SQL query:

Please contact the Cisco Technical Assistance Center (TAC).

Table 11-1 lists the errors that are generated if a problem is detected with any of the database functions. If you receive any of the following errors, contact the Cisco Technical Assistance Center (TAC).

### Table 11-1 Database Function Error Messages

<table>
<thead>
<tr>
<th>Error Code and Message</th>
<th>Possible Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA-00600 internal error code, arguments: [string], [string], [string], [string], [string], [string], [string]</td>
<td>This is the generic internal error number for Oracle program exceptions. This indicates that a process has encountered an exceptional condition.</td>
</tr>
<tr>
<td>ORA-00604 error occurred at recursive SQL level string</td>
<td>An error occurred while processing a recursive SQL statement (a statement applying to internal dictionary tables).</td>
</tr>
<tr>
<td>ORA-00050 operating system error occurred while obtaining an enqueue</td>
<td>Could not obtain the operating system resources necessary to cover an oracle enqueue. This is normally the result of an operating system user quota that is too low.</td>
</tr>
<tr>
<td>ORA-00052 maximum number of enqueue resources (string) exceeded</td>
<td>Ran out of enqueue resources.</td>
</tr>
<tr>
<td>ORA-00053 maximum number of enqueues exceeded</td>
<td>Ran out of enqueue state objects.</td>
</tr>
<tr>
<td>ORA-00055 maximum number of DML locks exceeded</td>
<td>Ran out of DML lock state objects.</td>
</tr>
<tr>
<td>ORA-00059 maximum number of DB_FILES exceeded</td>
<td>The value of the DB_FILES initialization parameter was exceeded.</td>
</tr>
<tr>
<td>ORA-00060 deadlock detected while waiting for resource</td>
<td>Transactions deadlocked one another while waiting for resources.</td>
</tr>
<tr>
<td>ORA-00250 archiver not started</td>
<td>An attempt was made to stop automatic archiving, but the archiver process was not running.</td>
</tr>
</tbody>
</table>
### Table 11-1   Database Function Error Messages (continued)

<table>
<thead>
<tr>
<th>Error Code and Message</th>
<th>Possible Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA-00255 error archiving log string of thread string, sequence # string</td>
<td>An error occurred during archiving.</td>
</tr>
<tr>
<td>ORA-00257 archiver error. Connect internal only, until freed.</td>
<td>The archiver process received an error while trying to archive a redo log. If the problem is not resolved soon, the database will stop executing transactions. The most likely cause of this message is the destination device is out of space to store the redo log file.</td>
</tr>
<tr>
<td>ORA-01033 ORACLE initialization or shutdown in progress</td>
<td>An attempt was made to log on while Oracle is being started up or shutdown.</td>
</tr>
<tr>
<td>ORA-01035 ORACLE only available to users with RESTRICTED SESSION privilege</td>
<td>Logins are disallowed because an instance started in restricted mode. Only users with RESTRICTED SESSION system privilege can log on.</td>
</tr>
<tr>
<td>ORA-01520 number of data files to add (string) exceeds limit of string</td>
<td>CREATE TABLESPACE statement specifies more files than is permitted for this database.</td>
</tr>
<tr>
<td>ORA-01536 space quota exceeded for tablespace 'string'</td>
<td>The space quota for the segment owner in the tablespace has been exhausted and the operation attempted the creation of a new segment extent in the tablespace.</td>
</tr>
<tr>
<td>ORA-01659 unable to allocate MINEXTENTS beyond string in tablespace string</td>
<td>Failed to find sufficient contiguous space to allocate MINEXTENTS for the segment being created.</td>
</tr>
<tr>
<td>ORA-27100 shared memory realm already exists</td>
<td>Tried to start duplicate instances, or tried to restart an instance that had not been properly shutdown.</td>
</tr>
<tr>
<td>ORA-27102 out of memory</td>
<td>—</td>
</tr>
<tr>
<td>ORA-27103 internal error</td>
<td>—</td>
</tr>
<tr>
<td>ORA-27146 post/wait initialization failed</td>
<td>OS system call failed.</td>
</tr>
</tbody>
</table>

### Using the emdbctl Utility to Manage the Embedded Database

If you are using RHCS/ADG or Veritas gateway server high availability, freeze the cluster services *before* using `emdbctl` with the `stop`, `start`, `restore`, `restore_db`, or `enable_backup` options. These options will stop and restart the cluster services. If the cluster is running and detects that the services are down, it may attempt to restart them. When used with Oracle ADG, reconfigure the database replication after restoring the primary DB. For more information on replication process, see Oracle ADG Replication Process and Configuration Files, page 18-9.

You can use the `emdbctl` command to perform embedded database backup and restore operations, collect logs and reports, and other administrative actions. The `emdbctl` command is located in `NETWORKHOME/Main/scripts/embedded_db`. It takes the following options:

```
emdbctl [ --start | --stop | --backup | --enable_backup | --restore | --restore_db | --collect | --change_backup_time | --install_db_sec_patch]
```
Chapter 11  Working With an Embedded Database

Managing an Embedded Database

You must be logged in as network user to use this command. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; an example of network user is network39.)

The following illustrates an example session of the emdbctl start and stop options:

```
# emdbctl --stop
Stopping Prime Network
Stopping NCCM DM Server...
- DM server is up, about to shut it down
- Sent graceful shutdown command to the dm Server (pid 25499), waiting for 2 seconds
- Checking if DM server is still up (1st)
- The DM Server is down
AVM unregistered successfully
Stopping AVMs.....Done.
Stopping the database and listener
#
# emdbctl --start

- Starting the database and listener
- Starting MVM..........................................................Done.
- Starting Gateway ..............................................................Done.
```

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--stop</td>
<td>Stops Prime Network on the gateway and units, and stops the embedded database services and listener.</td>
</tr>
<tr>
<td>--start</td>
<td>Starts the embedded database services and listener, and starts Prime Network on the gateway and units (if the units are down)</td>
</tr>
<tr>
<td>--backup</td>
<td>Backs up the embedded database and Prime Network, including the registry. For more information, see Backing Up an Embedded Database and Prime Network, page 11-10.</td>
</tr>
<tr>
<td>--restore</td>
<td>Restores the embedded database and Prime Network, including the registry using valid backup files. For more information, see Restoring an Embedded Database and Prime Network, page 11-13</td>
</tr>
<tr>
<td>--restore_db</td>
<td>Restores the embedded database only.</td>
</tr>
<tr>
<td>--enable_backup</td>
<td>Enables the automatic backup mechanism. See Enabling Backups (Embedded Database), page 11-11.</td>
</tr>
<tr>
<td>--collect</td>
<td>Collects embedded database logs and reports. It collects logs and trace files from the database server, runs a database diagnostic tool, zips the output together, and copies it to the gateway at NETWORKHOME/Main/logs/emdb/ana_collector.zip. It can be run alone or as part of the artifacts of the ANA Profiler Tool (available from the Cisco Developer Network).</td>
</tr>
<tr>
<td>--change_backup_time</td>
<td>Allows to change the database backup time. See Changing the Database Backup Time, page 11-12</td>
</tr>
<tr>
<td>--install_db_sec_patch</td>
<td>Allows to update the database security patches after the install or the upgrade. See Installing the Security Patches, page 11-13</td>
</tr>
</tbody>
</table>
Adding Additional Storage to an Embedded Database

Prime Network provides two utilities for adding additional storage to an embedded database:

- To add storage to the entire database, see Adding Datafiles to the Database (add_emdb_storage.pl), page 11-5.
- To add storage to a specific tablespace, see Adding Datafiles to a Specific Tablespace (add_storage_for_tablespace.pl), page 11-6.

Adding Datafiles to the Database (add_emdb_storage.pl)

Use the add_emdb_storage.pl script to add database files according to the database size you estimate you will need. When you use these scripts you will be prompted to enter your database profile (the estimated database capacity) and the history size for events and workflows. This enables the script to calculate the maximum size of the database, and to create the data files, temp files, and redo logs.

If you need assistance estimating the database size, contact your Cisco representative. The representative can provide the Memory Assessment Tool to help you with the sizing.

**Step 1**
Log into the Prime Network gateway as network user. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

**Step 2**
Change directories to NETWORKHOME/Main/scripts/embedded_db and enter the following command:

```
./add_emdb_storage.pl
```

**Step 3**
Enter the appropriate response at the prompts:

- Writing log to /export/home/network39/Main/logs/emdb/add-storage-xxx.log
- Retrieving registry information & initializing connection
- How would you estimate your DB profile?

1) 1 actionable events per second (POC/LAB deployment)
2) Up to 5 actionable events per second
3) Up to 20 actionable events per second
4) Up to 50 actionable events per second
5) Up to 100 actionable events per second
6) Up to 200 actionable events per second
7) Up to 250 actionable events per second

1-7 [default 1]

- Insert the event archiving size in days. Prime Network default archive is 14 days: [default 14]
- Insert the workflow archiving size in days. Prime Network default archive is 7 days: [default 7]

**Note**
If you enter incorrect values—such as the wrong database profile estimate—you can rerun the script with different inputs.

If you encounter any errors, messages similar to the following examples are displayed.

- If there is not enough disk space to create the additional database files or redo logs:
  - There isn’t enough space on the current disks to create an additional of 6144 MB. Please enter a new location for creating the remaining DB files. Before you continue:
    1. Verify user <os-db-user> has writing permissions on the new location or run the following command as the OS root user:
       chown -R <os-db-user>:oinstall <path>
2. Verify the new location is mounted as UFS with 'forcedirectio' option

New location:

Enter another location.

- If the files or redo logs cannot be created for any reason, you will see an error message and the following prompt:

  - How would you like to continue?
    1) Retry
    2) Skip (move to the next in list)
    3) Abort
    (1 - 3) [default 1]

For example, if the correct permissions were not set, you would see the following.

Failed to add datafile for network39:
-1119: ORA-01119: error in creating database file '/2del/network39_DATA11.dbf'
ORA-27040: file create error, unable to create file
Linux-x86_64 Error: 13: Permission denied

The menu choices provide you with an opportunity to fix the permissions and retry creating the file or log.

The log file is located in NETWORKHOME/Main/logs/emdb/add-storage-time-stamp.log.

Adding Datafiles to a Specific Tablespace (add_storage_for_tablespace.pl )

Use the add_storage_for_tablespace.pl script to add database files to a specific tablespace.

**Before You Begin**

You will need the following information to use this script:

- The name of the tablespace that requires more datafiles. You can get this from the System event described in Tablespace Usage on Database Server, page 11-9.
- Additional space required for the above tablespace.
- The full directory name where the new datafiles will be created.

This example adds tablespace to the network39 database schema.

**Step 1**

Log into the Prime Network gateway as network user. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

**Step 2**

Change directories to NETWORKHOME/Main/scripts/embedded_db and enter the following command:

```
# ./add_storage_for_tablespace.pl
```

or enter the following command to provide all the information in advance

```
#./ add_storage_for_tablespace.pl  --tablespace <tablespace_name>  --space <additional_required_space_in_MB> --location <additional location>
```

For example:
Step 3 Enter the appropriate response at the prompts when `./add_storage_for_tablespace.pl` command is used.

This script will add an additional datafile for a certain tablespace in the DB

+Retrieving registry information & initializing connection
+Choose one of the following Prime Network tablespaces to add datafiles to:

<table>
<thead>
<tr>
<th>TABLESPACE_NAME</th>
<th>FREE_SPACE_MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNDOTBS1</td>
<td>1992.25</td>
</tr>
<tr>
<td>NETWORK39_DWE</td>
<td>1018.375</td>
</tr>
<tr>
<td>NETWORK39_XMP</td>
<td>1009.625</td>
</tr>
<tr>
<td>NETWORK39_EP</td>
<td>928.6875</td>
</tr>
<tr>
<td>NETWORK39</td>
<td>271.8125</td>
</tr>
<tr>
<td>NETWORK39_ADMIN</td>
<td>98.375</td>
</tr>
<tr>
<td>SYSAX</td>
<td>37.375</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>6.75</td>
</tr>
<tr>
<td>USERS</td>
<td>3.6875</td>
</tr>
</tbody>
</table>

- Enter tablespace name: NETWORK39

+Choose one of the following locations for the new datafile/s to be created at:

- Enter location: /export/home/oracle/oradata/anadb/

- Enter the required size in MB (For Example: 1000): 100

+About to add 100 MB to network39 on /export/home/oracle/oradata/anadb/
Successfully added 100 M on /export/home/oracle/oradata/anadb/ to network39

The log file is located in `NETWORKHOME/Main/logs/emdb/add-storage-to_tbs-time-stamp.log`.

---

**Purging Data and Checking Space on an Embedded Database**

Prime Network performs a variety of tests and checks to maintain system stability; these are described in Archiving and Purging Data, page 10-4. If an embedded database is installed, Prime Network performs the following additional cron jobs.

<table>
<thead>
<tr>
<th>Detail of Cron Job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitors disk usage on database server</td>
<td>Hourly job that generates a System event and an e-mail notification if the database disk usage exceeds these thresholds: 50%, 70%, 80%. For more details, see Disk Usage on Database Server, page 11-8.</td>
</tr>
<tr>
<td>Checks available space in the tablespaces</td>
<td>Hourly job that generates a System event and an e-mail notification if the tablespace usage exceeds these thresholds: 80%, 90%. For more details, see Tablespace Usage on Database Server, page 11-9.</td>
</tr>
</tbody>
</table>
Managing an Embedded Database

An hourly cron job checks the available database disk space on the server that is hosting the database. These disks are used for data files, redo logs, backup files, and so on. If more than 50% of the disk space is in use, Prime Network generates a System event and an e-mail notification. The System event has the following format:

The directory-type directory (full-pathname) has reached x% of its space. If this is unexpected, please refer to the Cisco Prime Network Administrator Guide.

The event severity depends on how much space is used:

<table>
<thead>
<tr>
<th>Disk Space Used</th>
<th>Event Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>50-70%</td>
<td>Warning</td>
</tr>
<tr>
<td>70-80%</td>
<td>Minor</td>
</tr>
<tr>
<td>80% and above</td>
<td>Major</td>
</tr>
</tbody>
</table>

The e-mail notification has a similar format, as shown in the following example:

Subject: Prime Network database disk usage alert!
From: oracle@gkleinma-vmsim-05.cisco.com
The Database’s Redo Logs directory (/export/home/oracle/redo/) has reached 58% of its space. If this is unexpected, please refer to the Cisco Prime Network Administrator Guide.

Prime Network generates one System event when any database directory exceeds any of the thresholds listed in the previous table. It will generate another event (one hour later, at the next cron job) if:

- The same directory’s disk usage surpasses the next threshold.
- Another directory’s disk usage surpasses any threshold.

The same cron job is repeated one hour later. If the disk space is unchanged, no new System events are generated.

If the problem continues, you can do the following:

1. Ask your system administrator to add disk space to the relevant file systems.
2. If more disk space cannot be added, contact the Cisco Technical Assistance Center for information on how to reduce history size. This will not change the disk usage, but will eliminate the need to add disk space.
Tablespace Usage on Database Server

An hourly cron job checks the available space in the database tablespaces. Each tablespace has two configurable thresholds: for 80% of capacity, and for 90% of capacity. The tablespaces that are checked are listed in NETWORKHOME/Main/scripts/embedded_db/cron/TS_ALERTS.prm.

Note

You can change the thresholds by editing the TS_ALERTS.prm file. Prime Network will use the new threshold numbers when it performs the next hourly cron job.

If a tablespace exceeds its capacity, Prime Network Prime adds a new data file to the tablespace and generates a System event and an e-mail notification. If the operation was successful, the System event has the following format:

tablespace-name tablespace was x% full. Cisco Prime Network resolved this by adding x MB to this tablespace.

If the operation fails, the System event has the following format

tablespace-name tablespace is x% full. Cisco Prime Network tried, but failed to add storage to this tablespace. If this is unexpected please refer to the Cisco Prime Network Administrator guide

The event severity depends on how much space is used:

<table>
<thead>
<tr>
<th>Disk Space Used</th>
<th>Event Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>80-90%</td>
<td>Minor</td>
</tr>
<tr>
<td>90% and above</td>
<td>Major</td>
</tr>
</tbody>
</table>

The e-mail notification has a similar format, as shown in the following example:

Subject: Prime Network database tablespace usage alert!
From: network39@kleinma-vmsim-05.cisco.com
TEST tablespace was 92.4623116 % full.
Cisco Prime Network resolved this by adding 44.7 MB to this tablespace.

Prime Network will generate an hourly System event until the problem is fixed.

If the problem continues, do the following:

1. If you have the required disk space, add data files using the add_storage_for_tablespace.pl utility.
   See Adding Datafiles to a Specific Tablespace (add_storage_for_tablespace.pl), page 11-6.
2. Contact the Cisco Technical Assistance Center.
Backing Up an Embedded Database and Prime Network

The following topics explain the backup mechanism used for an embedded database.

- **Overview of the Backup Procedure (With Embedded Database), page 11-10**
- **Enabling Backups (Embedded Database), page 11-11**
- **Performing a Manual Backup of an Embedded Database and Prime Network, page 11-12**
- **Changing the Database Backup Time, page 11-12**

### Overview of the Backup Procedure (With Embedded Database)

The backup procedure follows the same guidelines as those described in Overview of the Backup Procedure, page 8-1, with the following changes and additions for an embedded database.

#### When Backups Are Performed

Backups are automatically performed if you enabled the backup mechanism either during installation or by using the procedure in Enabling Backups (Embedded Database), page 11-11. The backup procedure for installations with an embedded database consists of a two backups:

- Prime Network data (registry, encryption keys, reports, and so forth), which is backed up according to the description in Overview of the Backup Procedure, page 8-1.
- Embedded database, which is backed up according to the profile selected at installation:
  - **1-50 actionable events per second** — Full backup is performed every Saturday at 1:00 a.m.; and incremental backups are performed every Sunday-Friday at 1:00 a.m.
  - **51-250 actionable events per second** — Full backup is performed every Tuesday and Saturday at 1:00 a.m.

#### How Many Backups Are Saved

By default, Prime Network saves database backups taken in last 8 days and 16 Prime Network data backups. For this reason you must back up the database’s backup and archive directories to tape on a daily basis.
Where Backups Are Stored

The backup is stored in the location selected at installation time. You cannot modify these settings.

Enabling Backups (Embedded Database)

The following procedure enables the backup mechanism for an embedded database. You must enable the mechanism if you want to perform manual or automatic backups. This procedure requires both Oracle and Prime Network to be restarted.

Before You Begin

The script will prompt you for the following information:

- The destination folders for the backup files and the archive log
- Your database profile.

To enable the backup mechanism for an embedded database:

Step 1

If you did not specify a backup location at installation time, do the following:

a. Create the folders for the backup files and the archive logs.

b. Verify that the OS database user (oracle, by default) has write permission for the folders, or run the following command as the operating system root user:

```
chown -R os-db-user:oinstall path
```

Step 2

Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39). Change the directory to the Main/scripts/embedded_db directory:

```
# cd $ANAHOME/Main/scripts/embedded_db
```

Step 3

Start the backup.

```
# emdbctl --enable_backup
```

The following is an example of a complete --enable_backup session.

```
# emdbctl --enable_backup
   Reading Prime Network registry
   - Enter the destination for the backup files:/export/home/oracle/backup
   You must create the target destination (path-to-backup-dir) before you continue
   - Enter the destination for the archive log:/export/home/oracle/arch
   - How would you estimate your database profile?
     -----------------------------------------------
     1) 1 actionable events per second (POC/LAB deployment)
     2) Up to 5 actionable events per second
     3) Up to 20 actionable events per second
     4) Up to 50 actionable events per second
     5) Up to 100 actionable events per second
     6) Up to 200 actionable events per second
     7) Up to 250 actionable events per second
     (1 - 7) [default 1] 1
   Updating Prime Network registry
   Stopping Prime Network
```
Performing a Manual Backup of an Embedded Database and Prime Network

If you have installed an embedded database, you can perform a backup using the following procedure. The backup will contain the following data:

- Prime Network embedded database
- Prime Network data that is listed in Which Files Are Backed Up, page 8-1

This procedure uses the `emdbctl` command, which is described in Using the emdbctl Utility to Manage the Embedded Database, page 11-3. By default, the information is backed up to the location specified at installation time. For information on backups, see Overview of the Backup Procedure (With Embedded Database), page 11-10.

**Before You Begin**
The automatic backup mechanism must be enabled. If you did not enable it during the installation, follow the directions in Enabling Backups (Embedded Database), page 11-11.

**Step 1**
Log into the gateway as `network user` (where `network user` is the operating system account for the Prime Network application, created when Prime Network is installed; for example, `network39`).

**Step 2**
Change the directory to the `Main/scripts/embedded_db` directory:

```
# cd $ANAHOME/Main/scripts/embedded_db
```

**Step 3**
Start the backup:

```
# emdbctl --backup
  Reading Prime Network registry
  Backing up the database
  Backing up Prime Network
```

Changing the Database Backup Time

The following procedure enables to reschedule the database backup time for an embedded database. This procedure uses the `emdbctl` command, which is described in Using the emdbctl Utility to Manage the Embedded Database, page 11-3.
Chapter 11  Working With an Embedded Database

Step 1  Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39).

Step 2  Change the directory to the Main/scripts/embedded_db directory:

```
# cd $ANAHOME/Main/scripts/embedded_db
```

Step 3  Change the database backup time:

```
# emdbctl --change_backup_time
Reading Prime Network registry
Configuring the DB backup time
Please enter the new hour for the DB Backup (0..23) : 3
Please enter the new minute for the DB Backup (0..59) : 19
DB backup time was changed successfully
```

Installing the Security Patches

The following procedure allows you to install the database security patches after the install or the upgrade for an embedded database. This procedure uses the emdbctl command, which is described in Using the emdbctl Utility to Manage the Embedded Database, page 11-3.

Step 1  Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39).

Step 2  Change the directory to the Main/scripts/embedded_db directory:

```
# cd $ANAHOME/Main/scripts/embedded_db
```

Step 3  Change the database backup time:

```
# emdbctl --install_db_sec_patch
```

```
network39@sh-t1000-00k [~/Main/scripts/embedded_db]% ./emdbctl --install_db_sec_patch
Installing July 2011 DB security patch
Make sure Prime Network is down
This may take around 90 minutes, Do you want to continue (Y/N) ? Y
Security Patch installation completed successfully, Please start Prime Network
```

Restoring an Embedded Database and Prime Network

The restore procedure for installations with an embedded database consists of two restorations:

- Restoring the embedded database to any hour within a valid backup file.
- Restoring Prime Network data (registry, encryption keys, and so forth) to the point when the backup was taken.

By default, the Prime Network data is backed up twice a day at 4:00 a.m. and 4:00 p.m. and can be restored to only those points in time. But the embedded database backups are scheduled according to the database size, and can be restored to any hour within the last 8 days, as described in When Backups Are Performed, page 11-10. Therefore, you should consider finding out the time and date of the latest Prime Network data backup, and restoring the data and your database to that time.
You do not have to stop Prime Network, the database, or any other processes before performing the restore operation. The script will do this for you. You can use this restore procedure even if the database is down.

To restore the embedded database and Prime Network data:

**Step 1** Log into the gateway as `network user` (where `network user` is the operating system account for the Prime Network application, created when Prime Network is installed; for example, `network39`).

**Step 2** Change to the directory `NETWORKHOME/Main/scripts/embedded_db`:

```
# cd $ANAHOME/Main/scripts/embedded_db
```

**Step 3** Execute the restoration script:

```
# ./emdbctl --restore
```

Please enter the date and time information for the restore process

- Restore year (YYYY) : 2012
- Restore month (1..12) : 5
- Restore day (1..31) : 10
- Restore hour (0..23) : 7
- Restore minute (0..59) : 00

Selected Restore time (MM-DD-YYYY HH:MI): 05-10-2012 07:00

In case of a wrong or impossible date for restore, the DB will be restored to the latest possible point in time

Do you want to continue (Y/N) ? Y

Stopping Prime Network
Stopping AVMs....Done.

Restoring the database to 05-10-2012 07:00
Successfully restored the database!

Restoring Prime Network
Enter Prime Network's backup directory (the default location is $ANAHOME/backup/date+time): /export/home/network39/backup/20120510040

Checking that the system is down...
Prime Network not running on the gateway
Backup_dir: /export/home/network39/backup/20120510040
Backing-up current registry to /export/home/network39/backup_before_restore.jar
Restoring registry
Restoring to_backup
Before restoring encryption key, backing up last installation encryption key
Restoring encryption key
Before restoring reports, backing up current reports
Restoring reports
Setting Main/registry ownership
Setting Main/reportfw/rptdocument ownership
Done

Would you like to start Prime Network? (yes,no) [default yes] no

**Step 4** Once all of your data is restored, restart the gateway.
Workflow Administration Tasks

These topics briefly describe workflows and how to administer the stored workflows and templates in Prime Network Administration:

- Workflows and the Workflow Engine Windows, page 12-1
- Viewing and Deleting Templates, page 12-3
- Viewing and Administering Workflows, page 12-4

For more information about the Workflow Engine window elements, see Workflow Engine Windows, page 1-33.

Workflows and the Workflow Engine Windows

Workflows are logical flows of atomic tasks (activation commands) that often include complex rollback scenarios. The logic enables you to define relationships between tasks, the sequence of tasks, when to branch to other tasks, and what to do if a task fails.

You can create workflows using the Prime Network Workflow Editor. You can also use the service activation workflows that are provided with Prime Network Activation. For more information on these tools, see the *Cisco Prime Network 3.9 Customization User Guide*. You do not have to perform any special tasks to allow users to manage workflows.

Once they are created, all templates and workflows are displayed in the Workflow Engine windows in Prime Network Administration. The Workflow engine resides on the Prime Network gateway using AVM 66.

By default, base workflows (as opposed to Prime Network Activation workflows) are saved for seven days and are then purged from Prime Network by the integrity service. Templates and workflows are saved in the database under the `network user_dwe` schema. For information on how long Prime Network Activation workflows are saved, see the information on purging workflows in the *Cisco Prime Network 3.9 Customization Guide*.

The Workflow Engine windows include the following:

- Templates—Displays a list of the deployed workflow templates and enables you to view the properties of a workflow template.
- Workflows—Displays a search window from which you can locate and display the workflows in which you are interested, including workflow properties and output.

Figure 12-1 presents the process required when working with and managing workflows. The tasks are described in the order in which they must be performed.
Figure 12-1  Flow For Creating, Testing, Deploying, Running, and Viewing a Workflow

Step 1: Create a command using Command Builder and preview it

Step 2: Define tasks and workflows using the Workflow Editor

Step 3a: Copy the command descriptor scripts
Step 3b: Edit the command descriptor scripts
Step 3c: Add workflow and task attributes

Step 4: Test the workflow locally

Step 5: Deploy the workflow on the gateway

Step 6: Run the workflow

Step 7: View the workflow in Prime Network Administration

Step 8: View the workflow results in Prime Network Events
Viewing and Deleting Templates

You can perform the following template management tasks from Prime Network Administration:

- Viewing Available Workflow Templates and Their Properties, page 12-3
- Deleting a Workflow Template, page 12-3

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

**Viewing Available Workflow Templates and Their Properties**

To view the list of templates and template properties:

**Step 1** Choose Workflow Engine > Templates. The list of all workflow templates is displayed in the table.

**Step 2** Right-click a template, then choose Properties. The Workflow Template window displays an alphabetical list of the templates in the system.

**Step 3** Click in the top right-hand corner to close the Template Properties dialog box.

**Deleting a Workflow Template**

Deleting a workflow template permanently removes the template from the Prime Network system. To delete a workflow template:

**Step 1** Choose Workflow Engine > Templates. The list of workflow templates is displayed in the table.

**Step 2** Right-click a workflow template, then choose Delete. A warning message is displayed.

**Step 3** Click Yes. The selected workflow template is deleted and no longer appears in the table.
Viewing and Administering Workflows

When you perform workflow operations from Prime Network Administration, you have access to all workflows that are stored in the system. This is different from performing these same operations from Prime Network Vision, where you can only access Prime Network Activation workflows.

These topics describe how to search for and manage the workflows that are in the Prime Network Administration system.

- Searching for Workflows, page 12-4
- Viewing Workflows, Workflow Properties, and Workflow Output, page 12-5
- Aborting and Deleting Workflows, page 12-6
- Adjusting the Performance of Workflow Searches, page 12-6

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

**Searching for Workflows**

When you choose **Workflow Engine > Workflows**, Prime Network displays a workflow search tool you can use to view specific workflows. This tool is useful because the system can easily contain thousands of workflows. (The actual number of workflows in the system is indicated by the counter in the top left of the workflow search window.)

To improve performance, you can adjust the total number workflows that are returned in any search result. By default the value is set to 5,000 workflows. To change this value, use the procedure described in Adjusting the Performance of Workflow Searches, page 12-6.

This procedure explains how to use the workflow search tool.

---

**Step 1** Choose **Workflow Engine > Workflows** to display the workflow search tool.

**Step 2** In the Execution Time area, enter the time period you want to search. By default the current day is selected. (This is a required field.)

**Step 3** In the Match area, enter the criteria you want the search to match.

**Note** If you want to search by date only, choose **None** from the Match drop-down list.

a. Select the Match operator:
   - None—Return the workflow if it does not match any of the rules. This is normally used if you want to perform a search based only on a time frame.
   - Any—Return the workflow if it matches any of the rules.
   - All—Return the workflow if it matches all of the rules. You must enter

b. Create a rule by selecting an attribute, operator, and value. The operators and values that are displayed depend on the attribute you select. Values are case-insensitive; wild cards are not supported.
Note
Fully-populated results are returned only if the utility can match an attribute with information in the database. If the search results table contains empty fields (for example, some IP address fields are empty), this means the attributes were either not included in the workflow/service (and are not in the database), or the attribute search criteria was not correctly entered (with an operator and value).

Step 4
Click Search to display the results. The timestamp above the table indicates when the query was executed (the results are a snapshot of the data at that time and are not updated unless the search is rerun). You can filter the table of results by using the tools that are directly above the table.

The table information is described in Viewing Workflows, Workflow Properties, and Workflow Output, page 12-5.

The following buttons are also provided:
- Previous Criteria—Displays the criteria settings from the previous search.
- Clear—Clears all table data and criteria from the previous search.

Viewing Workflows, Workflow Properties, and Workflow Output
When you choose Workflow Engine > Workflows, Prime Network displays a tabular list of all workflows sorted according to their Workflow ID. The total number of workflows in the Prime Network system is listed at the top left of the window. This counter that is updated whenever a workflow is deleted or added to the system.

Step 1
Choose Workflow Engine > Workflows to display the workflow search tool.

Step 2
Perform a query as described in Searching for Workflows, page 12-4.

The table of workflows lists the following data. To filter the table data, use the tool buttons provided above the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow ID</td>
<td>Unique identifier for the workflow (assigned by Prime Network).</td>
</tr>
<tr>
<td>Template Name</td>
<td>Name of the template used by this workflow. (All Prime Network Activation templates are indicated by the prefix NSA_.)</td>
</tr>
<tr>
<td>Template Display Name</td>
<td>Name as displayed in Prime Network.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the workflow.</td>
</tr>
<tr>
<td>Execution Time</td>
<td>When the workflow was started.</td>
</tr>
<tr>
<td>User</td>
<td>User that executed the workflow.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Devices affected by the workflow. This data is gathered from workflows that contain any DeviceName* attributes.</td>
</tr>
<tr>
<td>Device IP</td>
<td>IP address of devices affected by the workflow. This data is gathered from workflows that contain any DeviceIP* or IPAddress* attributes.</td>
</tr>
<tr>
<td>Information</td>
<td>Informational data supplied when the workflow was created. This data is gathered from workflows that contain any <em>Info</em> attributes.</td>
</tr>
</tbody>
</table>
Step 3  To view a workflow’s properties, right-click the workflow, then choose **Properties**. The Properties window displays all of the workflow attributes and their values. (This is different from viewing Prime Network Activation workflow output from Prime Network Vision, where only a limited number of attributes are displayed.)

Step 4  To view a workflow’s output, right-click the workflow, then choose **Show Output**. The Output window displays the commands that were sent, progress messages, script results, and so forth.

---

**Aborting and Deleting Workflows**

When a workflow is aborted, Prime Network rolls back all activation scripts that have already been run (by Execute BQL tasks). A workflow rollback has the following characteristics:

- The commands that are executed are those that are defined in the rollback section of the script (defined in Command Builder).
- Scripts are rolled back in the reverse order of their execution.

**Note**  Gateway commands do not support rollback.

A workflow is also aborted automatically if any of its tasks are aborted.

Rollback can be disabled for specific BQL tasks by setting the RollbackEnabled value task attribute to false in the respective BQL task. This is useful for a BQL task executing a script that does not have an appropriate rollback, or a BQL task executing a gateway command.

When a workflow is deleted, it is removed from the database.

To abort a running workflow, or delete a workflow:

**Step 1**  Choose **Workflow Engine > Workflows** to display the workflow search tool.

**Step 2**  Use the workflow search tool to locate the workflows in which you are interested. For more information, see **Searching for Workflows**, page 12-4.

**Step 3**  Right-click the workflow and perform the appropriate action:

- **Abort** to roll back all scripts that have run to that point. The workflow remains in the system but its state is changed to Aborted.
- **Delete** to remove the workflow from the system.

**Step 4**  Click **Yes** in response to the confirmation message.

---

**Adjusting the Performance of Workflow Searches**

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

By default, the maximum number of search results displayed is 5,000. You can adjust this to a lower number to get faster results. We do not recommend entering a value higher than 5,000 because this can negatively impact the performance of the search tool.

For information on the format of the **runRegTool** command, see **Changing Registry Settings Using runRegTool.sh**, page C-2.
Step 1  Log into the gateway server as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; an example of network user is network39).

Step 2  Change to the Main directory:

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

Step 3  Enter the following command to adjust the total workflow search results that are displayed by the GUI client:

```
runRegTool.sh -gs gw-IP set unit-IP "site/cvm/management/workflow/searchResultMaxRawSize" value
```

This example changes the maximum results 1,000 workflows:

```
# runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/cvm/management/workflow/searchResultMaxRawSize" 1000
```

The change is applied to all GUI clients that connect to the gateway. For open GUI clients, close and reopen them to apply the change.
System Security

These topics describe the major security features of Prime Network and their configurable points:

- Communication Security, page 13-1
- Device Communication Security: SSH and SNMPv3, page 13-4
- Registry Security, page 13-6
- User Authentication and Authorization, page 13-6

Communication Security

Figure 13-1 illustrates the different forms of secure communication that are implemented between the Prime Network gateway server, units, clients, and database.
A socket factory service that runs on the gateway server implements SSL sockets between:

- The gateway and all units
- The gateway and all clients

With SSL version 3.0, keys are created when you install Prime Network on the gateway server. All secured connections use the same private key and certificate for SSL authentication. After installation, these keys are distributed by the gateway to the clients and other units. SSL keys can be recreated (as described in the *Cisco Prime Network Integration Developer Guide*).

Whenever a socket cannot be opened, a System event is generated and is displayed in Prime Network Events.

If you upgrade your version of Prime Network, be sure to upgrade all components—gateway server, units, and clients—to avoid problems with connections.

For information on Prime Network Change and Configuration Management communication security, see *Cisco Prime Network 3.9 Change and Configuration Management User Guide*.

**Gateway Server and Unit Communication Security**

Communication between the gateway server and units is called transport communication. Transport connections are encrypted when the unit and gateway are on different machines, but are not encrypted when both are local to the same machine. Similarly, AVMs use transport communication, and communication between AVMs is encrypted when the AVMs are on different machines. There is no option to change this behavior in the GUI clients.
Prime Network uses the SSH protocol for administrative messages (such as scp) between the gateway and units. A random certificate (that is privately signed) is generated on the gateway at installation time. When Prime Network is installed on any unit (or the unit is restarted), the keys are copied from the gateway to the unit.

**Gateway Server and Client (Including BQL) Communication Security**

For gateway and client communication, Prime Network uses a proprietary protocol called **PTP** (Point to Point communication). This is encrypted using SSL. The SSL keys are downloaded to Prime Network clients using the JNLP (Webstart) protocol.

For BQL clients, the gateway server allows secured and unsecured connections from local clients (on port 9002), but only secured connections from clients on other machines. By default, port 9002 only allows unsecured connections. Information on how to change this behavior is described in the BQL documentation in the *Cisco Prime Network Integration Developer Guide*.

For a client to communicate with the Prime Network gateway using Perl, a certificate in .pem format is required. This can be generated from the .cer format using the two-stage process described in the *Cisco Prime Network Integration Developer Guide*.

If a client trusts all servers, the public key is automatically imported as part of the SSL handshake. However, for a client to validate a server’s public key, the .truststore file must be manually copied from the server.

For more information on SSL sockets and BQL, such as the architecture and negotiation process, see the *Cisco Prime Network Integration Developer Guide*.

**Database Connections**

Prime Network is connected to the database using an Oracle encryption feature. The default encryption settings are as follows:

- Client-to-database connections are encrypted.
- Server-to-database connections are:
  - Encrypted if are using an embedded database.
  - Not encrypted for all other database installations, although you can change this (and choose an encryption type) at installation time.

**Updating the Database’s Connections Encryption**

To enable or modify encryption on PrimeNetwork connections to the database (client side), modify the following entries of the registry:

```bash
# ./runRegTool.sh -gs localhost set 0.0.0.0 site/persistency/nodes/<scheme_name>/EncryptionClient <VALUE>
# ./runRegTool.sh -gs localhost set 0.0.0.0 site/persistency/nodes/<scheme_name>/EncryptionTypesClient <VALUE/VALUES>
```

where:

- `<scheme_name>` : The scheme for which the encryption has to be changed. These schemes could be:
  - main, ep, xmp, admin, main_rep or ep_rep.
  - You should execute these commands for every scheme you want to update.
- EncryptionClient value : REJECTED, ACCEPTED, REQUESTED or REQUIRED
Device Communication Security: SSH and SNMPv3

- EncryptionTypesClient value: It can be one more of the following algorithms (comma separated):
  RC4_128,RC4_40,RC4_56,RC4_256,AES256,AES192,AES128,3DES168,3DES112

Note: The values set on the registry should be compliant with the values set on the server’s side (the database server).

The database schemas are described in Prime Network Database Schemas, page 10-1.

Gateway and Unit Servers Behind Firewalls or NAT Devices

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.

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

Managed Devices Behind Firewalls or NAT Devices

If there is a firewall between a GUI client and a managed device, all attempted Telnet connections to the device will fail. The Prime Network Administration GUI client provides a device proxy feature that, when enabled, routes connections from the client through the gateway server and units, as required, to reach the device. Supported connections are Telnet, Ping, and SSH. When it is enabled, dedicated SSH connections are used between the gateway and the unit. For information on how to configure this feature, see Managing Configurations with Firewalls (Device Proxy), page 9-2.

Device Communication Security: SSH and SNMPv3

In Prime Network, protocol collectors are the components responsible for actively polling devices and transporting information between devices and the Prime Network gateway. Protocols collectors are part of the instrumentation layer of Prime Network VNEs. A device has a collector for each protocol it supports, such as one collector for SSH and another collector for SNMP. Each collector contains the necessary logic for its specific protocol.

The security of device communication is maintained by specifying SSH and SNMPv3 authentication and encryption methods when you create the VNE. Table 13-1 summarizes the security methods that are supported by each protocol.
Table 13-1  Device Communication Security Features in SSHv1, SSHv2, and SNMPv3

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Supported Security Feature for Device Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSHv1</td>
<td>Encryption ciphers: DES, 3DES, Blowfish</td>
</tr>
<tr>
<td>SSHv2</td>
<td>Client Authentication: password, public keys</td>
</tr>
<tr>
<td></td>
<td>Server Authentication Method: none, save-first-auth, preconfigured</td>
</tr>
<tr>
<td></td>
<td>Server Authentication Key: fingerprint or public key (not used if none is chosen for server authentication method)</td>
</tr>
<tr>
<td></td>
<td>Key exchange: DH-group1-sha1, DH-group1-exchange-sha1</td>
</tr>
<tr>
<td></td>
<td>MAC algorithm: SHA1, MD5, SHA1-96, MD5-96</td>
</tr>
<tr>
<td></td>
<td>Ciphers: 3DES, AES-128, AES-192, AES-256, Blowfish, Arcfour</td>
</tr>
<tr>
<td></td>
<td>Host Key Algorithm: DSA, RSA</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>Authentication settings: NoAuthPriv (authentication without encryption), AuthPriv (authentication and encryption)</td>
</tr>
<tr>
<td></td>
<td>Ciphers: DES, AES128, AES192, AES256</td>
</tr>
<tr>
<td></td>
<td>Encryption algorithms: MD5, SHA</td>
</tr>
</tbody>
</table>

Note  The use of SNMP V3 with AES192 or AES256 might be subject to import restrictions on cryptography key strength in some countries. Therefore, if you want to use these combinations, please open a TAC case.

Table 13-2 Registry Settings for SSHv2 Communication Between Device and VNE

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-alg</td>
<td>Allow MAC algorithms</td>
<td>sha1,md5,sha1-96,md5-96,</td>
</tr>
<tr>
<td>keys-exchange-alg</td>
<td>Allow Key exchange algorithms</td>
<td>diffie-hellman-group1-sha1,diffie-hellman-group1-exchange-sha1,</td>
</tr>
<tr>
<td>host-key-alg</td>
<td>Allowed host key algorithms</td>
<td>dsa,rsa,</td>
</tr>
<tr>
<td>encryption-alg</td>
<td>Permitted encryption (ciphers) algorithms</td>
<td>3des,aes-128,aes-192,aes-256,blowfish,arcfour</td>
</tr>
</tbody>
</table>

The following procedure shows how to check and change your current settings.
Step 1  Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39), and change to the Main directory by entering the following command:

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

Step 2  Issue the following command to check the current default SSHv2 security settings for VNE and device communication:

```
#/runRegTool.sh -gs 127.0.0.1 get 127.0.0.1 "agentdefaults/da/ip_default/protocols/telnet/connection/algorithms"
```

```
<key name="algorithms">
  <entry name="mac-alg">sha1,md5,sha1-96,md5-96</entry>
  <entry name="keys-exchange-alg">diffie-hellman-group1-shal,diffie-hellman-group1-exchange-shal</entry>
  <entry name="host-key-alg">dsa,rsa</entry>
  <entry name="encryption-alg">aes-128,aes-192,aes-256</entry>
</key>
```

For example, the following command overwrites the encryption (ciphers) algorithms so that 3DES is no longer allowed for any newly-created VNEs:

```
Note  Each algorithm type should have at least one algorithm entry (supported algorithm).

#/runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/agentdefaults/da/ip_default/protocols/telnet/connection/algorithms/encryption-alg" "aes-128,aes-192,aes-256,"
```

Step 3  Restart the AVM.

Registry Security

The Golden Source registry is the master registry responsible for maintaining, distributing, and updating registry configuration files to all Prime Network units and the Prime Network gateway. The master copy of the Golden Source files is centrally located on the gateway server at:

```
NETWORKHOME/Main/registry/ConfigurationFiles
```

Credentials data is encrypted. This includes the SNMP, Telnet, and SSH credentials for VNEs, and the database password. Sections that are encrypted are marked with an ENCRYPTED_ENTRY_AES prefix.

User Authentication and Authorization

```
Note  These features are disabled if Prime Network is installed with Cisco Prime Central. If a user tries to log into Prime Network, they will be redirected to the suite login page. The only exception is the Prime Network emergency user, who will still be allowed to log into standalone Prime Network.
```
Prime Network uses a combination of methods to manage user authentication and authorization:

- **User authentication** can be managed locally by Prime Network or externally by an LDAP application. Either method can be used to validate user accounts and passwords, thus controlling who can log into Prime Network. If you use Prime Network, user information and passwords are stored in the Prime Network database. If you use an external LDAP application, passwords are stored on the external LDAP server. See **Overview of User Authentication and Authorization**, page 7-1.

- **User authorization** is managed through a combination of **user access roles** and **scopes**:
  - User access roles control the actions a user can perform in the Prime Network GUI clients. When a user’s account is created, the user is assigned an access role that determines the user’s **default permissions**. For more information, see **Prime Network User Roles**, page 7-2.
  - Scopes are groups of network elements that are created by administrators. Once a scope is created, you can assign it to users. A user’s default permissions determine the actions the user can perform on the network elements in the scope. These actions are referred to as the user’s **security level** on that scope. If desired, you can assign the user a more strict user access role for a scope. For more information, see **Device Scopes**, page 7-3.

When creating a user account, the password has to meet stringent rules. These rules can be set globally and are documented in **Setting Global Password Rules**, page 7-14. That topic also describes how administrators can specify how many login attempts are allowed, after which a user account is disabled. Administrators can also configure a period after which inactive accounts are disabled; see **Automatically Disabling Accounts for Inactive Users**, page 7-15.

Administrators can set up a daily message that is displayed when a user logs in. The message must be acknowledged to get to the login screen. For information, see **Creating a GUI Client Banner Message**, page 2-5.
Managing the Event Collector (AVM 100)

These topics describe the Prime Network Event Collector, the fault management tasks it performs, and how to configure multiple Event Collectors:

- Overview of the Event Collector and Event Processing, page 14-1
- Configuring the Event Collector: Examples, page 14-6
- Enabling a Single Event Collector on a Gateway or a Unit, page 14-11
- Configuring and Enabling Multiple Event Collectors, page 14-12
- Registering VNEs with a Non-Default Event Collector, page 14-15
- Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15
- Disabling and Re-Enabling Event Archiving, page 14-16

Overview of the Event Collector and Event Processing

When a trap or syslog is sent from a device to Prime Network, it is received by the Event Collector, which runs on AVM 100. Figure 14-1 illustrates how Prime Network responds to incoming notifications from devices. The exact flow depends on how Prime Network is configured in your network.

Note

Figure 14-1 illustrates the logical flow of events through Prime Network. The actual network communication is subject to the transport configuration between the gateway server and units.
Chapter 14      Managing the Event Collector (AVM 100)

Overview of the Event Collector and Event Processing

Figure 14-1  How Prime Network Responds to Incoming Notifications from Devices

Figure 14-1 also illustrates the two entities that store fault information, both of which reside in the Prime Network database:

- Event Archive—Contains all raw events (traps, and syslogs) received from devices. The Event Archive also stores information from unmanaged devices (if notification from unmanaged devices is enabled; see the Cisco Prime Network Integration Developer Guide). The database schema name is network user_ep, where network user is the is the operating system user account for the Prime Network application. (This account is created when Prime Network is installed.) For example, if network user is named network39, the Event Archive schema is called network39_ep.

You can only view information in the Event Archive using the reports mechanism. Event archiving is enabled by default, but you can disable it using the procedure in Disabling and Re-Enabling Event Archiving, page 14-16.

- Fault Database—Contains all the actionable events (events that Prime Network knows how to parse and can therefore participate in correlation). The Fault Database also contains information such as tickets, alarms, and severity information. The Fault Database schema name is network user. For example, if network user is named network39, the main schema is called network39.

You can view information in the Fault Database using the Prime Network Events and using Prime Network Vision GUI clients.

Event Archive and Fault Database data is archived and saved according to the settings in the Global Settings > Event Management Settings window in the Prime Network Administration GUI client. (See Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6.)

The following topics describe how the Event Collector, VNEs, and the Fault Agent (AVM 25) work together to process incoming notifications from devices. For more details about the event flow illustrated in Figure 14-1, see the Cisco Prime Network Integration Developer Guide.
**Event Collector (AVM 100)**

The Event Collector is the first receiver for incoming event notifications from devices. It is an internal service that is part of AVM 100. During installation, Event Collectors are created on the gateway and all units, but a single Event Collector AVM is started only on the gateway. By default, all new VNEs will register with the Event Collector on the gateway server. This Event Collector has the internal address 0.0.0.0 (this address is not related to the device IP address).

---

**Note**

If desired, you can configure a filter that will drop “pure noise” at the Event Collector level. In other words, this filter will drop all raw events before any processing or archiving is done; the events are not processed by VNEs or forwarded using the Event Notification Service. Complete instructions for configuring this type of filter is provided on the Cisco Developer Network at [http://developer.cisco.com/web/prime-network/home](http://developer.cisco.com/web/prime-network/home). (This is different from the global event filter that drops events at the VNE level when the system moves into safe mode; see Automatic Overload Prevention (AOP/Safe Mode), page 9-17.)

---

When an event, trap, or syslog is received by the Event Collector, the Event Collector does the following:

1. Performs initial parsing to obtain basic information about each event.
2. (If a global filter is implemented) Filters out (drops) any events that match the filter. By default, no filters are implemented. To configure a filter, see Configuring the Event Collector: Examples, page 14-6.
3. Stores all events, traps, and syslogs in the Event Archive (if event archiving is enabled, which it is by default). Events are saved in the Event Archive only if the device has corresponding VNE which is registered to the Event Collector. This can also include information from unmanaged devices if notification from unmanaged devices is enabled (see the Cisco Prime Network Integration Developer Guide). If a syslog is sent as an SNMP trap by way of the CISCO-SYSLOG-MIB, the Event Collector interprets it to be a syslog.
4. If enabled, forwards events from unmanaged devices to the Event Notification Service. (See Configuring Event Notifications, page 6-1.)
5. Distributes each event to its corresponding VNE (if the VNE is registered with the Event Collector).

The Event Collector AVM requires a database connection when event archiving is enabled. If event archiving is disabled, a connection to the database is not required. To disable or reenable event archiving, see Disabling and Re-Enabling Event Archiving, page 14-16.

**Event Collector and Unit Server High Availability**

You can configure the Event Collector to run on a unit instead of the gateway. If the unit is also configured with unit server high availability, the Event Collector on the standby unit will drop all events because the Event Collector is disabled. This is by design; it should not start until a switchover occurs.

The standby unit contains a port watchdog script that listens for events on the unit’s Syslog and SNMP ports. The script prevents unnecessary ICMP unreachable messages being sent back to the network. If a switchover occurs, the standby unit and Event Collector AVM will start, and the watchdog script releases the ports.

When the original unit comes back up, the standby Event Collector AVM goes back down, and the watchdog script recommences listening on the standby unit’s Syslog and SNMP ports.
Overview of the Event Collector and Event Processing

Note

If the Cisco Prime Performance Manager application is also installed (with Prime Central), the Prime Network Event Collector will receive threshold crossing alarm (TCA) events from Prime Performance Manager components and do the following:

- Save TCA events in the Event Archive.
- Forward TCA events to appropriate VNEs. The events are currently not parsed by the VNE. They will be identified as generic traps and will be dropped. If desired, you can forward them to an Event Notification Service (see Configuring an Event Notification Service, page 6-3).

No special configuration is required.

Prime Network also receives EPM-MIB traps from the network. By default Prime Network receives EPM-MIB traps from any source in the network. If desired, you can configure Prime Network to only process EPM-MIB traps arriving from a specific Prime Performance Manager server. The instructions for doing this are provided on the Cisco Developer Network at http://developer.cisco.com/web/prime-network/home.

VNEs

When a VNE receives an event from the Event Collector, the VNE does the following:

- Attempts to match the event with a predefined pattern. Events that are successfully matched are designated as actionable events. The VNE attempts to extract information from the raw event (the source, the problem, and the severity).
  
  Events that are not matched can still be forwarded to configured recipients. This is done by enabling an Event Notification Service to forward generic syslogs/enterprise trap syslogs. See Figure 6-3 on page 6-6 for an example of how this is done from the Event Notification Service in the Prime Network Administration GUI client.

- If the event is actionable, correlates the event and, if possible, identifies a root cause.

Sends the parsed event and correlation information to AVM 25 to be saved to the Fault Database. The Fault Database also contains information such as tickets, alarms, and severity information.

These actions are performed by a process within the VNE called the event manager, which is responsible for handling all network events, whether they are syslogs or traps, discovered during normal polling, or threshold-crossing alarms.

VNEs must be registered with an Event Collector’s internal address (this address is not related to the device IP address). When a VNE is first initialized, the following occurs:

- The VNE reads this Event Collector’s internal address from the registry. (By default, all new VNEs will register with the Event Collector on the gateway server. This Event Collector has the internal address 0.0.0.0.)

- The VNE registers its management IP address with this Event Collector.

If the Event Collector receives a trap or syslog, and the trap or syslog’s source IP address matches the VNE’s management IP address, the Event Collector will forward the syslogs or trap to that VNE.

A VNE may have more than one IP address registered with the Event Collector (for example, when the device is using other IP addresses as sources for syslogs or traps). These IP addresses can be discovered automatically from the device configuration but can also be manually configured using the VNE Event settings in Prime Network Administration (see VNE Events Settings, page 19-42).
Overview of the Event Collector and Event Processing

AVM 25 (Fault Agent)

When a VNE forwards an event to AVM 25, the Fault Agent does the following:

1. Saves the information to the Fault Database.
2. If necessary, creates a new ticket based on the correlation information and event type. Some event types are configured as ticketable and others are not; this is controlled in the registry. Prime Network will create a ticket for ticketable events, even if they are non-correlated events.

AVM 25 requires a database connection to store information in the Fault Database so that it can be subsequently viewed in Prime Network Events. If a direct connection is not available, you can configure AVM 25 without connectivity to forward its events to another AVM 25 that does have a database connection. This is called using a proxy AVM 25. How to do so is described in Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15.

Keep these items in mind when starting and stopping AVM 25:

• Avoid stopping AVM 25 to make sure that Prime Network does not drop events
• If you stop and restart AVM 25, you do not have to restart user-created AVMs.
• User-created AVMs will not start if AVM 25 is not running; they will be Unreachable.

Example of Full Event Flow

The following steps show the flow of events when Device A sends a Port Down notification to the Event Collector.

1. The Event Collector receives the notification and persists the Port Down event to the Event Archive. The Event Collector forwards the syslog to the corresponding VNE.
2. The VNE polls the device and issues a Link Down service event. The VNE correlates the Port Down event to the Link Down service event. The VNE sends all of this information to AVM 25.
3. AVM 25 saves all of this information to the Fault Database and opens a Link Down ticket with the Link Down event as the root cause. AVM 25 updates the severity aspect.

At this point, the Fault Database contains:

– A Link Down ticket with the Link Down event as its root cause.
– A Port Down event that has been correlated to the Link Down event.

At this point users can view the ticket in Prime Network Vision, but the Port Down event will not be in the ticket’s correlation information.

4. When it queries the Fault Database, the Ticket Agent will pick up the Port Down event because it is correlated to a Link Down event, but not associated with any ticket. The Ticket Agent updates the Link Down service event, associates the Port Down event with the Link Down ticket, updates the ticket information and severity aspect.
Configuring the Event Collector: Examples

During installation, Event Collector AVMs are created on the gateway and all units, but a single Event Collector AVM is started only on the gateway. You can configure an Event Collector to run on a unit instead, or configure multiple Event Collectors. These topics describe the supported scenarios.

Deploying multiple Event Collectors does not increase the overall rate at which Prime Network parses, correlates, and saves information in the Fault Database. If Prime Network can parse and correlate 100 events per second, and you deploy two Event Collectors this number will not increase to 200.

When considering which scenario is best for you, consider the following points:

- If event archiving is disabled, the Event Collector AVM does not require database connectivity.
- The Event Collector on a unit in standby mode will not forward any events to the Event Archive; it will drop all events.
- AVM 25 always requires database connectivity. If a connection is not available, you can configure AVM 25 to use a proxy AVM 25. (See Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15.)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Appropriate for:</th>
<th>For an example, see:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Event Collector on gateway</td>
<td>Systems with exceptional reliability (where gateway is never expected to go down).</td>
<td>Figure 14-2 on page 14-7</td>
</tr>
<tr>
<td>Single Event Collector on unit</td>
<td>Systems where you want to localize Event Collector functionality to one unit (if the unit goes down, the system will operate but will lose the unit’s functionality).</td>
<td>Figure 14-3 on page 14-8</td>
</tr>
<tr>
<td>Single Event Collector on unit with high availability</td>
<td>Systems where you want to localize Event Collector functionality to one unit (if unit goes down, the system will operate with no loss of unit functionality).</td>
<td>Figure 14-4 on page 14-9</td>
</tr>
<tr>
<td>Multiple Event Collectors on units</td>
<td>Systems with either or both of the following characteristics:</td>
<td>Figure 14-5 on page 14-10</td>
</tr>
<tr>
<td></td>
<td>• Systems with devices that have connectivity issues with the configured single Event Collector; or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Systems with a relatively high events-per-second rate that are using SNMPv3, and find it desirable to spread network event decryption and initial parsing across several machines</td>
<td></td>
</tr>
</tbody>
</table>

Deploying multiple Event Collectors does not increase the overall rate at which Prime Network parses, correlates, and saves information in the Fault Database. For information on increasing SNMPv3 decryption capabilities and other deployment information and recommendations, contact your Cisco representative.
Example: Single Event Collector on Gateway Server

Figure 14-2 illustrates how events should be forwarded in a configuration where a single Event Collector is enabled on the gateway server.

For this scenario, because the Event Collector AVM is enabled on the gateway server by default, all you must do is:

1. Configure the network elements to forward events to the gateway server.
2. Make sure all other Event Collectors are disabled. The Event Collector AVM is enabled on the gateway server by default. If you have to manually enable it, see Enabling the Event Collector on the Gateway Server, page 14-11.

No other configuration changes are required. New VNEs will automatically register to this Event Collector.
Example: Single Event Collector on Unit Server (No High Availability)

Figure 14-3 illustrates how events should be forwarded in a configuration where one Event Collector is enabled on a unit server.

**Figure 14-3 Single Event Collector On Unit Server**

For this scenario, you must do the following:

1. If it is enabled, disable the Event Collector AVM on the gateway server (it is enabled on the gateway server by default).
2. Configure the network elements to forward events to the unit server that will host the enabled Event Collector.
3. Start the Event Collector AVM on the unit server and make sure all other Event Collectors are disabled. See Enabling a New Event Collector on a Unit, page 14-12.
4. If the unit with the running Event Collector does not have connectivity to the database, disable event archiving on the unit as described in Disabling and Re-Enabling Event Archiving, page 14-16. (In addition, you should configure a proxy AVM 25 on this unit. See Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15.)

No other configuration changes are required. New VNEs will automatically register to this Event Collector.

If the unit with the enabled Event Collector fails and is not operational, you must do the following:

1. Repeat the previous steps on the new machine.
2. Move all AVMs to the new machine (see Moving and Deleting AVMs, page 4-13). When the moved VNEs start, they will automatically register to the new Event Collector.
Example: Single Event Collector on Unit Server with High Availability

Figure 14-4 illustrates how events should be forwarded in a configuration where one Event Collector is enabled on a unit server, and the unit server is part of a protection group that contains Unit A (an active unit with an enabled Event Collector), Unit B (standby unit with disabled Event Collector), and Unit C (active unit). See AVM 100 and Unit Server High Availability, page 16-3, for details about how the Event Collector operates in a unit server high availability scenario.

In Figure 14-4, devices are managed by Unit A.

Figure 14-4  Event Collector On Unit Server with High Availability

For this scenario, you must do the following:

1. If it is enabled, disable the Event Collector AVM on the gateway (it is enabled on the gateway by default).
2. Configure and start the Event Collector AVM on the active unit as explained in Enabling a New Event Collector on a Unit, page 14-12. (The Event Collector AVM on the standby unit should not be enabled.)
3. Configure the network elements to forward events to both the active and standby units.
4. If any of the units with a running Event Collector do not have connectivity to the database, disable event archiving on them as described in Disabling and Re-Enabling Event Archiving, page 14-16. (In addition, you should configure a proxy AVM 25 on this unit. See Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15.)

If the unit with the enabled Event Collector fails, the Event Collector on the standby unit is automatically started and the VNEs are automatically reregistered with the Event Collector on the standby unit. See AVM 100 and Unit Server High Availability, page 16-3 for information on what happens if the failed unit comes back up.
Example: Multiple Event Collectors on Unit Servers (No High Availability)

Prime Network supports multiple enabled Event Collectors. The Event Collectors can be on the gateway and units, or just the units.

Figure 14-5 illustrates how events should be forwarded in a configuration with two Event Collectors enabled on different unit servers. This configuration is appropriate to a network in which devices have connectivity issues with the configured single Event Collector.

Deploying multiple Event Collectors does not increase the overall rate at which Prime Network parses, correlates, and saves information in the Fault Database. If Prime Network can parse and correlate 100 events per second, and you deploy two Event Collectors this number will not increase to 200.

This scenario can also increase SNMPv3 decryption capabilities. For information on this and other deployment information and recommendations, contact your Cisco representative.

For this scenario, you must do the following:

1. If it is enabled, disable the Event Collector AVM on the gateway (it is enabled on the gateway by default).
2. Configure and start the Event Collectors as explained in Enabling a New Event Collector on a Unit, page 14-12.
3. Configure the network elements to forward events to one of the units with an enabled Event Collectors.
4. If any units do not have connectivity to the database, disable event archiving and configure a proxy AVM 25 on those units. See Configuring Proxy AVM 25 for Units Not Connected to Database, page 14-15.

5. For the group of VNEs you want to use the newly defined Event Collector, you must manually register the VNEs with the new Event Collector. See Registering VNEs with a Non-Default Event Collector, page 14-15.

## Enabling a Single Event Collector on a Gateway or a Unit

During installation, an Event Collector AVM is created on the gateway and all units, but it is started only on the gateway. By default, the enabled Event Collector has the internal address 0.0.0.0 (this address is not related to the device IP address). All new VNEs will register with the Event Collector on the gateway server.

### Enabling the Event Collector on the Gateway Server

Although the Event Collector runs on the gateway by default, there may be instances where it has been stopped. If so and you need to restart it, use the following procedure.

**Before You Begin**

- Configure the network elements to forward traps and syslogs to the gateway server that will contain the enabled Event Collector.
- Make sure all other Event Collectors are disabled.

If no other Event Collector was enabled after the gateway Event Collector was stopped, do the following to restart the Event Collector:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the All Servers branch, open the gateway branch.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Right-click the Event Collector AVM and choose Actions &gt; Start.</td>
</tr>
</tbody>
</table>

If an Event Collector was enabled on another unit, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Stop the Event Collector AVM on the unit.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Stop the unit on which the Event Collector was enabled.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Restart the gateway.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Start the Event Collector AVM on the gateway.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Start the unit.</td>
</tr>
</tbody>
</table>

The Event Collector will begin processing events when they are received. By default, any new VNEs will register with the Event Collector on the gateway server.
Configuring and Enabling Multiple Event Collectors

Configuring a network to have two Event Collectors enabled on different unit servers is appropriate to a network in which devices have connectivity issues with the configured single Event Collector. However, deploying multiple Event Collectors does not increase the overall rate at which Prime Network parses, correlates, and saves information in the Fault Database. If Prime Network can parse and correlate 100 events per second, and you deploy two Event Collectors this number will not increase to 200.

An illustration of this configuration is provided in Example: Multiple Event Collectors on Unit Servers (No High Availability), page 14-10.

Note

This scenario can also increase SNMPv3 decryption capabilities. For information on this and other deployment information and recommendations, contact your Cisco representative.

To configure multiple Event Collectors you must edit the registry using the runRegTool.sh script. The runRegTool.sh script is in the directory NETWORKHOME/Main and uses the following format:

```
runRegTool.sh -gs 127.0.0.1 set unit-IP “vne-avm/agents/da/vne-name/trap/xidip” event-collector-address
```
The `runRegTool.sh` script accepts the following arguments:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>unit-IP</code></td>
<td>The IP address of the machine on which the AVM resides (if the AVM resides on the gateway, this should be 127.0.0.1). This IP address is defined during installation and configuration.</td>
</tr>
<tr>
<td><code>vne-avm</code></td>
<td>The AVM on which the VNE is configured.</td>
</tr>
<tr>
<td><code>vne-name</code></td>
<td>The name of the VNE in Prime Network.</td>
</tr>
<tr>
<td><code>event-collector-address</code></td>
<td>The internal IP address of the Event Collector (internally, this is called the XIDIP of the Event Collector). This address is used for communication between the VNEs and the Event Collector and is unrelated to the device IP address. <code>event-collector-address</code> can have the following values based on how many Event Collectors are running in the system.</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>The default <code>event-collector-address</code>. Used when only one Event Collector is running on a system.</td>
</tr>
<tr>
<td><code>unit-IP</code></td>
<td>Used when configuring additional Event Collectors.</td>
</tr>
</tbody>
</table>

### How To Configure Multiple Event Collectors

Complete the following procedure for each additional Event Collector that needs to be configured. Because this is a completely new Event Collector, you do not have to stop or restart any AVMs.

#### Before You Begin

Configure the network elements to forward traps and syslogs to the appropriate Event Collector. If you are using unit server high availability, traps and syslogs should be forwarded to both the active and standby units.

To configure multiple Event Collectors:

**Step 1**  
From the gateway, issue the following `runRegTool.sh` script to add an additional Event Collector to Prime Network:

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP "avm100/agents/trap/xidip" unit-IP
```

The update is automatically propagated from the gateway to the relevant units.

**Step 2**  
Start the Event Collector AVM on the unit with Prime Network Administration by right-clicking the AVM and choosing Actions > Start.

**Step 3**  
If you want any existing VNEs to register with an Event Collector other than the default (at 0.0.0.0), perform the instructions in Registering VNEs with a Non-Default Event Collector, page 14-15.

When you add new VNEs, you must register the VNEs to the appropriate Event Collector as described in Registering VNEs with a Non-Default Event Collector, page 14-15.
Example Procedure for Configuring Two Event Collectors on Two Units

This example illustrates how to configure an Event Collector to run on one unit, and a second Event Collector to run on a second unit. The configuration is as follows:

- Gateway IP address: 192.168.10.1
- Unit 1 IP address: 192.168.10.2
  - Contains AVM 100, which is an Event Collector with the address 192.168.10.2.
  - Contains AVM 200, which is an AVM that contains user-created VNEs.
- Unit 2 IP address: 192.168.10.3
  - Contains AVM 100, which is an Event Collector with the address 192.168.10.3.
  - Contains AVM 300, which is an AVM that contains user-created VNEs.

In this example, two Event Collectors are configured, one on each unit. Each Event Collector handles the events (SNMP traps and syslogs) sent from the network elements that correspond to the VNEs it manages.

After installing the gateway and the two units, configure the Event Collectors and the VNEs:

**Step 1** Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; an example of network user is network39), and change to the Main directory by entering the following command:

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

**Step 2** Issue the following commands to configure the Event Collector addresses:

```
# ./runRegTool.sh -gs 127.0.0.1 set 192.168.10.2 "avm100/agents/trap/xidip" 192.168.10.2
# ./runRegTool.sh -gs 127.0.0.1 set 192.168.10.3 "avm100/agents/trap/xidip" 192.168.10.3
```

**Step 3** Issue the following commands to configure the VNEs to register to their Event Collector:

a. For each VNE configured to receive traps and syslogs from the Event Collector (AVM 100) on Unit 1, use the following command:

```
# ./runRegTool.sh -gs 127.0.0.1 set 192.168.10.2 "avm200/agents/da/vne-name/trap/xidip" 192.168.10.2
```

b. For each VNE configured to receive traps and syslogs from the Event Collector (AVM 100) on Unit 2, use the following command:

```
# ./runRegTool.sh -gs 127.0.0.1 set 192.168.10.3 "avm300/agents/da/vne-name/trap/xidip" 192.168.10.3
```

c. Restart the reconfigured VNEs.

**Step 4** Start each new Event Collector with Prime Network Administration by right-clicking the Event Collector AVM and choosing Actions > Start.
Registering VNEs with a Non-Default Event Collector

If you do not want a VNE to be registered with the default Event Collector—that is, the Event Collector that uses the internal address 0.0.0.0—you must manually change the VNE registration. (This internal address is not related to the device IP address.)

**Note**
Before performing the following procedure, verify that all VNEs are configured in the relevant units.

Complete the following procedure to register VNEs to an enabled Event Collector:

**Step 1** Choose the Event Collector that is to receive the traps and syslogs for the VNE.

**Step 2** Locate the AVM on which the VNE resides.

**Step 3** Log into the gateway as `network user` (where `network user` is the operating system account for the Prime Network application, created when Prime Network is installed; an example of `network user` is `network39`), and change to the Main directory by entering the following command:

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

**Step 4** Issue the following `runRegTool.sh` script (`vne-key` is the VNE name):

```
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP "avm39/agents/da/vne-key/trap/ip" unit-IP
```

The update is automatically propagated to the relevant units. For details on the command syntax, see Example Procedure for Configuring Two Event Collectors on Two Units, page 14-14.

**Step 5** Reload the VNE with Prime Network Administration by right-clicking the VNE and choosing Actions > Start.

Configuring Proxy AVM 25 for Units Not Connected to Database

If a unit server does not have a direct connection to the database, you can configure another unit to be its proxy and persist event information to the Fault Database. However, because there is no proxy support for the Event Collector (AVM 100), raw events will not be saved to the Event Archive. Therefore, you should disable raw event archiving as described in Disabling and Re-Enabling Event Archiving, page 14-16. If you do not disable event archiving, the log will contain errors because events are not being forwarded to VNEs nor are system events being generated.

To configure a proxy AVM 25, you must edit the registry (the avm25.xml file) for the unit that does not have database connectivity. The proxy unit will process the events as part of its normal event flow.

**Step 1** Disable event archiving on the unit that does not have a database connection. See Disabling and Re-Enabling Event Archiving, page 14-16.

**Step 2** On the unit that has no database connection, edit the registry to add the proxy instructions using the following `runRegTool.sh` scripts:

```
runRegTool.sh -gs 127.0.0.1 add unit-IP "avm25/services/management/proxy"
runRegTool.sh -gs 127.0.0.1 set unit-IP "avm25/services/management/proxy/IP" proxy-unit-IP
```
Disabling and Re-Enabling Event Archiving

By default, Prime Network archives all event notifications it receives from devices and saves them in the Event Archive. Events are saved according to the settings that are configured in the Global Settings > Event Management Settings window in the Prime Network Administration GUI client (see Customizing Archive and Purge Settings for the Fault Database and Event Archive, page 10-6). If you do not want to save any raw events to the Event Archive, you can disable it by using the following procedure.

Note

If you disable this feature, the data will not be available for event-related reports.

Step 1

Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; an example of network user is network39), and change to the Main directory by entering the following command:

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

Step 2

Issue the following command to disable event archiving:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/trap/agents/trap/netEventPersistencyEnabled" false
```

Disabling and Re-Enabling Event Archiving

This runRegTool.sh scripts requires the following arguments:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit-IP</td>
<td>The IP address of the unit server that does not have a database connection.</td>
</tr>
<tr>
<td>proxy-unit-IP</td>
<td>The IP address of the unit server that has a database connection and will act as a proxy for the unit server at unit-IP.</td>
</tr>
</tbody>
</table>

The following is an example:

- Unit 1 (192.168.10.2) does not have a database connection.
- Unit 2 (192.162.11.1) has a database connection and will act as a proxy for Unit 1.

To configure Unit 1 to use Unit 2 as a proxy for AVM 25, enter these commands:

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 add 192.168.10.2 "avm25/services/management/proxy"
# ./runRegTool.sh -gs 127.0.0.1 set 192.168.10.2 "avm25/services/management/proxy/IP" 192.162.11.1
```

Step 3

Restart the unit that has no database connectivity (in the example this would be Unit 1):

```
# networkctl restart
```

(This will also restart any VNEs on Unit 1 that are using a non-default Event Collector, which is also required.)
To reenable event archiving, use this command:

```
#/runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/trap/agents/trap/netEventPersistencyEnabled" true
```

**Step 3** Restart the Event Collector A VM from Prime Network Administration by right-clicking the A VM and choosing *Actions > Stop* and (when it is down) *Actions > Start*. 
Utility Scripts

The following topics describe some additional Prime Network utility scripts that you can use to do the following:

- Changing Passwords: Prime Network Database Schemas, page 15-1
- Changing Passwords: bosenable, bosconfig, and bosusermanager, and root, page 15-4
- Running a Command on All Prime Network Units, page 15-5
- Using the vne_creation_script to Add VNEs, page 15-5

Changing Passwords: Prime Network Database Schemas

By default, an operating system account for the Prime Network application is created when Prime Network is installed. When the database is created, it uses this operating system account name as the basis for naming the schemas. The following are the database schemas that are created by Prime Network. As an example, in the following table the Prime Network operating system account (network user) is named network39. (For more details about these schemas, see Prime Network Database Schemas, page 10-1.)

<table>
<thead>
<tr>
<th>Schema Name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>network user</td>
<td>Prime Network general data</td>
<td>network39</td>
</tr>
<tr>
<td>network user_ep</td>
<td>Prime Network event persistence and archiving data</td>
<td>network39_ep</td>
</tr>
<tr>
<td>network user_dwe</td>
<td>Prime Network Workflow Engine data</td>
<td>network39_dwe</td>
</tr>
<tr>
<td>network user_xmp</td>
<td>Prime Network Change and Configuration Management data</td>
<td>network39_xmp</td>
</tr>
<tr>
<td>network user_admin</td>
<td>Prime Network maintenance and administration data</td>
<td>network39_admin</td>
</tr>
</tbody>
</table>

At installation time, the network-conf script assigns the same password to all of the schemas. After installation, you can assign different passwords to each schema. The following procedure describes how to change any or all of the passwords. Note that you have to change the password in two places: in the Oracle software and in the Prime Network software.
In the following procedure, *network user-DB*, *network user-EP-DB*, *network user-DWE-DB*, *network user-admin-DB*, and *network user-XMP-DB* are the user accounts for the four database schemas.

**Step 1**  
Log into the Prime Network gateway server as *network user*.

**Step 2**  
To change the *network user-DB* password (for the general data):

**a.** Enter the following `sqlplus` command to change the *network user-DB* password in the Oracle software:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
network user-DB network user-DB-new-password DB-IP DB-port SID
```

For example:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql system systempassword
network39 network39newDBpassword 127.0.0.1 1521 MCDB
```

**b.** Enter the following to change the *network user-DB* password in the Prime Network software (the gateway server must be up and running):

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 setEncrypted 0.0.0.0 "site/persistency/nodes/main/PASS" network user-DB-new-password
```

**Step 3**  
To change the *network user-EP-DB* password (for the event persistence and archiving data):

**a.** Enter the following `sqlplus` command to change the *network user-EP-DB* password in the Oracle software:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
```

For example:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql system systempassword
network39_ep EPnewDBpassword 127.0.0.1 1521 MCDB
```

**b.** Enter the following to change the *network user-EP-DB* password in the Prime Network software (the gateway server must be up and running):

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 setEncrypted 0.0.0.0 "site/persistency/nodes/ep/PASS" network user-EP-DB-new-password
```

**Step 4**  
To change the *network user-DWE-DB* password (for the Workflow Engine data):

**a.** Enter the following `sqlplus` command to change the *network user-DWE-DB* password in the Oracle software:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
network user-DWE-DB network user-DWE-DB-new-password DB-IP DB-port SID
```

For example:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql system systempassword
network39_dwe DWEnewDBpassword 127.0.0.1 1521 MCDB
```

**b.** Enter the following to change the *network user-DWE-DB* password in the Prime Network software (the gateway server must be up and running):

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 setEncrypted 127.0.0.1 avm66/services/workflow/engine/databasePassword network user-DWE-DB-new-password
```
Step 5  To change the network user-admin-DB password (for administration and maintenance data):

a. Enter the following sqlplus command to change the network user-admin-DB password in the Oracle software:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
network user-admin-DB network user-admin-DB-new-password DB-IP DB-port SID
```

For example:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql system systempassword
network39_admin adminnewDBpassword 127.0.0.1 1521 MCDB
```

b. Enter the following to change the network user-admin-DB password in the Prime Network software (the gateway server must be up and running):

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 setEncrypted 0.0.0.0
"site/persistency/nodes/admin/PASS" network user-admin-DB-new-password
```

Step 6  To change the network user-XMP-DB password (for the Change and Configuration Management):

---

**Note** The password should not contain ampersand (@) or forward slash (/) characters. If you enter either of these special characters, future installations will fail.

---

a. Enter the following sqlplus command to change the network user-XMP-DB password in the Oracle software:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql DBA-username DBA-password
network user-XMP-DB network user-XMP-DB-new-password DB-IP DB-port SID
```

For example:

```
# sqlplus /nolog @$ANAHOME/Main/unix/setPassword.sql system systempassword
network39_xmp network39XMPnewDBpassword 127.0.0.1 1521 MCDB
```

b. Enter the following to change the network user-XMP-DB password in the Prime Network software:

```
# cd $XMP_HOME/bin
# xmpchangepw.ksh network user-XMP-DB-old-password network user-XMP-DB-new-password
```

Step 7  Stop the gateway server and units:

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

Step 8  Run the unlock command to ensure that the Prime Network Oracle accounts are not locked. A lock can happen if Prime Network accesses the database (which it does constantly) between the time when you run the sqlplus setpassword.sql command and the time when you run the runRegTool.sh or xmpchangepw.ksh scripts. In that period of time, the passwords are not in sync.

a. As the Oracle UNIX user, log in to sqlplus:

```
# sqlplus /nolog
SQL> connect /as sysdba
```

b. Run the unlock command. You need only run the unlock command on accounts that were changed—other words, in the following command, account-name can be network user, network user-EP-DB, network user-DWE-DB, or network user-XMP-DB from the previous steps.

```
SQL> alter user account-name account unlock
```
Step 9  

Start the gateway server and units:

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

---

## Changing Passwords: bosenable, bosconfig, and bosusermanager, and root

The passwords for bosenable, bosconfig, bosusermanager, and root are established during the Prime Network installation. Use the following to change the bos passwords.

To change the root password, you can use Changing a User’s Prime Network Password, page 7-24. If you have lost the root password, you can use this procedure to reset it.

### Step 1

Using an SSH session, log in to the Prime Network gateway as `network user`. (`network user` is the operating system account for the Prime Network application, created when Prime Network is installed; for example, `network39`.)

### Step 2

Switch to the Main directory:

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

### Step 3

Encrypt the new password in Prime Network using the following command:

```
java -classpath ./jars/classes.jar com.sheer.metromission.authentication2.PasswordEncrypt password
```

The encrypted password is listed in the command output (after the comma). You will need this information in Step 4.

For example, the following command creates a new password for `test`. The portion of the output that is in bold is what you will need in the subsequent step.

```
# java -classpath ./jars/classes.jar com.sheer.metromission.authentication2.PasswordEncrypt test
'test' -> 'PEv1:DC57A2A7', '7E84D3A8F60F30B7B62946D532E24608'
```

### Step 4

Log in to the Oracle database and change the password for bosenable, bosconfig, bosusermanager, and root in the database.

a. Log in to the Oracle database as `network user`. In the following example, `network user` is network39 and the `network user` password is admin.

```
sqlplus network39/admin
```

b. Change the password using the following command, where `xxx` is the second string of output from Step 3, and `user` is `bosenable`, `bosconfig`, `bosusermanager` or `root`. In this example, the bosenable password is being changed:

```
update bosuser set ENCRYPTEDPASSWORD='xxx' where username='bosenable';
```

For example:

```
SQL> update bosuser set ENCRYPTEDPASSWORD='7E84D3A8F60F30B7B62946D532E24608' where username='bosenable';
1 row updated.
```

To update the root user password, you would use the following command:
Changing Passwords: Diagnostics Tool

The username and password for the Diagnostics Tool (described in Obtaining Diagnostic Information Using Graphs, page 9-6) is established during the Prime Network installation.

To change the passwords:

**Step 1** Using an SSH session, log in to the Prime Network gateway as network user. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

**Step 2** Switch to the Main directory:
```
# cd $ANAHOME
```

**Step 3** Change the username and password for the Diagnostics tool using the following command, where operating-system is either linux or solaris, depending on your configuration:
```
# utils/operating-system/apache/bin/htpasswd ./Main/webroot/.passwd new-username
```

The utility will prompt you for a new password for new-username.

Running a Command on All Prime Network Units

The script rall.csh is a utility used to run 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
```

Using the vne_creation_script to Add VNEs

**Note** In general, you should use the Prime Network Administration GUI client to add VNEs. The GUI has built-in mechanisms to ensure that you enter data correctly.
The `vne_creation_script.pl` allows you to add VNEs in bulk. This includes Cloud VNEs, AVMs, and maps, and associating all of the VNEs to specific units. The `vne_creation_script.pl` resides in `NETWORKHOME/Main/scripts`. This script reads a configuration file with the relevant VNE information, adds the VNEs to Prime Network, and produces a report log file for your reference.

Follow these steps to import a list of VNEs into Prime Network:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>See:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Create a configuration file that contains the VNEs that you want to add.</td>
<td>Create the Configuration File, page 15-6</td>
</tr>
<tr>
<td>2.</td>
<td>If any of the VNEs to be imported use reduced polling, create a new version of the <code>vne_creation_script.pl</code> and update it to ensure that the reduced polling settings are preserved.</td>
<td>Additional Step for VNEs Using Reduced Polling, page 15-9</td>
</tr>
<tr>
<td>3.</td>
<td>Run the <code>vne_creation_script.pl</code> command.</td>
<td>Running the <code>vne_creation_script.pl</code>, page 15-10</td>
</tr>
</tbody>
</table>

**Create the Configuration File**

The `vne_creation_script.pl` script takes the name of a configuration file as its argument. The configuration file contains information about the VNEs that you want to add to Prime Network and uses a flat text file format.

Table 15-1 describes the format of the configuration file and how to enter the various types of information that describe your network.

**Note**

A defined variable will be applied to any applicable elements that follow it. For example, after adding an AVM, all VNEs will be added to that AVM until another AVM is defined. Similarly, all VNEs will use a configured scheme until another scheme is specified.
### Table 15-1  
**Supported Entries for a vne_creation_script.pl Configuration File**

<table>
<thead>
<tr>
<th>Format</th>
<th>Description and Usage Notes</th>
</tr>
</thead>
</table>
| `gateway gateway-IP`<br>`user root-user`<br>`password root-user-password`<br>`unit unit-IP | Adds the Prime Network gateway, units, and network user that will manage the items in the configuration file. The units are uplinked to the gateway.  
  - `root-user` is the root user for the Prime Network GUI applications.  
  - If no units are specified, enter the unit line as unit.  
  - `unit unit-ip` specifies additional unit server(s). Any AVMs or VNEs that follow will be allocated to that unit. If there are no other units, use `unit gw-ip`.  
  - `unit auto` specifies that any AVMs or VNEs that follow will be allocated among all available units. (See **Adding AVMs Using Auto-Add, page 4-8** and **How VNE Auto-Add Works, page 19-11**.) |
| `scheme scheme-name`<br>`[[vne-name] vne-IP vne-properties]` | Defines the scheme to be used by the VNEs listed in the lines that follow.  
  - Supported schemes are `ipcore`, `product`, or `default`.  
  - VNEs listed on the line that directly follow `scheme scheme-name` will use that scheme.  
  - To add a different scheme, enter `scheme scheme-name` on a new line, followed by VNEs that should use that scheme. |
| `avm {number [memory] | auto}}`<br>`[[vne-name] vne-IP vne-properties]` | Creates an AVM. If no VNEs follow the avm line, the AVM is created but is empty.  
  - `avm number [memory]` specifies additional AVMs (and, optionally, their memory allocation). Any VNEs that follow will be allocated to that AVM.  
  - `avm auto` specifies that any VNEs that follow will be auto-allocated among all of the AVMs in the previously-created unit (or gateway, if no units are created). |
| `[vne-name] vne-IP vne-properties` | Creates a VNE with the specified properties.  
  - If `vne-name` is not supplied, device will use SYSNAME. See **Table 15-2** for `vne-properties` format guidelines.  
  - If a VNE definition does not directly follow an AVM declaration, the VNE creation will fail (the log will contain error information).  
  - If a VNE definition is mistakenly repeated but has conflicting information, the VNE creation is ignored (the log will contain error information). |
| `cloud-vne-name vne-IP cloud` | Creates a Cloud VNE. |
| `[map map-name]`<br>`[[vne-name] vne-IP vne-properties]`<br>`[map]` | (Optional) Creates a map named `map-name`. If you do not want to create any maps, do not supply a name.  
  - VNEs listed on the line that follows `map map-name` will be added to that AVM.  
  - To continue to create VNEs but stop adding them to a map, end the VNEs list with the word `map` (with no `map-name` argument). |
| `load avm-number ...` | (Optional) Starts the AVMs after they have been created. You can leave this line out and manually start AVMs after they are created. |
| `read_file BQL-filename` | Places the specified BQL file content into the gateway. (This can be used for adding static links.)  
  For information on BQL, see the **Cisco Prime Network Integration Developer Guide**. |

---

1. VNEs are allocated as long as there is a “safe target AVM” in the system. See **How VNE Auto-Add Works, page 19-11**.
VNEs are added using the format [vne-name] vne-ip vne-properties, as described in the previous table. The values for vne-properties depend on the protocols and credentials for the device. Table 15-2 provides guidelines for adding VNEs to a configuration file.

**Note**
If you do not enter any SNMP read/write information, Prime Network uses public/private.

**Note**
If Prime Network is installed with Cisco Prime Central, be sure to use a device’s SYSNAME as its VNE name. This allows the device to be recognized across the common inventory. Also, do not use None or All as the SYSNAME, because those names have internal meaning to Cisco Prime Central.

### Table 15-2 Defining VNEs in a vne_creation_script.pl Configuration File

<table>
<thead>
<tr>
<th>Value for vne-properties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>telnet **** telnet-seq [snmpr read-commu-string] [snmpw write-comm-string] ****</td>
<td>Creates a VNE that uses Telnet with SNMP v1.</td>
</tr>
<tr>
<td>sshv1 username;password;prompt_sequence [snmpr read-community-string]</td>
<td>Creates a VNE that uses SSH v1 with SNMP v2.</td>
</tr>
<tr>
<td>sshv2 username;password;server-auth[pre-fingerprint];prompt_sequence [snmpr read-community-string]</td>
<td>Creates a VNE that uses SSH v2 with SNMPv3. server-auth can be none, save, or pre. If you use pre, enter it as: pre;fingerprint</td>
</tr>
<tr>
<td>sshv3 username;password;server-auth[pre-fingerprint];prompt_sequence [snmpr read-community-string]</td>
<td></td>
</tr>
</tbody>
</table>

When you are done, your configuration file might resemble the following:

gateway 192.1.1.1
user root
password rootpassword
unit 192.2.2.2
avm 150 1024
VNE_example5 5.5.5.5 telnet ":,admin,Router>,enable,,:,admin,Router#,
load 150

scheme ipcore

avm 200 1024
VNE_example6 6.6.6.6 telnet ":,admin,Router>,enable,,:,admin,Router#,
load 200

avm auto
map mymap
VNE_example1 1.1.1.1 telnet "Password:,admin,myPrompt#" snmpr snmpReadComm snmpw
snmpWriteComm
VNE_example2 2.2.2.2 sshv1 des;myUser;myPassword;:,admin,myPrompt# snmpr public
VNE_example3 3.3.3.3 sshv2 myUser;myPass;none;# snmpr public snmpv3
sha;myUser;myPass;des;myEncPass
4.4.4.4 telnet "Password:,admin,myPrompt#" snmpr snmpReadComm snmpw snmpWriteComm
map
Using the vne_creation_script to Add VNEs

Additional Step for VNEs Using Reduced Polling

If any of the VNEs are using reduced polling, you must modify the vne_creation_script.pl file to add instructions that will preserve the reduced polling settings after the import. We recommend you create a special form of the script which you can use with reduced polling VNEs. Other VNEs can use the standard script.

The following procedure adds the necessary information to three points in the script.

---

**Step 1** Log into the Prime Network gateway as user network user. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

**Step 2** Go to NETWORKHOME/Main/scripts.

**Step 3** Create a copy of vne_creation_script.pl and give it a meaningful name; for example:

```
# copy vne_creation_script.pl vne_reducedpolling_creation_script.pl
```

**Step 4** Open the new script file with a text editor.

**Step 5** Locate the three instances of the $add_agent_command variables, which appear below the sub set_bql_commands. You can locate the instances using the following information:

<table>
<thead>
<tr>
<th>Variable Instance</th>
<th>Instance is preceded with the following text:</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNEs that use Telnet</td>
<td>$telnet_used = 0 ; $add_agent_command...</td>
</tr>
<tr>
<td>VNEs that use SSHv1</td>
<td>} elsif ($sshv1_used){ $sshv1_used = 0; $add_agent_command...</td>
</tr>
<tr>
<td>VNEs that do not use Telnet or SSHv1</td>
<td>} else { $add_agent_command...</td>
</tr>
</tbody>
</table>

**Step 6** Add the following line to end of the $add_agent_command variable:

```
<ReducedPollingMode type="com.sheer.types.enums.ReducedPollingModeEnum">Reduced polling (event-based) *</ReducedPollingMode>
```

**Step 7** Save the file and exit the text editor.

The following is an example of an $add_agent_command definition after being edited:

```
...<SnmpVersionEnum type="Integer">$_snmpv3_enum</SnmpVersionEnum>
<TelnetEnabled type="Boolean">true</TelnetEnabled>
<TelnetSequence type="String">$tel_seq</TelnetSequence>
<ReducedPollingMode type="com.sheer.types.enums.ReducedPollingModeEnum">*
Reduced polling (event-based) *</ReducedPollingMode>
</management.IElementManagement>
```
Running the vne_creation_script.pl

Log into the Prime Network gateway as user *network user* to run this command. (*network user* is the operating system account for the Prime Network application, created when Prime Network is installed; for example, *network39*.)

The *vne_creation_script.pl* script uses the following command format:

```
perl vne_creation_script.pl configuration_filename
```

The command will display output similar to the following.

```
+ Trying to login.                          [OK]
+ Executing commands.                       [OK]
+ Logs:
  - Log file path: /export/home/network39/Main/logs/vneCreation081811-185112.txt
  - Verbose log file path:
    /export/home/network39/Main/logs/vneCreation081811-185112.verbose

Finished with: 0 ERRORs 0 WARNINGS
```

When the *vne_creation_script.pl* script has successfully executed, you can view the additions in Prime Network Administration or the log files. The log files are placed in *NETWORKHOME*/*Main/logs* and are named vneCreation-*mmddyy-hhmss*.txt and vneCreation-*mmddyy-hhmss*.verbose.

If errors appear, check your setup in Prime Network Administration, correct the configuration file accordingly, and run the command again.
Unit Server High Availability and AVM Protection

The unit server high availability and AVM protections architecture ensures continuous availability of Prime Network functionality by detecting and recovering from a wide range of hardware and software failures. The distributed design of the system enables the impact radius caused by a single fault to be confined. This prevents all types of faults from setting into motion the “domino” effect, which can lead to a crash of all the management services.

These topics describe how you can use Prime Network for unit redundancy and process protection:

- Overview of Unit Server High Availability, page 16-1
- Creating Unit Protection Groups and Designating Standby Units, page 16-8
- Managing the Watchdog Protocol (AVM Protection), page 16-10
- High Availability Registry Settings, page 16-11

For information on high availability for gateway servers, see Using Veritas Gateway Server High Availability, page 17-1 and Using RHCS/ADG Gateway Server High Availability, page 18-1.

Overview of Unit Server High Availability

High availability of the server backbone is achieved at several complementary levels. For example:

- NEBS-3 compliant carrier-class server hardware.
- Watchdog within each unit, responsible for monitoring and, if necessary, automatically reloading failed processes.
- N+m warm standby protection for unit groups.

See the following topics for more information:

- Watchdog Protocol for AVM Protection, page 16-1
- Unit N+m High Availability, page 16-2

Watchdog Protocol for AVM Protection

The watchdog protocol monitors the AVM processes to make sure any AVMs that have failed are restarted. This is called AVM protection and the GUI, the watchdog protocol is controlled by the AVM Protection check box. Each unit executes several processes: one control process and several AVM processes that execute VNEs. Each process within the unit is completely independent. The isolation
Overview of Unit Server High Availability

concept is tailored throughout the design so that a failure of a single process does not affect other processes on the same machine. The exact number of processes on each unit depends on the capacity and computational power of the unit.

The control process executes a watchdog protocol, which continuously monitors all other processes on the unit. This watchdog protocol requires each AVM process to continuously handshake with the control process. A process that fails to handshake with the control process after a number of times is automatically cancelled and reloaded.

The dynamic design of the control process implements runtime adaptation and escalation. The escalation procedure moves the AVM to suspended mode; that is, the process is suspended. An example of an escalation procedure is to stop reloading a process that has crashed more than \( n \) times within a given period, because it is suspected of having a recurring software problem.

The reload process is local to the unit, and thus very rapid, with a minimal amount of downtime. In many cases the process can use its previous cache information (temporary persistency used to improve performance), once the stuck process is detected, reloading the process takes only a few seconds with no data loss. This is the case for user-created AVMs that are hosting VNEs. However, for reserved AVMs that perform special function in Prime Network, some data loss will occur. All watchdog activity is logged and an alarm is generated and sent when the watchdog reloads a process.

Note

An alarm persistency mechanism enables the system to clear alarms that relate to events that occurred while a VNE, an AVM, a unit, or the whole system was down, thus preserving system integrity. For more information about alarm persistency, see Chapter 26, “VNE Persistency Mechanism.”

All watchdog protocol parameters, such as pulse interval and retry times, are configurable in the registry. The higher these parameter values are, the longer the AVM or unit failure lasts, but this increases the certainty that a failure has actually occurred. Configuring these parameters with lower values may shorten the AVM or unit recovery, but might result in a “false positive” which could unnecessarily restart an AVM or revert to a standby unit when the AVM is just busy or the unit is processing a heavy load of data. For information on these registry settings, see High Availability Registry Settings, page 16-11.

Unit N+m High Availability

The clustered N+m unit server high availability mechanism uses the Prime Network fabric is designed to handle the failure of a unit. Such failures include hardware failures, operating system failures, power failures, and network failures, which disconnect a unit from the Prime Network fabric.

Unit availability is established in the gateway, running a protection manager process, which continuously monitors all the units in the network. Once 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), taking over all of its managed network elements. This design provides many possibilities for trading off protection and resources. These possibilities range from segmenting the network into clusters without any extra machines, to having a warm-swappable empty unit for each unit in the setup.

When the Prime Network software is installed on a unit, the unit can be designated as active or standby. Using the GUI, you can designate a group of active and standby units to belong to a protection group, giving the group the name of your choice. A protection group can have multiple standby units, and you can define more than a single protection group.

A unit switchover results in the unavoidable loss of information. The impact depends on how long the unit is down, and the functions the unit performed.
Figure 16-1 shows a protection group (cluster) of units controlled by a gateway with one unit configured as the standby for the protection group.

**Figure 16-1  Prime Network Protection Groups—Example**

In the example configuration, when the gateway determines that one of the units in the protection group has failed, it notifies the standby unit of the protection group to immediately load the configuration of the failed unit. The standby unit loads the configuration of the failed unit, including all AVMs and VNEs, and functions as the failed unit. We recommend that you have two standby units per cluster. In this case, if a unit fails, another standby unit is still available.

Because events are recorded in Prime Network Events, you can check for the specific problem and take action to bring the failed unit up again.

**AVM 100 and Unit Server High Availability**

You can configure AVM 100 to run on a unit instead of the gateway. If the unit is also configured with high availability, the AVM 100 on the standby unit will drop all events because it is not running. This is by design; it should not start until a switchover occurs.

The standby unit contains a port watchdog script that listens for events on the unit’s Syslog and SNMP ports. The script prevents unnecessary ICMP unreachable messages being sent back to the network. If a switchover occurs, the standby unit and AVM 100 will start, and the watchdog script releases the ports.

When the original unit comes back up, the standby AVM 100 goes back down, and the watchdog script recommences listening on the standby unit’s Syslog and SNMP ports.
Overview of Unit Server High Availability

Recommendations for Configuring High Availability

Keep the following guidelines in mind when configuring protection groups:

- Units in a protection group must have the same operating system.
- Protection groups should be designed according to geography.
- For heavily loaded protection groups, add an additional standby unit.
- Units (active and standby) should not be assigned to more than one protection group.

Estimating the Impact of Unit or AVM Failures

When a failure occurs in a unit or AVM, the length of time that the system is down depends on the type of failure, how long it takes to detect that the component is not working, and the length of the recovery period (during which the unit or AVM reloads and the system begins to function normally again). Three types of failure can occur, as described in these topics:

- Impact of Catastrophic AVM Process Failure, page 16-4
- Impact of AVM Timeouts and Restarts, page 16-6
- Impact of Unit Timeouts and Switchovers, page 16-8

Impact of Catastrophic AVM Process Failure

Each AVM has a log file which is constantly monitored by a Perl process for log messages about catastrophic failures, such as AVM processes running out of memory. When such a failure occurs, the Perl process restarts the AVM almost immediately, so the mean time to repair (MTTR) is based on the AVM loading life cycle.

Table 16-1 describes the impact on different AVMs when experiencing such a failure.

Table 16-1  Catastrophic Process Failure Impact on AVMs

<table>
<thead>
<tr>
<th>AVM Process</th>
<th>Results of AVM Failure</th>
<th>Average Time To Repair Failed AVM</th>
<th>Degree of Impact to System if AVM Fails</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVM 0 (High availability/ switch)</td>
<td>Loss of messages to and from the machine.</td>
<td>1 minute to reach bootstrap.</td>
<td>High. Messages are constantly being sent and received in the system.</td>
</tr>
<tr>
<td>AVM 11 (Gateway)</td>
<td>Loss of persistence information for faults (except for the I persistency information handled by AVM 25 and AVM 100). No user authentication will be performed on gateway connections, and GUI clients will lose gateway connectivity.</td>
<td>6-10 minutes to reach bootstrap.</td>
<td>High. AVM 11 handles Oracle communication and various gateway functions such as alarm processing.</td>
</tr>
</tbody>
</table>
Table 16-1  Catastrophic Process Failure Impact on AVMs (continued)

<table>
<thead>
<tr>
<th>AVM Process</th>
<th>Results of AVM Failure</th>
<th>Average Time To Repair Failed AVM</th>
<th>Degree of Impact to System if AVM Fails</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVM 25 (Event persistence)</td>
<td>Loss of persistence information and new tickets for actionable network events that are processed while AVM 25 is down. When it comes up, new events that correlate to “lost” events will be persisted but will not be associated with a ticket until the integrity process identifies the broken chains (due to lost events) and opens new tickets.</td>
<td>1 minute to reach bootstrap.</td>
<td>High. Network events are constantly processed in a live, scaled system.</td>
</tr>
<tr>
<td>AVM 35 (Service discovery)</td>
<td>Network services displayed on maps (such as Ethernet service and MPLS-TP) are not updated to reflect network changes.</td>
<td>1 minute to reach bootstrap, plus several minutes to redisplay already discovered services, plus time required to detect changes that occurred when the AVM was down (30 minutes to 10 hours, depending on number, type, services, etc.).</td>
<td>Low: Network services display would be updated after a discovery resynch process is finished.</td>
</tr>
<tr>
<td>AVM 66 (Workflow engine)</td>
<td>Running workflows would abort and scheduled workflows would not run. Templates would not be deployed.</td>
<td>1 minute to reach bootstrap, but with large number of workflows in the system, this may increase.</td>
<td>Low, because AVM 66 should sustain a large number of executed workflows (per the system limitations). Templates would need to be redeployed and aborted workflows would need to be rerun. Check the Provisioning events in Prime Network Events to verify what ran prior to failure, and then issue an rollback (no automatic rollback is done).</td>
</tr>
<tr>
<td>AVM 76 (Job scheduler)</td>
<td>No jobs can be added, executed, or removed.</td>
<td>1 minute to reach bootstrap.</td>
<td>Depends on job types.</td>
</tr>
<tr>
<td>AVM 77 (Change and Configuration Management)</td>
<td>Loss of device configuration changes. Configuration changes will not be backed up to the archive during down time.</td>
<td>10 minutes for DM server startup and bundle deployment, plus time to fetch all configurations for managed devices.</td>
<td>High (if using Change and Configuration Management); because configuration change notifications can happen all the time.</td>
</tr>
<tr>
<td>AVM 78 (VNE topology)</td>
<td>Topology links between VNEs on different units will not be discovered.</td>
<td>1 minute to reach bootstrap.</td>
<td>Low; there may be some missing topology links.</td>
</tr>
<tr>
<td>AVM 83 (TFTP server for Change and Configuration Management)</td>
<td>Change and configuration management TFTP operations will fail. (Operations using secure protocol or FTP will not be affected.)</td>
<td>5 minutes.</td>
<td>High (if using Change and Configuration Management); Change and Configuration Management device properties would fail.</td>
</tr>
</tbody>
</table>
Table 16-1  Catastrophic Process Failure Impact on AVMs (continued)

<table>
<thead>
<tr>
<th>AVM Process</th>
<th>Results of AVM Failure</th>
<th>Average Time To Repair Failed AVM</th>
<th>Degree of Impact to System if AVM Fails</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVM 84 (Reports)</td>
<td>Loss of reports. When AVM 84 is down running reports will fail.</td>
<td>1 minute.</td>
<td>Low; reports would need to be rerun.</td>
</tr>
<tr>
<td>AVM 99 (Management)</td>
<td>Loss of registry notifications on changes made to golden source registry.</td>
<td>1 minute to reach bootstrap.</td>
<td>Low, because registry modifications are made only when the VNE is first loaded into the system. Modifications are rarely made while the system is up and running. For the first 30 minutes after AVM 99 has started, there is no system monitoring for unit server high availability. This allows the system enough time to get up and running</td>
</tr>
<tr>
<td>AVM 100 (Event Collector)</td>
<td>Loss of traps and syslogs from devices, including raw event persistency.</td>
<td>1 minute to reach bootstrap, plus time for all the VNEs to register again for traps and syslogs. Normally a matter of minutes.</td>
<td>High, because raw events from devices are constantly received in a live, scaled system. Only devices registered to the failed AVM 100 are affected. No events will be handled during downtime. See AVM 100 and Unit Server High Availability, page 16-3. (Raw event persistency is recovered before events are forwarded to the VNEs.)</td>
</tr>
<tr>
<td>AVM 101-999 (User-defined AVMs)</td>
<td>Loss of management to a section of devices managed by the AVM; alarm state inconsistencies (user will have to clear tickets).</td>
<td>1 minute to reach bootstrap, plus time to load the VNEs (depending on number, type, services, etc.).</td>
<td>High (but only for a period of one minute), because no raw events sent to the VNEs can be processed when the AVM is down.</td>
</tr>
</tbody>
</table>

Impact of AVM Timeouts and Restarts

Each AVM is constantly monitored by the management AVM (AVM 99) using a watchdog protocol pulse message sent to the AVM at preconfigured intervals. When the AVM fails to respond to the pulse message after a preconfigured number of attempts, the management AVM restarts the process.

The management process also keeps a history of the number of times it has restarted the AVM. When it reaches the maximum number of preconfigured restart times, the management AVM stops restarting the AVM because this indicates a serious problem with the AVM. Each restart is logged as a System event except when AVM 11 is restarted, because this AVM handles all persistency.

Failures on AVMs in the system are measured in a way similar to that used for catastrophic process failures (see Table 16-1), with the addition of the watchdog protocol overhead. This is measured by the pulse interval multiplied by the number of restart attempts.

Keep the following in mind when evaluating an AVM failure:

- The maximum number of preconfigured restart times is five, after which the management process does not try to reload the AVM.
- It takes approximately one minute for the system to detect that an AVM (including AVM 100) is not working.
• The recovery period during which an AVM (including AVM 100) reloads and the system starts to function normally again is approximately five minutes, depending on the number of VNEs per AVM and the complexity of each.

Figure 16-2 provides a typical example of how unit server high availability timer parameters work while monitoring AVMs.

If you are using gateway server high availability, note that there is no overlapping between the processes that AVM 99 monitors that are illustrated in Figure 16-2, and the process that Veritas Cluster Manager monitors (the ANA Gateway Veritas agent). For an illustration, see Figure 17-7 on page 17-10.

**Measuring Fault-Processing Down Time for AVMs**

When a failure occurs on an AVM, the time during which ticket processing is down is measured as the sum of the following factors:

- The time it takes to determine that the AVM has failed.
- The time it takes for the AVM to reload, depending on the number of VNEs.
- The time it takes to pass syslogs or traps to the VNEs (in the case of AVM 100), or to pass events to the gateway (in the case of AVM 101-999).
Chapter 16  Unit Server High Availability and AVM Protection

Creating Unit Protection Groups and Designating Standby Units

Note
For the first 30 minutes after AVM 99 (the management AVM) has started, there is no monitoring of the system to find unit server high availability issues. This allows the system enough time to get up and running.

Impact of Unit Timeouts and Switchovers

The Prime Network gateway constantly monitors units by sending a watchdog protocol pulse message to the unit management AVM at preconfigured intervals. If the unit management AVM fails to respond to the pulse message after a preconfigured number of retries, the gateway loads the standby unit to replace it.

The impact of such a failure on the system is that the unresponsive unit does not manage the devices for a period of time. This unmanaged period of time is measured by the pulse interval multiplied by the number of retry times, plus the unit load time.

Note
Unit load time depends on the configuration of the unit—the hardware, the number of VNEs, the types of VNEs, and the services running on the VNEs. All of these factors impact the load time required for the VNEs to complete their modeling, as described in Table 16-1.

(On the other hand, if the problematic unit has not completely failed and continues to operate after the switchover, you may see duplicate events in the database. In this case you should stop the original problematic unit using networkctl stop.)

Measuring Ticket-Processing Down Time for Units

When a failure occurs on a unit, the time during which ticket processing is down is measured as the sum of the following factors:

- The time it takes to determine that the unit has failed (depending on the ping interval).
- The time it takes for the unit to reload, depending on the number of AVMs and VNEs in the unit.
- The time it takes to pass correlated events to the gateway (a minimum of five minutes to obtain device history, plus a variable time depending on the number of VNEs per AVM).

Creating Unit Protection Groups and Designating Standby Units

New units are added to Prime Network using the installation scripts described in the Cisco Prime Network 3.9 Installation Guide. By default, units are added to a protection group named default-pg. Each protection group, or cluster of units, should have at least two standby unit servers.

Note
Units in a protection group must have the same operating system.

These topics explain how to create new protection groups and work with standby units:

- Creating a Protection Group and Adding Units to the New Group, page 16-9
- Switching to a Standby Unit, page 16-9
Creating a Protection Group and Adding Units to the New Group

By default, all units in the Prime Network fabric belong to one group (or cluster), the default-pg protection group. You can create additional groups as your network grows. You should have at least two standby units for each cluster.

Note
Units in a protection group must have the same operating system.

To create or edit a protection group:

**Step 1**
Create the new protection group.

a. Choose **Global Settings > Protection Groups**.

b. Open the New Protection Group dialog box by right-clicking **Protection Groups**, then choose **New Protection Group**. For an existing group, right-click the group and choose **Properties**.

c. Enter a name and description, or edit the description.

d. Click **OK**. The content area displays details of the new protection group and all currently defined protection groups in the Protection Groups table.

**Step 2**
Add units to the new protection group.

a. Right-click the unit and select **Properties**.

b. In the Protection Group drop-down list, select the new protection group and click **OK**.

Switching to a Standby Unit

Prime Network Administration enables you to switch to a standby unit either manually or automatically.

- Automatic switchover to a standby unit occurs when the gateway discovers that one of the active units has failed. Such failures include hardware failures, operating system failures, power failures, and network failures, which disconnect a unit from the Prime Network fabric. For more information on automatic switchover, see **Unit N+m High Availability**, page 16-2.

  If the problematic unit has not completely failed and continues to operate after the switchover, you may see duplicate events in the database. In this case you should stop the original problematic unit using `networkctl stop`.

- Manually switching to a standby unit is useful if you must temporarily shut down the unit for maintenance.

When a switchover occurs, Prime Network automatically transfers all data from the failed unit to a standby unit in the same protection group. The original unit is removed from the standby setup and is no longer displayed in Prime Network Administration.

Note
When a unit switches to its standby, all VNEs on the unit that were in maintenance mode will be moved to the VNE Down state.
Managing the Watchdog Protocol (AVM Protection)

To manually switch to a standby unit:

- **Step 1** Expand the All Servers branch and select the required unit.
- **Step 2** Right-click the required unit, then choose **Switch**. A confirmation message is displayed.
- **Step 3** Click **Yes**. The standby unit becomes the active unit and is displayed in the All Servers branch. The original unit is removed from the setup and can be safely shut down. It is no longer displayed in the Prime Network Administration window.

**Note** In the event of unit failover, the Prime Network gateway randomly selects a redundant unit when more than one standby unit is available.

Managing the Watchdog Protocol (AVM Protection)

The following topics describe how to define AVMs for units and enable or disable protection (the watchdog protocol) on the AVM:

- Enabling AVM Protection (Watchdog Protocol) on AVMs, page 16-10

**Enabling AVM Protection (Watchdog Protocol) on AVMs**

Every AVM in the Prime Network fabric is, by default, managed by the watchdog protocol. Prime Network Administration enables you to define AVMs for units and enable or disable the watchdog protocol on each AVM.

To define an AVM:

- The unit must be installed.
- The unit must be connected to the transport network.
- The following default AVMs must be running:
  - AVM 0—The switch AVM.
  - AVM 99—The management AVM.
  - AVM 100—The trap management AVM (one instance must be running either on the gateway server or one of the units).
- The new AVM must have a unique identifier within the unit.

**Note** For detailed information on defining AVMs, see Viewing AVM Properties, page 4-6.

To enable AVM protection on an AVM:

- **Step 1** Open the New AVM dialog box by right-clicking the required unit (or gateway), then choose **New AVM**.
- **Step 2** Define the properties of the AVM. For more information, see Viewing AVM Properties, page 4-6.
Step 3  Check the Enable AVM Protection check box to enable the watchdog protocol.

Note  We strongly recommended that you do not uncheck the Enable AVM Protection check box.

Step 4  Click OK. The new AVM, with the watchdog protocol enabled, is added to the selected unit and is displayed in the content area.

Adding the new AVM creates the registry information for the new AVM in the specified unit. The AVM can now host VNEs.

Viewing and Changing AVM Protection (Watchdog Protocol) Settings

Note  For detailed information on defining and editing AVMs, see Chapter 4, “Basic AVM and VNE Administration Tasks.”

To view and edit AVM settings:

Step 1  Open the AVM Properties dialog box by right-clicking the required AVM, then choose Properties.

Step 2  Edit the details of the AVM, as required.

Note  We strongly recommended that you do not uncheck the Enable AVM Protection check box.

Step 3  Click OK. The new properties for the AVM are displayed in the content area.

High Availability Registry Settings

The high availability and AVM watchdog protocol functions are controlled by settings in the registry. The registry entries and default values are provided in Table 16-2.

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

Table 16-2  Registry Settings for Unit Server High Availability and AVM Watchdog Protocol

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent_defaults/delay</td>
<td>Grace period (in milliseconds) during which events are not raised. The grace period begins at system startup. It defines the amount of time during which the system does not perform high availability operations of any kind on the configured target (either the AVM or the unit). There is one exception: When the configured target responds for the first time with a ping, the grace period is over.</td>
<td>1800000 (30 minutes)</td>
</tr>
</tbody>
</table>
Table 16-2  Registry Settings for Unit Server High Availability and AVM Watchdog Protocol (continued)

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent_defaults/timeout</td>
<td>Timeout (in milliseconds) for AVMs. This is the initial recovery period. This period includes device polling and inventory buildup. End-to-end services, such as RCA and topology, can take longer before they become available.</td>
<td>300000 (5 minutes)</td>
</tr>
<tr>
<td>haservice/timeout</td>
<td>Timeout (in milliseconds) for units.</td>
<td>300000 (5 minutes)</td>
</tr>
<tr>
<td>agent_defaults/maxTimeoutReloadTime</td>
<td>Threshold (in milliseconds) for AVM reload retries. When exceeded, the AVM is suspended.</td>
<td>1800000 (180 minutes)</td>
</tr>
<tr>
<td>agent_defaults/maxTimeoutReloadTries</td>
<td>Maximum number of retries for AVM reloads. When exceeded, the AVM is suspended.</td>
<td>5</td>
</tr>
</tbody>
</table>
Using Veritas Gateway Server High Availability

These topics describe the gateway server high availability solutions that use Veritas software. Use the architecture described in these topics as a reference point and adjust them to meet the needs of specific deployments. Both the local redundancy and geographic redundancy configurations are independent of and compatible with the unit server high availability mechanism (described in Unit Server High Availability and AVM Protection, page 16-1).

- Veritas Gateway Server High Availability Architecture, page 17-1
- Veritas Local Redundancy, page 17-6
- Veritas Geographical Redundancy, page 17-13

For information on the gateway server high availability solution that uses Red Hat Cluster Suite and Oracle Active Data Guard, see Using RHCS/ADG Gateway Server High Availability, page 18-1.

Veritas Gateway Server High Availability Architecture

While different deployments may necessitate different architectures, the architecture described in these topics can be used as a reference point and be adjusted to meet the needs of specific deployments. Both the local redundancy and geographic redundancy configurations are independent of and compatible with the unit server high availability mechanism (described in Unit Server High Availability and AVM Protection, page 16-1). However, do not manage remote failover through unit server high availability. For example, a unit at a local site should not have a standby unit (and protection group) at the remote failover site. Members of a unit protection group should be at the same site.

Veritas Local Redundancy

Gateway local redundancy is implemented as a 1+1 warm standby in a dual-node cluster, as shown in Figure 17-1. This architecture consists of one cluster that contains two servers, both of which are normally active:

- One Prime Network (P1) server which hosts the Prime Network gateway processes. The Prime Network server has its own logical IP address.
- One Oracle (P2) server which hosts the Oracle database application. The Oracle server also has its own logical IP address.

Both servers are active during normal operation. Each server provides redundancy for the other server in case of failure.
The license directory \textit{NETWORKHOME/Main/ha/licenses} should contain a copy of all license files for both nodes. This directory will be available to both nodes because it is part of the partition that is shared. If you add new licenses, you must copy them to this directory and run the \texttt{resetLicenses.pl} command to read the licenses. See \textit{Licensing and Gateway Server High Availability}, page 5-2.

The Prime Network and Oracle applications maintain their data on separate external volumes. Each external volume is connected to both the Prime Network and Oracle servers using redundant connections. The external volumes can be mounted on either server using VxVM. The two servers maintain a heartbeat between them that allows the VCS application (running on each server) to monitor the health of the other server.

\textit{Figure 17-1 Architecture for Veritas Gateway Local Redundancy}

For hardware and software requirements for local redundancy, see the \textit{Cisco Prime Network 3.9 Installation Guide}. 
Chapter 17      Using Veritas Gateway Server High Availability

Veritas Gateway Server High Availability Architecture

Veritas Geographical Redundancy

Gateway geographical redundancy is implemented by taking the dual-node cluster (used in the local redundancy configuration) and adding an additional single-node cluster at a geographically remote site, which acts a 1+1 cold standby for the primary cluster. The two clusters form a single global cluster using the VCS Global Cluster option.

This architecture consists of two clusters, as follows:

- The primary or local site (dual-node cluster) has the same characteristics as the Local Redundancy architecture—that is, it contains two servers (P1 and P2) and two external data volumes. One server hosts the Prime Network gateway processes, and the other server hosts the Oracle database application.
- The secondary or remote site (single-node cluster) has the following characteristics:
  - Contains a single server (S1) which is normally running but has no active applications.
  - Is connected to two additional external data volumes that are replicas of the two data volumes (Prime Network and Oracle data) at the primary site. If the primary site fails over, these additional data volumes become the primary copy of the system data.

The license directory NETWORKHOME/Main/ha/licenses on the active gateway should contain a copy of all license files for all servers. This directory will be available to all servers because it is part of the Prime Network partition that is replicated among servers. If you add new licenses, you must copy them to this directory and run the resetLicenses.pl command to read the licenses. See Licensing and Gateway Server High Availability, page 5-2.

Replication is performed either using VVR or via storage-based replication.

The local and remote clusters maintain a heartbeat over the IP network that allows the VCS application on each server to monitor the health of the other servers.

An example of a global cluster that implements geographical redundancy is provided in Figure 17-2.
In the geographical redundancy solution illustrated in Figure 17-2, only the gateway is protected. A full disaster recovery capability may require an additional set of unit servers at the remote site. This is illustrated in Figure 17-3.
If a failure at the local site is also likely to affect any local unit servers, consider placing additional units at the remote site. The remote unit servers can provide full or partial geographical redundancy, as needed.

**Note**

In this configuration, unit redundancy does not mean the units at both the local and remote sites are managed by the unit server high availability feature. The unit redundancy illustrated here differs from unit server high availability in two ways: in this scenario, the units are up but have no running AVMs, and after failover, you must manually move the AVMs between the two sites. (In unit server high availability, standby units are down until failover, and AVMs are automatically moved at failover.)

If a local site failure occurs and the local units are not affected, you can connect them to the redundant server at the remote single-node cluster. (Depending on the distance between the local units and remote server, communication may be significantly slower.)

Detailed requirements (hardware, software, and network) for both configurations are provided in the *Cisco Prime Network 3.9 Installation Guide*. 
Veritas Local Redundancy

The following topics provide additional information on how to manage a local redundancy configuration:

- **Configuration Details for Veritas Local Redundancy (Dual-Node Cluster), page 17-6**, describes how the different components of a locally redundant network work together, including disks, partitions, IP addresses, service groups, and application dependency.

- **How Automatic Failover is Triggered (Veritas Local Redundancy), page 17-11**, describes how automatic failover is triggered, and how the Prime Network and Oracle applications react.

### Configuration Details for Veritas Local Redundancy (Dual-Node Cluster)

The local redundancy configuration includes a dual-node cluster, and the two servers are both normally active. One server hosts the Prime Network gateway processes and has its own logical IP address; the other server hosts the Oracle database application and has its own logical IP address. Each server has its own external data volume. The hardware configuration is illustrated in Figure 17-4.

**Figure 17-4   Hardware Configuration for Dual-Node Cluster in Veritas Local Redundancy**

- Dual Gigabit Ethernet connections to different switches on LAN backbone for network and backup heartbeat
- Dual Gigabit Ethernet crossover connections for heartbeat
- Dual connections from each server to the external disk storage unit
- Database:
  - 1 or more data volumes
  - 1 archive volume
  - 1 redo log volume
  - 1 backup volume (embedded database only)
  - 1 SRL volume, all with mirroring/RAID protection
- Cisco Prime Network:
  - 1 ANA volume with mirroring/RAID protection
  - 1 SRL volume with mirroring/RAID protection
- Oracle database server:
  - 2 internal disks
  - (1 OS + 1 mirror)
Disks and Replication

The disks in the external storage (where the Prime Network and Oracle data resides) are managed by VxVm. For the primary site, some type of redundancy method should be used, such as mirroring or RAID.

In both cases, the specific disk being used at any time is transparent to the user. If a disk fails, the system will automatically failover to the redundant disk for continuous operation.

Disk Partitions

The internal disk on each server in the dual-node cluster contains the root (/) partition. Only the operating system and Veritas software are installed on this root partition. A server’s root partition is completely independent of the redundant server’s root partition. If you make any changes to any of the system files on one of the servers (such as /etc/system, /etc/hosts, /etc/passwd, or /etc/group), you must also manually make the change on the redundant server.

The disks on which the Prime Network and Oracle data resides are divided into multiple volumes. These volumes correspond to the partitions in Table 17-1.

Table 17-1 Disk Partitions for Veritas Local Redundancy

<table>
<thead>
<tr>
<th>Partition</th>
<th>Contents</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>/export/home</td>
<td>Prime Network application and registry</td>
<td>Yes</td>
</tr>
<tr>
<td>/opt/db</td>
<td>Oracle application and data files</td>
<td>Yes</td>
</tr>
<tr>
<td>/opt/dbarch</td>
<td>Oracle archive files</td>
<td>Yes</td>
</tr>
<tr>
<td>/opt/dbbackup</td>
<td>Oracle backup files</td>
<td>Yes</td>
</tr>
<tr>
<td>/opt/dblogs</td>
<td>Oracle log files</td>
<td>Yes</td>
</tr>
<tr>
<td>/opt/dbdata</td>
<td>Additional partition for Oracle data files (can be added on separate external volume if you want more historical data)</td>
<td>No</td>
</tr>
</tbody>
</table>

1. For information on embedded databases, see Working With an Embedded Database, page 11-1.

For geographical redundancy, if using VVR, two additional SRL volumes are necessary to act as buffers for the replication (one for Prime Network data volume, and one for the set of Oracle data volumes).

For more information on Oracle disk recommendations, see the Cisco Prime Network 3.9 Installation Guide.

IP Addresses

In addition to a physical IP address, there are two logical addresses: one for the ANA (Prime Network) service group and one for the Oracle service group. All applications connecting to Prime Network and Oracle use the logical addresses. In this way, the specific servers on which Prime Network and Oracle are running remains transparent. The hardware configuration is illustrated in Figure 17-5.
Veritas Local Redundancy

Chapter 17  Using Veritas Gateway Server High Availability

Veritas Local Redundancy

Figure 17-5  Logical Addressing for a Veritas Dual-Node Cluster (Example)

![Logical Addressing for a Veritas Dual-Node Cluster (Example)](image)

The examples in these topics use the following hostname aliases to represent the logical IP addresses:

- **ana-cluster-ana** for the ANA service group logical IP
- **ana-cluster-oracle** for the Oracle service group logical IP

Service Groups

For Prime Network, the single-node is configured using two service groups: an ANA (Prime Network) service group and an Oracle service group.

An individual service group contains, in a virtual manner, the software and hardware resources that are required by a specific application. Thus the ANA service group contains all of the hardware and software resources needed by the Prime Network application, and the Oracle service group contains all of the hardware and software resources needed by the Oracle application. Both the ANA and Oracle service groups contain, at the lowest level, the hardware resources: the NIC resource and the disk group. The IP resource depends on the NIC resource, and the mount resource depends on the disk group. These dependencies are illustrated in Figure 17-6. All of these groups and resources are monitored by standard Veritas agents.

Both the ANA and Oracle service groups contain components arranged in a hierarchical manner, as illustrated in Figure 17-6.

- ANA service group—Contains a custom ANA Gateway resource that starts, stops, and monitors the Prime Network gateway. The ANA Gateway resource depends on its IP and mount resources (which depend on the low-level NIC resource and disk group).
- Oracle service group—Contains the Oracle listener resource, which depends on the Oracle database resource. Finally, the database resource depends on the IP and mount resources (which depend on the low-level NIC resource and disk group). These are monitored by the Veritas Oracle agents.
This hierarchy also determines the startup and shutdown order of the components within the resource group. Each group is brought online from bottom to top of the tree. For example, the components within the Oracle service group come online in the following order:

1. NIC resource and disk group
2. IP and mount resources
3. Oracle database application
4. Oracle listener

Likewise the ANA service groups components come online in this order:

1. NIC resource and disk group
2. IP and mount resources
3. ANA Gateway resource

When taken offline, the components shut down in the reverse of the above.

**Note**

Note that once the Oracle and Prime Network gateway applications are being monitored by VCS, they should only be started and stopped using the Veritas Cluster Manager application or CLI commands. Stopping the applications using the regular application commands without the awareness of the cluster software can cause the service group to failover.

**Prime Network Gateway Processes**

If you are using gateway server high availability, note that there is no overlapping between the processes that Veritas Cluster Manager monitors (the ANA Gateway Veritas agent in Figure 17-7), and the processes that AVM 99 monitors. For an illustration of the unit server high availability processes, see Figure 16-2 on page 16-7.
A custom ANA Gateway agent is available as part of the gateway server high availability installation. The ANA Gateway agent provides an interface to stop, start, and monitor Prime Network (or more specifically, AVM 99, which is the Prime Network bootstrap process). The ANA Gateway agent runs as the operating system root user. Before running the stop and start commands, the agent actually switches to network user. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; an example of network user is network39.)

The processes begin as follows:

1. The anactl_ha.csh wrapper script starts the ANA Gateway resource. anactl_ha.csh is installed with gateway server high availability and is stored in NETWORKHOME/Main/ha.

2. In a local redundancy setup, anactl_ha.csh starts Prime Network by calling the mvmcheck.sh script which is stored in NETWORKHOME/Main/scripts. (It does not call mvm.sh, which is usually called to start Prime Network.)

3. The mvmcheck.sh script verifies whether only AVM 99 is down, or all AVMs are down:
   - If only AVM 99 is down, mvmcheck.sh runs mvm.csh with the -nokill option. This causes mvm.csh to start only AVM 99.
   - If all AVMs are down, mvmcheck.sh runs mvm.csh without any command line options, which stops any running AVM processes using the system kill command.

**Application Dependency**

During gateway startup, the ANA Gateway agent’s primary role is to make the Prime Network gateway process (AVM 11) start up with the Oracle listener in a synchronized manner, without creating a dependency between the ANA and Oracle service groups. When the agent comes online, it employs the logic shown in Figure 17-9:
If the Oracle application fails, the two Prime Network processes that connect to the database—the gateway process (AVM 11) and AVM 25—reconnect to the new instance on their own. This happens on both gateways and units.

**How Automatic Failover is Triggered (Veritas Local Redundancy)**

If one of the critical resources fails, the dual-node cluster is configured for automatic failover. The following topics describe what happens when these components failover:

- Heartbeat Failure, page 17-12
- Hardware Failure, page 17-12
- Oracle Listener/Database Failure, page 17-12
- Prime Network Application Failure, page 17-12

Each node provides redundancy for the other node. Because the Prime Network application directly depends on all resources in its service group, all of its resources—IP, mount, NIC, disks—are designated as critical, along with the Prime Network process (ANA Gateway). While allowances are made for restarts, if any of the resources fail, the ANA (Prime Network) service group will failover. The same is true for the Oracle service group: Any resource failure, apart from allowances for restarts, causes the Oracle service group to failover.
When a failover occurs, all of the resources on the current gateway are shut down (from the top of the tree down). This means that the ANA service group shuts down first because it depends on the Oracle service group. After the shutdown, the resources on the new active gateway are started from the bottom up, with the startup of Oracle service group followed by the startup of ANA service group.

By default, all resources are polled every 60 seconds, which means fault detection can take up to 60 seconds. Once a fault is detected:

- If Prime Network has a failover, it may take 2-3 minutes until the Prime Network application begins the startup process on the redundant server. At that point, Prime Network gateway startup time will vary, depending on the configuration. During this time, no alarms will be recorded by the gateway.

- Likewise, if Oracle has a failover, it may take 2-3 minutes until the Oracle database application begins the startup process on the redundant server. This process may take up to 20 minutes, depending on the number of transactions.

Default polling times can be changed or overridden using the Veritas Cluster Manager.

The dual-node cluster is designed to operate with one service group running on each server. If a failover occurs, both service groups will be running on the same server. A hardware failure on the redundant server could cause a situation where the Veritas application requires a relatively long time (approximately 10-15 minutes) to register the faults to both service groups and have both service groups failover to the other server. The problem should be corrected and cleared, and the service group switched back to its original server, as soon as possible.

**Heartbeat Failure**

The two gateways constantly exchange LLT heartbeats between them. In case of loss of heartbeat, the VCS will automatically failover to the redundant gateway. This underscores the importance each external volume having redundant connections to both servers. This redundant heartbeat path prevents the dangerous situation where the heartbeat is interrupted, and VCS starts one of applications on the other server. You can configure VCS to send an SMTP message and/or a SNMP trap to report the heartbeat failure.

**Hardware Failure**

In the event of a network or disk failure, the service group running on the faulty server will failover to the redundant server. The application in the affected service group is shutdown, the service group’s external shared disk is unmounted and then remounted on the other server, and the application is brought online on the redundant server. You can configure FCS to send an e-mail and/or SNMP trap to report the server hardware failure.

**Oracle Listener/Database Failure**

If the Oracle database application fails, the Oracle service group will failover to the redundant server as described in How Automatic Failover is Triggered (Veritas Local Redundancy), page 17-11. The two Prime Network processes that connect to the database—the gateway process (AVM 11) and AVM 25 (whether on the gateway or the units)—will reconnect to the new instance on their own.

If the listener fails, the Veritas agent will attempt one restart before failing over to the redundant server.

**Prime Network Application Failure**

In the event of a Prime Network process (AVM 99) failure, the ANA Gateway agent attempts one restart. If Prime Network cannot be restarted, the ANA service group will failover to the redundant server as described previously.
Veritas Geographical Redundancy

The following topics provide additional information on how to manage a geographical redundancy configuration:

- **Configuration Details for Veritas Geographical Redundancy (Global Cluster), page 17-13**, describes how the different components of a geographically redundant network work together, including disks, partitions, IP addresses, and service groups.

- **Understanding Manual Failover (Veritas Geographical Redundancy), page 17-17**, describes when to perform a manual failover and why automatic failover is not recommended.

- **Veritas Geographical Redundancy Failure and Failback Scenarios, page 17-19**, provides information about what happens during a gateway and/or unit failover and failback.

Configuration Details for Veritas Geographical Redundancy (Global Cluster)

A geographical redundancy configuration—the global cluster—includes a dual-node cluster at the primary site, and an additional redundant single-node cluster at a geographically remote site for a full DR solution. The server in the redundant single-node cluster is normally running, but with no active applications. If there is a failure at the local dual-node cluster site, an operator can manually switch to the remote redundant server. The single-node cluster at the remote site is connected to storage containing two additional data volumes that are replicas of the two data volumes (Prime Network and Oracle data) at the primary dual-node site. The hardware configuration is illustrated in Figure 17-10. (For a high-level illustration of geographical redundancy, see Figure 17-2 on page 17-4.)
Disks, Partitions, and Replication

The two external data volumes at the remote single-node site are replicas of the two data volumes (Prime Network and Oracle data) at the primary dual-node site. If the applications from the primary dual-node site fails over, these additional data volumes become the principal copy of the system data.

For the global cluster, the Prime Network and Oracle data partitions at the local and remote sites must be kept in sync. The initial synchronization between the local and remote data may require a considerable amount of time. To save time, the primary and secondary servers should be located near each other for the initial synchronization. Afterwards, the redundant server can be moved to the remote location. Data replication should be done asynchronously.

The disks in the remote (redundant) single-node cluster can be mirrored based on the level of redundancy desired. Data replication between the local dual-node cluster and the remote single-node cluster can be implemented in either of the following ways:

- Storage-based replication (NAS or SAN), using any required additional hardware.

Redundancy is not required at the remote single-node cluster site because the local dual-node cluster should have the ability to be restored in a short period of time. If you foresee a need for the remote site to operate for a long period of time, you can augment the single-node cluster as follows:

- Add another disk, mirroring the internal disk
- Add a second connector to each external disk unit (to protect against connection failure).
IP Address

Two additional IP addresses are required by the WAC (Wide Area Connection) resources that are used to implement the VCS global cluster. One address is for the local cluster and one address is for the remote cluster.

In addition, the remote single-node cluster is assigned a single logical address. All Prime Network-related applications, including Oracle and northbound applications, use the logical addresses. In the event of a failover to the gateway at the secondary site, all northbound applications will have to reconnect using the new logical IP address at the remote cluster. The units servers will automatically be reconfigured to use the new IP address of the gateway.

Service Groups

For geographical redundancy, the baseline ANA and Oracle service groups require additional resources/service groups in order to integrate with the data replication process. The following example discusses the resource changes for replication using VVR. For storage-based replication, each replication solution supported by Veritas will have its own agent and, and the setup will vary. See the Veritas product documentation for the latest list of supported replication solutions and existing agents.

Replication with VVR

For VVR, dedicated VVR service groups are added to both the local and remote clusters.

For the local (dual-node) cluster, each application service group (ANA and Oracle) has a corresponding VVR service group. The NIC and IP resources, as well as the disk group resource from each application service group, are moved to the VVR service groups. The VVR service groups add an RVG resource, which is dependent on the IP and Disk Group. The application service groups add RVGPrimary resources, on which the applications become dependent. See Figure 17-11 for an illustration.
Veritas Geographical Redundancy

Figure 17-11 Local Dual-Node Cluster Resources Using VVR (Geographical Redundancy)

In the remote single-node cluster, the setup is similar, except that there is a single VVR service group that serves both application groups. The single NIC and IP resources, as well as the two disk group resources, reside in the VVR service group. Dependent on them are the RVG resources for both Prime Network and Oracle. This hierarchy is illustrated in Figure 17-12.
Understanding Manual Failover (Veritas Geographical Redundancy)

In the global cluster scenario, a failure in the local dual-node cluster means that a critical resource has failed on both servers in the cluster. If this happens, a user can manually failover to the server in the remote single-node site.

If one of the critical resources fails, the dual-node cluster is configured for manual failover. These topics describe what happens when these components failover:

- Heartbeat Failure, page 17-18
- Local Dual-Node Cluster Failure, page 17-19
- Local -> Remote Cluster Failover, page 17-19
- Local -> Remote Unit Failover, page 17-21
- Remote -> Local Cluster Failback, page 17-21
- Remote -> Local Unit Return, page 17-22
Automatic failover is not recommended for the following reasons.

- Possibility of a *split-brain* scenario. A split-brain scenario is when both the local dual-node site and the remote single-node site assume they should be running. Because the heartbeat between the two sites is sent over the network, the heartbeat could be interrupted due to a loss of connectivity between the two sites—which the remote site could interpret as a failure at the local site. If failover was automatic, the remote cluster would automatically start up and begin running in parallel with the local cluster. There, failover between sites should be performed manually.

- Human intervention is warranted. In the event of a failure at the local dual-node site, an operator should verify the failure. A site failure (as opposed to a localized hardware failure) is a major event that requires human intervention to assess the situation. For example, even if the two servers at the local site fail, units at the primary site might still be functioning. If the remote (redundant) single-node site also included a set of redundant units, an operator would need to determine whether only the gateway should failover, or if the units should also failover.

The manual site-to-site failover process includes the shutdown of both application service groups in the local dual-node cluster, and the startup of the corresponding service groups in the remote single-node cluster. After a failure at the local dual-node site, if the local VVR service groups are still online, VVR will try to replicate any unsynchronized data in the SRLs as part of switching the server at the remote site from secondary to primary. (The unsynched data is what was queued up in the buffer, but was not yet replicated.)

**Basic Steps in Manual Failover and Failback**

The following are the basic manual steps for a failover in a geographical redundancy configuration:

1. When a heartbeat loss occurs, verify the cause (it could be a simple loss of connectivity).
2. Verify that the applications are down and the disks are unmounted at the local dual-node site.
3. Start the failover.
4. Configure northbound applications to re-login to the remote single-node gateway using the new IP address.
5. When the original gateway and database servers are up at dual-node site, bring VVR resources online. Because the remote site now contains the master copy of the data, this ensures that data written to the Prime Network and Oracle volumes at the remote site can be replicated back to the local site.
6. When appropriate, failback to the local site.

**Heartbeat Failure**

The primary (local) and secondary (remote) clusters constantly exchange LLT heartbeats over the shared IP network. If there is a heartbeat loss, VCS registers the fault and awaits manual intervention for failover. The operator must determine whether the problem is due to a failure in the local dual-node cluster, or a loss of network connectivity between the two sites. If it is a network connectivity issue, no action is required. But if it is due to a critical resource failure on both servers in the dual-node cluster, the operator should perform the manual failover of the remote gateway (and the unit servers, if they also fail). You can configure VCS to send an SMTP message and/or a SNMP trap to report the heartbeat failure.
Veritas Geographical Redundancy Failure and Failback Scenarios

The basic steps for manual failover (and failback) are described in Understanding Manual Failover (Veritas Geographical Redundancy), page 17-17. That section also describes what happens when there is a heartbeat failure. These topics describe other failover and failback scenarios:

- Local Dual-Node Cluster Failure, page 17-19
- Local -> Remote Cluster Failover, page 17-19
- Local -> Remote Unit Failover, page 17-21
- Remote -> Local Cluster Failback, page 17-21
- Remote -> Local Unit Return, page 17-22

Local Dual-Node Cluster Failure

A local cluster failure occurs when either Prime Network or Oracle registers a fault on both servers in the dual-node cluster. If this occurs, both service groups are shutdown, and the failover awaits manual intervention. VCS can be configured to send an SMTP message and/or a SNMP trap to report the failure.

Local -> Remote Cluster Failover

When the local dual-node cluster fails over to the remote single-node cluster, all resources on the local cluster are shut down (if possible) and then started up on the remote cluster.

Data replication requires that the volumes being replicated be mounted at only one site at a time. In other words, when the local dual-node cluster is up, the disk resources at the remote single-node cluster should be offline. If the local dual-node cluster fails,

- If the remote cluster can verify the state of the disk resources in the local cluster, and the local resources are offline, the operator can initiate the failover process.
- If the remote cluster cannot verify the state of the disk resources in the local cluster (because communications are interrupted or hardware has failed), the operator must do the following:
  - Manually confirm that the disks at the local site are unmounted.
  - Start the failover process.

As mentioned in IP Address, page 17-15, switching to the remote (redundant) single-node gateway involves using a different gateway IP address. The anaclt_ha.csh script will automatically reconfigure the Prime Network/Oracle addresses and LDAP settings on both the gateway and units (which enables unit communication with the new Prime Network/Oracle instance). Any northbound applications that use an IP address to connect to the gateway will have to log in again using the new address of the gateway. If applications use a hostname to connect to the gateway, and a DNS resource is configured for the remote single-node cluster, a reconnect should not be required.

The Oracle listener will automatically start with the correct address for the remote single-node site, and the Prime Network startup process will automatically reconfigure the gateway to use the new listener address. This is because the locally-configured hostname alias (in /etc/hosts on each server) is configured with a different address for the local and remote clusters.

Figure 17-13 illustrates the steps that are invoked by the ANA Gateway resource when it fails over to the remote single-node cluster.
**Veritas Geographical Redundancy**

**Chapter 17  Using Veritas Gateway Server High Availability**

**Figure 17-13  ANA Application Process Flow at Failover (Local to Remote Cluster)**

**ANAGateway Agent (user=root)**
- get ANA IP and Oracle IP for dual-node cluster or single IP for single-node cluster

- run background script to reset GW address on running AVMs
- change GW IP address in uplinks in 127.0.0.1/avm0.xml
- change GW IP address in uplinks in unit_ip/avm0.xml
- change GW IP address in gs and haservice in unit_ip/avm99.xml
- run script via ssh on each unit to switch ANA IP address in registry
- change GW IP address in localhost in 127.0.0.1/avm99.xml
- change DB Server IP in workflow in 127.0.0.1/avm66.xml
- change DB Server IP in ep and main in 127.0.0.1/persistency.xml
- change DB Server IP in gs and haservice in unit_ip/persistency.xml
- change DB Server IP in ep and main in 0.0.0.0/persistency.xml
- change any LDAP parameters in 127.0.0.1/authentication.xml

- run script via ssh on each unit to switch ANA IP address in registry
- change GW IP address in localhost in 127.0.0.1/avm99.xml
- change DB Server IP in workflow in 127.0.0.1/avm66.xml
- change DB Server IP in ep and main in 127.0.0.1/persistency.xml
- change DB Server IP in gs and haservice in unit_ip/persistency.xml
- change DB Server IP in ep and main in 0.0.0.0/persistency.xml
- change any LDAP parameters in 127.0.0.1/authentication.xml

- management.attachToMvm command for each AVM on each Unit

- stop AVMs 99, 25, 0
- change GW IP address in gs and haservice in avm99.xml
- change DB server IP address in ep and main in persistency.xml
- change GW IP address in uplinks avm0.xml
Chapter 17  Using Veritas Gateway Server High Availability

Veritas Geographical Redundancy

Local -> Remote Unit Failover

Note

Do not manage local and remote site unit redundancy using unit server high availability. In other words, do not create a protection group that contains units from the local and remote site.

If redundant units are provided at the remote single-node site, the units are normally up but no AVMs are running. (This is different from a standby unit in a unit server high availability scenario, where the standby units are down.) If the local dual-node site has a failure that affects both the gateway and units, the operator will first failover the gateway, and then some manual steps must be performed.

When the gateway is up and running at the remote single-node site, do the following:

1. Move AVMs from the local units to the remote units. How many AVMs can be moved depends on how many unit servers are at the remote site. See Moving and Deleting AVMs, page 4-13.

2. If the failover occurred on the gateway or unit that had a running AVM 100 (AVM 100 contains the Event Collector):
   a. If AVM 100 was running on a unit that failed, start AVM 100 on the redundant unit. (If AVM 100 was running on a gateway that failed, it will be automatically restarted.) See Enabling a New Event Collector on a Unit, page 14-12.
   b. Reconfigure devices to forward events to the new unit or gateway that is running the Event Collector (if this was not already done). This is required because the IP address of AVM 100 will be different. (A port watchdog script, that runs on all units and gateways, will receive the incoming traps and syslogs on the failed gateway or unit. This ensures that the device sending the traps and syslogs does not receive error messages.)

Depending on the location of devices, the connection between devices and a remote unit may be across the WAN. Assuming that the relevant ports have been opened in the firewall, this configuration is supported for the geographical redundancy gateway server high availability solution.

Remote -> Local Cluster Failback

Once the primary site is online, you should switch the gateway back to the local cluster as soon as possible. As described in Disks, Partitions, and Replication, page 17-14, if the local dual-node site fails over, the two additional data volumes at the remote site become the principal copy of the system data. Before a switchover back to the local dual-node cluster, this data will have be replicated back to the disks in the local cluster.

To minimize downtime, bring the two VVR service groups online as soon as possible so that replication from the remote site to the local site can begin. Depending on how long the primary site was down, there may be a large amount of data to replicate. Prime Network can continue to run on the remote single-node cluster while the data is replicated to the local site. When the data at the two sites is synchronized, you can initiate the manual failback procedure.

Note

If you initiate failback before the data has been fully synchronized, the data synchronization will become part of the failback process. Depending on how much data needs to be synchronized, this may require a considerable amount of time.

Failing back to the local dual-node cluster involves the same steps as the failover, but in reverse order. When the remote single-node cluster fails back to the local dual-node cluster, all resources on the remote cluster are shut down and then started up on the local cluster.
The gateway IP address will switch back. As described in Local Dual-Node Cluster Failure, page 17-19, the `anaclt_ha.csh` script will automatically reconfigure the Prime Network/Oracle addresses and LDAP settings on both the gateway and units. Northbound applications will have to log in again using the new address of the gateway. If applications use a hostname to connect to the gateway, and a DNS resource is configured for the remote single-node cluster, a reconnect should not be required.

The Oracle listener will automatically start with the correct address for the remote single-node site, and the Prime Network startup process will automatically reconfigure the gateway to use the new listener address. This is because the locally-configured hostname alias (in `/etc/hosts` on each server) is configured with a different address for the local and remote clusters.

**Remote -> Local Unit Return**

Once the primary site is online and the gateway in the local dual-node cluster is operational, you should do the following:

- Move all AVMs back to their original units in the primary site.
- Stop the running AVM 100 on the remote unit, and restart it on the original unit at the primary site.

### Mean Time to Repair Veritas Gateway Server High Availability Failures

Table 17-2 provides some information about the average time required to recover from a component failure in a Veritas gateway server high availability configuration.

<table>
<thead>
<tr>
<th>Component</th>
<th>Results of Failure</th>
<th>Average Time To Repair Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of any resource in ANA service group</td>
<td>Gateway will not be available until failover to redundant gateway is complete.</td>
<td>2-3 minutes plus gateway startup time (system dependent).</td>
</tr>
<tr>
<td>Failure of any resource in Oracle service group</td>
<td>Database will not be available until failover to redundant database is complete.</td>
<td>2-3 minutes plus database startup time. Can be up to 20 minutes, depending on the transaction rate prior to failure.</td>
</tr>
<tr>
<td>Local site failure</td>
<td>Gateway and database will not be available until manual failover to remote server and database is complete.</td>
<td>Once initiated, 5 minutes plus time required to copy any unreplicated data in replication buffer plus gateway and database startup time (in parallel).</td>
</tr>
<tr>
<td>Local site failure including units</td>
<td>Gateway, database, and units will not be available until manual failover to remote site is complete.</td>
<td>Once initiated, 5 minutes plus time required to copy any unreplicated data in replication buffer plus gateway and database startup time (in parallel) plus unit start up time (system dependent).</td>
</tr>
</tbody>
</table>

**Note**

If the Event Collector (AVM 100) was running on a component that failed, the system will lose traps and syslogs sent from devices, and raw events will not be persisted. For more information on AVM failure and their impact, see Estimating the Impact of Unit or AVM Failures, page 16-4.
Using RHCS/ADG Gateway Server High Availability

These topics describe the gateway server high availability solutions that use Red Hat Cluster Suite (RHCS) and Oracle Active Data Guard (ADG). These solutions leverage the Prime Network embedded database and existing licensing terms. Use the architecture described in these topics as a reference point and adjust them to meet the needs of specific deployments. Both the local redundancy and geographic redundancy configurations are independent of and compatible with the unit server high availability mechanism (described in Unit Server High Availability and AVM Protection, page 16-1).

- Red Hat Cluster Suite (RHCS) Local Redundancy, page 18-1
- Oracle Active Data Guard (ADG) Geographical Redundancy, page 18-8

Note
This solution does not support IPv6 on the gateway or database. This solution also does not support a remote database. (In other words, for local redundancy, the database must be installed on the same server as the gateway. For geographical redundancy, the database must be installed on the standby server (with the gateway)).

For information on the gateway server high availability solution that uses Veritas software, see Using Veritas Gateway Server High Availability, page 17-1.

Red Hat Cluster Suite (RHCS) Local Redundancy

The RHCS local redundancy solution contains a dual-node cluster that provides an automatic failover solution for local hardware faults. Because the gateway and database use logical IP addresses (which they retain regardless of the node they are running on), if a failover occurs, there is no need to reconfigure IP addresses.

When this solution is initially installed, the gateway and database services are installed on and managed by one node in the cluster. The nodes are monitored by RHCS and if the node managing the services fails, the services are seamlessly moved to the other node.

If desired, one of the services can be moved to the other node using the RHCS web GUI or CLI (clusvcadm utility). This type of configuration is shown in Figure 18-1, where the Prime Network gateway service is on Server P1, the Oracle database service is on Server P2, and both servers are connected to an embedded database that is installed on an external device.
You cannot use the local redundancy configuration that is illustrated in Figure 18-1 for geographical redundancy because geographical redundancy requires a WAN and a dedicated connection from the gateway to the database.

Figure 18-1 Architecture for Gateway with RHCS Local Redundancy

The RHCS local redundancy solution also requires a fencing device, which is a hardware unit that disconnects a node from shared storage to ensure data integrity. For information on the supported fencing options, see the Cisco Prime Network 3.9 Installation Guide.

To troubleshoot problems with hardware and service failures, see the Cisco Prime Network 3.9 Installation Guide.

Configuration Details for RHCS Local Redundancy

Local redundancy requires that Red Hat Cluster Suite (RHCS) be installed on both nodes. Out of the box, both services run on the node from which the installation script is run. This configuration can be changed, if desired, using RHCS web GUI or CLI (clusvcadm utility).

The local redundancy solution also requires a fencing hardware unit for cutting a node off from the shared storage. This ensures data integrity and prevents a split brain scenario, where the node are disconnected from each other and each presumes the other has failed. If a failure occurs, the cut off can be accomplished by powering off the node with a remote power switch, disabling a switch channel, or revoking a host’s SCSI 3 reservations.

For complete redundancy, a configuration with no single point of failure is recommended.

In cases where your configuration has more than one port connection, you should consider adding a redundant fencing device. To troubleshoot problems with hardware failures, see the Cisco Prime Network 3.9 Installation Guide.
Fencing Devices

Each node in the cluster must use a fencing method. The fencing method is engaged when one of the nodes has a problem, and prevents the problematic node from writing to the shared storage. A complete list of supported fencing devices is provided in the Cisco Prime Network 3.9 Installation Guide. Manual fencing is also supported but is recommended as a temporary solution; for more information, see Fencing and Manual Fencing, page 18-7.

RHCS Services and Resources

Services are a set of resources that are grouped together. RHCS monitors two cluster configured services: `ana` and `oracle_db`.

The Oracle listener should be running before Prime Network, which allows the Prime Network gateway process (AVM 11) to connect to the database. If the listener is not running, the Prime Network agent contains logic to enable it to delay startup of the Prime Network processes while it waits for the listener to start. If the listener does not start up on time, the Prime Network gateway agent will abort the startup, resulting in a Prime Network resource failure.

Alternatively, you can also bring the service groups online in serial sequence, starting with the Oracle service group, then the Prime Network service group. (RHCS does not enforce this behavior.)

Table 18-1 lists the services that are monitored by RHCS.

<table>
<thead>
<tr>
<th>RHCS Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ana</code></td>
<td>Monitors AVM 99 (Prime Network) and consists of the following resources.</td>
</tr>
<tr>
<td></td>
<td>IP address: <code>ana_service_floating_IP</code></td>
</tr>
<tr>
<td></td>
<td>Scripts: <code>ana.sh</code></td>
</tr>
<tr>
<td><code>oracle_db</code></td>
<td>Monitors Oracle processes and listener and consists of the following resources.</td>
</tr>
<tr>
<td></td>
<td>IP address: <code>oracle_db_floating_IP</code></td>
</tr>
<tr>
<td></td>
<td>Scripts: <code>oracles.sh</code>, <code>lsnr.sh</code></td>
</tr>
</tbody>
</table>

Both nodes in the cluster must have identical RHCS versions and packages.

For information on the RHCS version that is supported and to troubleshoot service failures, see the Cisco Prime Network 3.9 Installation Guide.

IP Addresses

Both the Prime Network gateway process and the Oracle database services have their own virtual IP address (floating IPs). Because they retain their IP addresses when there is a failover or switchover, Prime Network clients interprets failovers or switchover as local service restarts. Virtual IP addresses must be in the same subnet. Use the gateway floating IP address when installing a new unit, using LDAP, etc.

Note

If you are using the `network-conf` script, when you are prompted for the IP address of units, use the floating IP address of the gateway.
Chapter 18      Using RHCS/ADG Gateway Server High Availability

Multicast Addresses

Each network switch and associated networking equipment in a Red Hat cluster must support and enable multicast addresses and IGMP. Because configuration procedures vary, refer to the appropriate vendor documentation or other information about configuring network switches, and associated networking equipment, to enable multicast addresses and IGMP.

Because the Prime Network installer does not validate the multicast address, you must manually verify that the multicast address meets RHCS requirements and is not blocked by a firewall.

File System Type

The RHCS local redundancy solution requires the ext3 file system.

Shared Storage and Disk Partitioning

Each cluster service should use one partition. If the partitions are on the same disk, use a single partition for each service.

If partitions are spread across disks, use a single disk for each service. Each disk must be labeled.

The storage related to the services managed by the cluster should not be automatically mounted (automounted) by the operating system upon reboot. RHCS will perform the mounting.

Security

When the RHCS local redundancy solution is installed, SSL keys are generated and copied to the other node in the cluster.

Licenses

The license directory NETWORKHOME/Main/ha/licenses on the active gateway should contain a copy of all license files for both nodes. This directory will be available to both nodes because it is part of the partition that is shared. If you add new licenses, you must copy them to this directory and run the resetLicenses.pl command to read the licenses. See Licensing and Gateway Server High Availability, page 5-2.

Failover and Switchover (RHCS Local Redundancy)

After the local redundancy cluster is deployed, failovers are automatic. In case of a single service failure, the cluster will attempt to restart the service. If the retries fail, the service will be relocated to the second node and started on that node. This does not impact the other service in the cluster.

Human intervention is required only in exceptional cases, such as when the database becomes corrupted or a component fails, and the component is not configured for redundancy. Manual switchovers are performed using the RHCS web GUI or the clusvcadm utility. Once a failed node is repaired, you must perform a manual switchover to revert the cluster to its original configuration. See Managing RHCS Local Redundancy, page 18-5

Note

For complete redundancy, a configuration with no single point of failure is recommended. See the RHCS documentation for recommended configurations.
Managing RHCS Local Redundancy

Before stopping the Prime Network or Oracle application processes, place the RHCS services in maintenance mode (also known as freezing the process) using clusvcadm. If you attempt to restart either the Prime Network or Oracle applications without freezing the RHCS process, the cluster may detect that the services are down and attempt to restart them. See Stopping and Restarting RHCS Services Using the RHCS CLI (clustat, clusvcadm), page 18-6.

These topics provide information pertaining to ongoing management of an RHCS local redundancy cluster.

RHCS Log Messages

The RHCS log messages provide information about cluster-related issues, such as service failure. Every 30 seconds, RHCS issues status commands to check the Prime Network, Oracle, and Oracle listener processes. These messages are logged to /var/log/messages and can be viewed by the root user (or from the RHCS web GUI). The following are some example messages.

Mar 23 13:45:47 csi-bvc clurgmgrd: [27961]: <info> Executing /usr/local/bin/ana.sh status
Mar 23 13:46:07 csi-bvc clurgmgrd: [27961]: <info> Executing /usr/local/bin/oracle.sh status
Mar 23 13:46:07 csi-bvc clurgmgrd: [27961]: <info> Executing /usr/local/bin/lsnr.sh status

To troubleshoot problems with service failures, see the Cisco Prime Network 3.9 Installation Guide.

RHCS Web GUI (luci)

The RHCS web client provides information about the status of the cluster (the status of each service, the node the service is running on, and so forth). You can also use the web GUI to:

- Check the cluster status, including the status of each service and the node each service is running on.
- Initiate a switchover of a service to the other node (relocate the service from the Services area of the GUI).

To stop or start the Prime Network and Oracle database services that are managed by the cluster, use clusvcadm, as described in Stopping and Restarting RHCS Services Using the RHCS CLI (clustat, clusvcadm), page 18-6.

The RHCS web interface is automatically configured by the Prime Network installation script. You can connect to the RHCS web interface by entering the following in the address field of your browser.

https://cluster-node-hostname:port/luci

For details on how to use the web GUI, see the appropriate RHCS documentation.
Stopping and Restarting RHCS Services Using the RHCS CLI (clusstat, clusvcadm)

**Note**

Before stopping the Prime Network or Oracle application processes, place the RHCS services in maintenance mode (also known as freezing the process) using `clusvcadm`. If you attempt to restart either the Prime Network or Oracle applications without freezing the RHCS process, the cluster may detect that the services are down and attempt to restart them.

The `clusstat` and `clusvcadm` commands are the basic CLI commands you can use to monitor and manage the local redundancy cluster. This topic describes some common uses for these commands. You must be logged in as root to use these commands.

The `clusstat` command checks a cluster’s members and overall status. In the following example, the cluster name is `ana_cluster` and `csi-bvc.cisco.com` is the node from which the command was run.

```bash
root@csi-bvc.cisco.com]# clusstat
Cluster Status for ana_cluster @ Thu Mar  3 10:24:50 2011
Member Status: Quorate

Member Name                                          ID    Status
------ ----                                          --    ------
csi-bvc.cisco.com                                      1   Online, Local, rgmanager
csi-w47.cisco.com                                      2   Online, rgmanager

Service Name                                  Owner (Last)                  State
------- ----                                  ----- ------                  ----- 
service:ana                                   csi-bvc.cisco.com             started
service:oracle_db                             csi-w47.cisco.com             started
```

If you need to restart Prime Network or the Oracle application processes, first use the `clusvcadm` command to stop the RHCS services using the following procedure.

**Step 1** Place the Prime Network and database RHCS services in maintenance mode (also called freezing) using the following command, where `service` is `ana` or `oracle_db`.

```bash
# clusvcadm -Z service
```

**Step 2** Confirm that the services are in maintenance mode. Run `clusstat` and verify that the output shows the service followed by a `[Z]`, which indicates the service is in maintenance mode (frozen). When the services are frozen, the cluster does not monitor them.

```bash
root@csi-bvc.cisco.com]# clusstat
Cluster Status for ana_cluster @ Thu Mar  3 12:31:55 2011
Member Status: Quorate

Member Name                                          ID    Status
------ ----                                          --    ------
csi-w47.cisco.com                                      1   Online, Local, rgmanager
csi-w47.cisco.com                                      2   Online, Local, rgmanager

Service Name                                  Owner (Last)                  State
------- ----                                  ----- ------                  ----- 
service:ana                                   csi-w47.cisco.com             started [Z]
service:oracle_db                             csi-w47.cisco.com             started [Z]
```
Step 3 After confirming that the **ana** and **oracle_db** cluster configured services are frozen, use the normal application commands to stop Prime Network and Oracle.

Step 4 After restarting the Prime Network and Oracle applications, move the RHCS services out of freeze mode and reinitiate the cluster’s monitoring of the ana and oracle services:

```
# clusvcadm -U service
```

### Fencing and Manual Fencing

A fencing device is a hardware unit that disconnects a node from the shared storage. This happens when a node needs to assume control of a service but cannot connect to the other node. Disconnecting the problematic node from the database ensures data integrity and prevents split-brain scenarios. You can reconfigure the fencing choice at any time using the RHCS web interface or other RHCS tools.

During the installation of the RHCS solution, you are prompted to select one of four fencing options. The first three are for specific fencing devices supported by the solution. If you choose one of these devices (or more specifically, one of these fencing agents), if an error occurs, the fencing agent will automatically disconnect the cluster node from the storage.

The fourth option is **manual fencing**. If you choose manual fencing, this means you are responsible for making sure that, when a problem occurs, the node and storage are disconnected (either by disconnecting the node and storage by hand or by using another fencing agent).

**Note**

We recommend that manual fencing only be used on a temporary basis. If you use manual fencing, it is your responsibility to make sure that when an error occurs, the node and the storage are disconnected during the cluster workflow. We recommend that you use manual fencing as a backup for your chosen fencing agent.

If you are using manual fencing and an error occurs that requires fencing intervention, a message is printed to `/var/log/messages` advising you to run the **fence_ack_manual** command on the gateway server. When you run it, this command asks for confirmation that you have disconnected the faulty node from the storage. Only then will the cluster workflow continue.

**Warning:** If the node “csi-bvc.cisco.com” has not been manually fenced (i.e. power cycled or disconnected from shared storage devices) the GFS file system may become corrupted and all its data unrecoverable! Please verify that the node shown above has been reset or disconnected from storage.

Are you certain you want to continue? [Y/N] **y**

To use the **fence_ack_manual** command, log into the gateway server as root and enter the command using the following syntax. The node that has been disconnected from storage is specified using the `-n nodename` option.

```
fence_ack_manual -n nodename
```

To troubleshoot hardware failures, see the *Cisco Prime Network 3.9 Installation Guide*. 
Oracle Active Data Guard (ADG) Geographical Redundancy

The ADG geographical redundancy solution uses a secondary site containing a single server that provides failover in case of a failure at the primary site. The remote secondary server, which is running but has no active applications, provides redundancy for the server (or servers) at the primary site, which contain the gateway and the database services.

The data stored in the server and database is continuously replicated between the two sites. The primary and standby database are monitored and synchronized using Oracle Active Data Guard; the Prime Network server files (registry and system files) are synchronized using the GWSync utility, which is based on Red Hat Enterprise Linux rsync. Prime Network periodically monitors and validates the replication process and issues a System event in case of a problem.

For disaster recovery (if the primary site becomes unavailable), a manual failover can be triggered from the standby site.

The gateway and database use logical IP addresses which are different between the two sites (the sites are most likely on different subnets). The utilities for managing the manual failover are described in Managing ADG Geographical Redundancy, page 18-14.

Figure 18-2 illustrates a geographical redundancy with the following members:

- A primary site, with Server P1 containing the Prime Network gateway service, and Server P2 containing the Oracle database service. Both servers are connected to an embedded database that is installed on an external device.
- A remote site, with Server S1 containing its own server, database, and storage, all located at another geographical location. The secondary site will be the backup to the first site.

Configuration Details for ADG Geographical Redundancy

The ADG geographical redundancy solution requires the following applications:

- Oracle Active Data Guard Option between the primary local and secondary remote machine—Replicates data to a standby database at remote site (the standby database is set up during installation of the ADG solution). See Oracle ADG Replication Process and Configuration Files, page 18-9.
• GWSync—Replicates the server home directory (and any file system data that is required for disaster recovery) to the server at the remote site. See GWSync Replication Process, page 18-11.

In addition, you must enable backups for the embedded database, as described in Enabling Backups (Embedded Database), page 11-11.

You cannot use the local redundancy configuration that is illustrated in Figure 18-1 on page 18-2 for geographical redundancy because geographical redundancy requires a WAN and a dedicated connection from the gateway to the database.

**Figure 18-3  Hardware Configuration for ADG Geographical Redundancy**

---

**Note**

Geographical redundancy does not allow the Prime Network service (ana) to be brought online on the local side while the Oracle service is online on the remote side (or vice versa).

**Oracle ADG Replication Process and Configuration Files**

When the ADG solution is installed, a standby database is created at the remote site. The remote standby database is an active (read-only) Oracle instance. The local active database, which operates in archive log mode, sends copies of the redo logs to the standby database for archiving. Data is synchronized using Redo-apply. When the high availability solution is installed, it sets up the cron jobs that will monitor the synchronization process.

ADG uses port 1521 for communication between the servers. This port must be open.

**Figure 18-4** illustrates how data is replicated between the local active database and the remote standby database.
The databases must have identical disk capacities and mount points.

The following tables provide example parameters for the ADG init.ora and tnsnames.ora configuration files. These files reside on both the local and remote servers. In these examples, the local active database is named anadb and the remote standby database is named anadb_sb.

**Table 18-2  Parameters for Oracle ADG init.ora Configuration Files**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition for init.ora at Local Active Site</th>
<th>Definition for init.ora Remote Standby Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>db_unique_name</td>
<td>anadb</td>
<td>anadb_sb</td>
</tr>
<tr>
<td>log_archive_dest_1</td>
<td>LOCATION=\log-archive-dest1-full-pathname</td>
<td></td>
</tr>
<tr>
<td>log_archive_dest_2</td>
<td>Service=anadb_sbASYNCLGWRVALID_FO R=(ONLINE_LOGFILES,PRIMARY_ROLE</td>
<td>Service=anadb_sbASYNCLGWRVALID_FO R=(ONLINE_LOGFILES,PRIMARY_ROLE</td>
</tr>
<tr>
<td></td>
<td>db_unique_name=anadb_sb</td>
<td>db_unique_name=anadb</td>
</tr>
<tr>
<td>log_archive_dest_state_1</td>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>log_archive_dest_state_2</td>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>standby_file_management</td>
<td>AUTO</td>
<td></td>
</tr>
</tbody>
</table>

Table 18-3 shows example configuration parameters for the tnsnames.ora file at the local and remote sites. These files must be identical at both sites.

**Table 18-3  Parameters for Oracle ADG tnsnames.ora Configuration Files**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANADB=</td>
<td>(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = ip-address)(PORT = 1521))</td>
</tr>
<tr>
<td></td>
<td>(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = anadb) ) )</td>
</tr>
<tr>
<td>ANADB_SB=</td>
<td>(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = ip-address(PORT = 1521))</td>
</tr>
<tr>
<td></td>
<td>(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = anadb) ) )</td>
</tr>
</tbody>
</table>
To troubleshoot problems with the replication process, see the *Cisco Prime Network 3.9 Installation Guide*.

**GWSync Replication Process**

The GWSync utility is based on RHEL rsync. GWSync replicates the local primary server home directory (and any file system data that is required for disaster recovery) on the remote secondary server. Cron jobs trigger synchronization at both the primary and secondary sites. Data is exchanged using SSH across secure channels.

Data is sent on an incremental basis. In other words, GWSync only sends data that has changed.

The initial GWSync is triggered when the geographical redundancy solution is installed; after that, the data is synchronized every 60 seconds. The installation process also sets up the cron jobs that trigger the synchronization process.

![Figure 18-5 How GWSync Replication Process is Monitored (ADG Geographical Redundancy)](image)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Local primary site generates local_timestamp file.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Remote secondary site pulls NETWORKHOME directory from local primary site (including remote site’s local_timestamp file).</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Primary site pulls remote site’s timestamp file as remote_timestamp.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Primary site compares local_timestamp and remote_timestamp files and, if too much time has passed, issues a System event.</td>
</tr>
</tbody>
</table>

To troubleshoot problems with the replication process, see the *Cisco Prime Network 3.9 Installation Guide*.

**Embedded Database**

Backups must be enabled for the embedded database, as described in *Enabling Backups (Embedded Database)*, page 11-11.

**IP Addresses and the network-conf Script**

If you are using the `network-conf` script, when you are prompted for the IP address of units, use the floating IP address of the gateway.

**File System Type**

The ADG geographical redundancy solution requires the ext3 file system.
Security

To secure the channel used for data replication, an SSH key exchange is performed during the Prime Network installation.

LDAP External Authentication

If you use LDAP authentication in a geographical redundancy configuration, the gateway servers must be configured to communicate with two different LDAP servers, one at the local site and one at the remote site. For this reason the switchover and failover utilities will prompt you for the relevant LDAP parameters. The LDAP parameters are set once using Prime Network Administration.

If for some reason the necessary IP addresses are not updated after a switchover or failover, you can set them manually (which includes setting the necessary LDAP parameters). See Changing the Gateway IP Address on a Gateway and All Units (changeSite.pl), page 18-22.

For more information on using LDAP for user authentication, see Using an External LDAP Server for Password Authentication, page 7-7.

Licenses

The license directory NETWORKHOME/Main/ha/licenses on the active gateway should contain a copy of all license files for all servers. This directory will be available to all servers because it is part of the Prime Network partition that is replicated among servers. If you add new licenses, you must copy them to this directory and run the resetLicenses.pl command to read the licenses. See Licensing and Gateway Server High Availability, page 5-2.

Switchover/Failover Scenarios (ADG Geographical Redundancy)

These topics provide overviews of the switchover, failover, and fallback scenarios for ADG geographical redundancy configurations. The utilities used for these operations are stored in /var/adm/cisco/prime-network/scripts/ha/util.

Switchover and Fallback

A switchover is a planned, scheduled move from the primary active site to the secondary standby site when both sites are up. It is performed from the primary site using the primeha-switch command. (If local redundancy is configured at the primary site, it is performed from the node that contains the primary database.) The switchover reverses the replication direction for ADG and GWSync. If units are configured, the switchover script reconfigures the units to use the new active gateway and database.

A fallback is the process of reverting back to the original configuration. A fallback is also performed using the primeha-switch command, which causes the replication processes to revert back to their original direction.

These operations can only be performed from the primary site. For information on using the primeha-switch command, see Performing a Schedule Site Move (primeha - switch), page 18-15.

Failover and Fallback

A failover is normally the result of a serious failure which renders the primary site unavailable. In the case of such a failure, you must manually trigger a failover using the primeha-fail command, which disconnects the two sites, stops the replication process, and starts the standby server so it becomes a standalone node (that is, without geographical redundancy). These operations are performed from
standby site. (If local redundancy is configured at the standby site, it is performed from the node that contains the standby database.) For information on how to use primeha, see Managing ADG Geographical Redundancy, page 18-14.

Whether any data is lost depends on whether one of the sites is down when the failover occurs, because the failover event interrupts the replication process. If both sites are up, an orderly migration of data can be performed. Because replication channels are severed during the failover, you must reestablish all replication using the setup_Prime_DR.pl script (as described in the Cisco Prime Network 3.9 Installation Guide).

After all failures have been addressed and repaired, and replication is reinitiated, use the primeha -switch command to perform a fallback to the original setup.

These operations are performed from standby site. (If local redundancy is configured at the standby site, it is performed from the node that contains the standby database.) For information on how to use primeha, see Managing ADG Geographical Redundancy, page 18-14.

Note

For complete redundancy, a configuration with no single point of failure is recommended. See the RHCS documentation for recommended configurations.

Recovering from a Disaster

Contact your Cisco account representative.
Managing ADG Geographical Redundancy

These topics provide information pertaining to ongoing management of an ADG geographical redundancy configuration.

Monitoring System Events

Prime Network generates the following System events for geographical redundancy monitoring:

- Informational event to indicate that both ADG and GWSync monitoring is active. This is done on an hourly basis based on cron jobs.
- Critical events when the following occur:
  - A GWSync has not occurred in the last 10 minutes.
  - The standby database is down.
  - The standby database is up but has been out of sync for 30 minutes.

To troubleshoot problems with the replication process, see the Cisco Prime Network 3.9 Installation Guide.

Monitoring Log Messages

The log files for data replication are described in the following table. To troubleshoot problems with the replication process, see the Cisco Prime Network 3.9 Installation Guide.

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETWORKHOME/.replication</td>
<td>Contains the local and remote timestamps used by GWSync.</td>
</tr>
<tr>
<td>NETWORKHOME/.replication_remote</td>
<td></td>
</tr>
<tr>
<td>NETWORKHOME/.replication_log</td>
<td>This log is only populated if the GWSync local and remote timestamps are more than 10 minutes apart (and a System event is generated), as in the following example:</td>
</tr>
<tr>
<td></td>
<td>Replication failed since: date</td>
</tr>
<tr>
<td>NETWORKHOME/oracle_monitoring.log</td>
<td>Information on the Redo-apply log from the standby server.</td>
</tr>
<tr>
<td></td>
<td>+ Testing the replication state on the remote database</td>
</tr>
<tr>
<td></td>
<td>- Redo transport lag:</td>
</tr>
<tr>
<td></td>
<td>NAME VALUE TIME_COMPLETED</td>
</tr>
<tr>
<td></td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>transport lag +00 00:00:00 04/14/2011 10:30:34</td>
</tr>
<tr>
<td></td>
<td>- Redo apply lag:</td>
</tr>
<tr>
<td></td>
<td>NAME VALUE TIME_COMPLETED</td>
</tr>
<tr>
<td></td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>apply lag +00 00:00:00 04/14/2011 10:30:35</td>
</tr>
<tr>
<td></td>
<td>- Active apply rate:</td>
</tr>
<tr>
<td></td>
<td>ITEM UNITS SO FAR</td>
</tr>
<tr>
<td></td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td>Active Apply Rate KB/sec 286</td>
</tr>
<tr>
<td></td>
<td>- Data base role: PHYSICAL STANDBY</td>
</tr>
</tbody>
</table>
Checking Overall Status Using primeha

The **primeha** command is a central tool for checking the status of the high availability nodes, performing switchovers and failovers, and stopping and resuming data replication. The following example shows a configuration for a network that has both local and geographical redundancy.

- The first portion of the output shows the status of the geographical redundancy configuration. The server csi-incy.cisco.com is the remote standby gateway and database server. The server csi-w47.cisco.com is the other node in the local redundancy cluster and he is not running any service.

- The second portion of the output (that begins with Cluster Status) shows the status of the local redundancy configuration. (This is displayed because this setup also contains a local redundancy configuration.)

```
# perl primeha -status
+ Installing perl for HA
- Installing ActivePerl-5.10.1.1007-x86_64-linux-glibc-2.3.3-291969
- Extracting additional modules

HOST                ANA SERVICE                              ORACLE SERVICE
---------- ---------------                          ----------
csi-bvc.cisco.com   Active Prime Network                     Active oracle    local
csi-exy.cisco.com   Standby Prime Network                    Standby oracle
csi-w47.cisco.com   Prime Network not running on this node    oracle not running on this node

Cluster Status for ana_cluster @ Mon Aug  1 12:34:40 2011
Member Status: Quorate

Member Name        ID Status
---------- ---- ------
csi-bvc.cisco.com  1 Online, Local, rgmanager
csi-w47.cisco.com  2 Online, rgmanager

Service Name       Owner (Last)        State
------- ---------- -----         ------
service:ana        csi-bvc.cisco.com  started
service:oracle_db  csi-bvc.cisco.com  started
```

Performing a Schedule Site Move (primeha - switch)

Use the **primeha -switch** command to perform a scheduled move from a local primary site to a remote secondary site, when both sites are active. This is called a switchover. This is used for planned switches initiated by administrators.

The **primeha -switch** command will use the inputs you provided when you installed the gateway server high availability solution but will also give you an opportunity to modify those settings before performing the switchover. The switchover process consists of the following:

- Switch the roles between the primary and secondary sites.
- Switch the data replication sides (ADG and GWSync). In other words, the new primary site will be replicated to the new secondary site.

You can also use the switchover command to fallback to the primary site when a failed server is brought back online. The switchover will again reverse the replication directions. After performing a manual switchover, move any AVMs from unreachable units at the primary site to reachable units at the remote site.
This script must be run from the server with the primary active database.

To perform a switchover:

**Step 1**
Log into the server that contains the primary active database. (You can validate this by running `primeha-status`.)

**Step 2**
Move to the proper directory and start the script. The script will use the inputs you provided when you installed the gateway server high availability solution but will also give you an opportunity to modify those settings before performing the switchover.

Keep the following notes in mind:

- If the setup includes a dual-node cluster, when you are prompted for the gateway and database IP addresses, use the floating IP addresses for the Prime Network and Oracle services.
- You are only prompted for the “other cluster node” if the utility is invoked from a server that is part of a local redundancy setup. You should enter the IP address of the other cluster node—that is, the node the script is not being run from.

```bash
# cd /var/adm/cisco/prime-network/scripts/ha/util
# perl primeha -switch
```

* Switching over to remote node
* These are the parameters for the switchover process you will switch over to:
  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateway</td>
<td>10.56.56.57</td>
</tr>
<tr>
<td>database</td>
<td>10.56.56.57</td>
</tr>
<tr>
<td>other cluster node</td>
<td>10.56.56.67</td>
</tr>
<tr>
<td>Prime Network user</td>
<td>network39</td>
</tr>
<tr>
<td>Prime Network user home</td>
<td>/export/home/network39</td>
</tr>
<tr>
<td>oracle user</td>
<td>oracle</td>
</tr>
<tr>
<td>oracle user home</td>
<td>/opt/ora/oracle</td>
</tr>
</tbody>
</table>

**Step 3**
Approve or edit your switchover choices at the following prompt:

Do you approve? (yes/no)

- If you say **yes** and the system is using external authentication (LDAP), provide the necessary information at the following prompt (see Table 7-3 on page 7-11):

  Does this setup have an LDAP configured? (yes/no)

  Otherwise, proceed to **Step 4**.

- If you say **no**, you are prompted for the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of the remote gateway server</td>
<td>IP address of the standby gateway. If the remote node is a member of a dual-node cluster, use the floating IP address.</td>
</tr>
<tr>
<td>Root password for the node that has the gateway mounted</td>
<td>For the remote gateway server, the root password for the operating system (required for SSH).</td>
</tr>
<tr>
<td>IP address of the remote database</td>
<td>IP address of the standby database. If the remote node is a member of a dual-node cluster, use the floating IP address.</td>
</tr>
<tr>
<td>Root password for the node that has the database mounted</td>
<td>For the remote database, the root password for the operating system (required for SSH).</td>
</tr>
</tbody>
</table>
### Chapter 18      Using RHCS/ADG Gateway Server High Availability

#### Oracle Active Data Guard (ADG) Geographical Redundancy

**Step 4** Confirm that you want to continue with the switchover. Prime Network proceeds and displays text similar to the following.

- Checking if Prime Network is mounted on local node  [MOUNTED]
- Verifying local oracle status
- Verifying remote oracle status
- Changing local Prime Network flag to remote  [OK]
- Stopping Prime Network on local side..  [OK]
- Switching local server to remote
- Copying scripts to remote database
- Running pre-switchover script on remote database
- Changing local oracle flag to remote
- Copying scripts to remote database
- Running switchover script on remote database
- Copying scripts to remote gateway
- Running switchover script on remote gateway
- Switching local server to recover mode
- Set db to read only mode

**Step 5** If required, manually move the AVMs from the unreachable units at the primary site to the reachable units at the remote site. See Moving and Deleting AVMs, page 4-13. (This is not required if the local units were not affected by a failure; the script will reconfigure the units to use the relevant gateway and database.)

**Step 6** Verify that the new gateway IP address and database IP addresses are correct. If needed, switch the IP address manually using one of the following procedures:

- Changing the Gateway IP Address on a Gateway and All Units (changeSite.pl), page 18-22
- Changing the Gateway IP Address on a Single Unit (switchUnit.pl), page 18-24

### Field Description Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of “other cluster node”</td>
<td>(If the local node is a member of a dual-node cluster) The IP address of the other node in the cluster.</td>
</tr>
<tr>
<td>Password for the other cluster node</td>
<td>(If the local node is a member of a dual-node cluster) For the other node in the cluster, the root password for the operating system (required for SSH).</td>
</tr>
<tr>
<td>Name for the OS user of the database</td>
<td>Name of database OS user.</td>
</tr>
<tr>
<td>Home directory of the user</td>
<td>Home directory for database OS user.</td>
</tr>
<tr>
<td>Name for the OS user for Prime Network</td>
<td>Name of Prime Network OS user.</td>
</tr>
<tr>
<td>Home directory of the user</td>
<td>Home directory for Prime Network OS user.</td>
</tr>
<tr>
<td>Whether the setup has LDAP configured</td>
<td>If system users LDAP (external authentication) for user authentication (see Table 7-3 on page 7-11).</td>
</tr>
</tbody>
</table>
Using Failover for Disaster Recovery (primeha -fail)

Caution

Failover is time-consuming and requires the system to be shut down. It should only be used when the primary site fails. Do not execute it until all other options for restoring the primary site are explored.

Note

A manual failover should only be performed when the primary site has failed.

Use the primeha -fail command to perform a site switch for disaster recovery. A site switch is a manual move from the local primary site to the remote secondary site. The script will use the inputs you provided when you installed the gateway server high availability solution but will also give you an opportunity to modify those settings before performing the failover. When you invoke primeha -fail, the command does the following:

- Disconnects the primary site from the secondary site.
- Stops the GWSync and ADG replication processes.
- Start the standby server as standalone node without geographical redundancy.

After performing a manual failover, move any AVMs from unreachable units at the primary site to reachable units at the remote site.

Note

The failover must be run from the node that contains the standby database. If the system is using external authentication (LDAP), you will have to provide the LDAP URL, distinguished name prefix and suffix, and the protocol (see Table 7-3 on page 7-11).

To perform a failover:

**Step 1**

As root, log into the active node that contains the standby database. (You can validate this by running primeha -status.)

Move to the proper directory and start the script. The script will use the inputs you provided when you installed the gateway server high availability solution but will also give you an opportunity to modify those settings before performing the failover.

Keep the following notes in mind:

- If the setup includes a dual-node cluster, when you are prompted for the gateway and database IP addresses, use the floating IP addresses for the Prime Network and Oracle services.
- You are only prompted for the “other cluster node” if the utility is invoked from a server that is part of a local redundancy setup. You should enter the IP address of the other cluster node—that is, the node the script is not being run from.

```bash
# cd /var/adm/cisco/prime-network/scripts/ha/util
# perl primeha -fail
+ Failing over to remote node
+ These are the parameters for the fail over process
  you will fail over to:
  gateway  : 10.56.56.74
  database : 10.56.56.41
  from :
    gateway  : 10.56.56.57
    database : 10.56.56.57
    other cluster node : 10.56.56.67
    Prime Network user : network39
```
Step 2
Approve or edit your switchover choices at the following prompt:

Do you approve? (yes/no)

- If you say yes and the system is using external authentication (LDAP), provide the necessary information at the following prompt (see Table 7-3 on page 7-11):

  Does this setup have an LDAP configured?

  If you say yes and the system is not using external authentication, proceed to Step 3.

- If you say no, you are prompted for the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of the remote gateway server</td>
<td>IP address of the standby gateway. If the remote node is a member of a dual-node cluster, use the floating IP address.</td>
</tr>
<tr>
<td>Root password for the node that has the gateway mounted</td>
<td>For the remote gateway server, the root password for the operating system (required for SSH).</td>
</tr>
<tr>
<td>IP address of the remote database</td>
<td>IP address of the standby database. If the remote node is a member of a dual-node cluster, use the floating IP address.</td>
</tr>
<tr>
<td>Root password for the node that has the database mounted</td>
<td>For the remote database, the root password for the operating system (required for SSH).</td>
</tr>
<tr>
<td>IP address of “other cluster node”</td>
<td>(If the local node is a member of a dual-node cluster) The IP address of the other node in the cluster.</td>
</tr>
<tr>
<td>Password for the other cluster node</td>
<td>(If the local node is a member of a dual-node cluster) For the other node in the cluster, the root password for the operating system (required for SSH).</td>
</tr>
<tr>
<td>Name for the OS user of the database</td>
<td>Name of database OS user.</td>
</tr>
<tr>
<td>Home directory of the user</td>
<td>Home directory for database OS user.</td>
</tr>
<tr>
<td>Name for the OS user for Prime Network</td>
<td>Name of Prime Network OS user.</td>
</tr>
<tr>
<td>Home directory of the user</td>
<td>Home directory for Prime Network OS user.</td>
</tr>
<tr>
<td>Whether the setup has LDAP configured</td>
<td>If system users LDAP (external authentication) for user authentication (see Table 7-3 on page 7-11).</td>
</tr>
</tbody>
</table>

Step 3
Confirm that you want to continue with the failover. Prime Network proceeds and displays text similar to the following.

- Checking if Prime Network is mounted on local node [MOUNTED]
- Verifying local oracle status
- Copying scripts to remote gateway
- Running failover script on remote gateway
- Copying scripts to remote database
- Running failover script on remote database
- Switching local db to active mode
- Changing remote oracle flag to local
- Starting replication monitoring cron [OK]
- Changing remote Prime Network flag to local [OK]
- Copying scripts to sub
- Running script on cluster standby node

**Step 4** Move any AVMs from unreachable units at the primary site to reachable units at the remote site. See Moving and Deleting AVMs, page 4-13.

**Step 5** Verify that the new gateway IP address and database IP addresses are correct. If needed, switch the IP address manually using one of the following procedures:
- Changing the Gateway IP Address on a Gateway and All Units (changeSite.pl), page 18-22
- Changing the Gateway IP Address on a Single Unit (switchUnit.pl), page 18-24

---

**Stopping Data Replication (primeha -stop)**

Use the stop replication command `primeha -stop` when you need to perform scheduled work on a server in the remote site. It stops the replication process to the remote site and shuts down the remote database. To resume replication, see Resuming Data Replication (primeha -start), page 18-21.

**Note** This command *must* be run from the server that contains the standby database. (You can validate this by running `primeha -status`.)

To run the stop replication command:

```
# cd /var/adm/cisco/prime-network/scripts/ha/util
# perl primeha -stop
```

The following is an example of a stop replication session. In this example:

- The remote standby gateway and database IP address is 10.56.56.57. The user wants to stop the replication of data from the local site to this remote site.
- The local gateway IP address is 10.56.57.74 and the local database IP address is 10.56.56.41.

This utility must be run from the server with the remote standby database (in this example, 10.56.56.57). This will stop replicating data and will shut down the remote database.

Keep these notes in mind when you are prompted for the following information:

- Remote server's gateway IP address—Enter the IP address for the primary gateway. If the primary site has a local redundancy setup, enter the floating IP address for the Prime Network service.
- Remote database IP address—Enter the IP address for the primary database. If the primary site has a local redundancy setup, enter the floating IP address of the Oracle service.
- Cluster sub server's IP address—(Is displayed only if the standby database is part of a cluster) Enter the physical IP address of the other cluster node—that is, the node the script is not being run from.

```
[root@10.56.56.57]# perl primeha -stop
```

+ Installing perl for HA
- Installing ActivePerl-5.10.1.1007-x86_64-linux-glibc-2.3.3-291969
- Extracting additional modules

+ Stopping replication to remote node
- Enter the remote server's gateway IP address: 10.56.56.74
- Enter the root password for the node that has the gateway mounted
- Enter the remote database IP address: 10.56.56.41
- Enter the root password for the node that has the database mounted
- Enter a name for the OS user of the database [oracle]
- Enter the home directory of the user (oracle) [/opt/ora/oracle]
- Enter a name for the OS user for Prime Network [network39]
- Enter the home directory of the user (Prime Network) [/export/home/network39]
- Checking if Prime Network is mounted on local node [MOUNTED]
- Removing local node Prime Network flag
- Stopping local db replication
- Removing local node database flag
- Stopping replication on remote gateway
- Copying scripts to remote database
- Running stop replication script on remote database
+ Removing perl for HA

Resuming Data Replication (primeha -start)

This command can only be used if (1) the remote database was stopped using primeha -stop, and (2) the remote database has not been down for more than seven days. If the remote database has been down for more than seven days, you must recreate the remote database by using the setup_Prime_DR.pl script (see the Cisco Prime Network 3.9 Installation Guide for information on how to use that script.)

Use the resume replication utility primeha -start to start the database at the remote site (in open, read-only mode) and restart the replication process. This command should only be used after stopping replication in order to perform scheduled work on the remote site.

This command must be run from the server that contains the remote standby database. (You can validate this by running primeha -status.)

Keep these notes in mind when you are prompted for the following information:

- Remote server’s gateway IP address—Enter the IP address for the primary gateway. If the primary site has a local redundancy setup, enter the floating IP address for the Prime Network service.
- Remote database IP address—Enter the IP address for the primary database. If the primary site has a local redundancy setup, enter the floating IP address of the Oracle service.
- Cluster sub server’s IP address—(Is displayed only if the standby database is part of a cluster) Enter the physical IP address of the other cluster node—that is, the node the script is not being run from.

To run the resume replication command:

```
# cd /var/adm/cisco/prime-network/scripts/ha/util
# perl primeha -start
```

The following is an example of a primeha -start session. It uses the same parameters as the stop replication example:

- The remote standby gateway and database IP address is 10.56.56.57. The user wants to restart the replication of data from the local site to this remote site.
- The primary gateway IP address is 10.56.57.75 and the primary database IP address is 10.56.56.41. The user wants to restart the remote database in read-only mode (in other words, make it the standby database), and resume replicating data. This utility is run from the node with the remote standby database (10.56.56.57).
[root@10.56.56.57]# perl primehah -start
  + Installing perl for HA
  - Installing ActivePerl-5.10.1.1007-x86_64-linux-glibc-2.3.3-291969
  - Extracting additional modules
  + Resuming replication to remote node
  - Enter the remote server’s gateway IP address: 10.56.56.74
  - Enter the root password for the node that has the gateway mounted
  - Enter the remote data base IP address: 10.56.56.41
  - Enter the root password for the node that has the data base mounted
  - Enter the home directory of the user (oracle) [/opt/ora/oracle]
  - Enter a name for the OS user for Prime Network [network39]
  - Enter the home directory of the user (Prime Network) [/export/home/network39]
  - Resuming local db replication
  - Adding local node data base flag
  - Checking if Prime Network is mounted on local node [MOUNTED]
  - Adding local node Prime Network flag
  - Resuming replication on remote gateway
  - Copying scripts to remote database
  - Running resume replication script on remote database
  + Removing perl for HA

### Changing IP Addresses (ADG Geographical Redundancy)

If all IP addresses are not automatically changed after a failover or switchover, use the following procedures, as appropriate.

- Changing the Gateway IP Address on a Gateway and All Units (changeSite.pl), page 18-22
- Changing the Gateway IP Address on a Single Unit (switchUnit.pl), page 18-24

#### Changing the Gateway IP Address on a Gateway and All Units (changeSite.pl)

If the gateway IP address is not updated on any of the units (or on the gateway) during a site-to-site failover or switchover, use the changeSite.pl utility to do so manually. This procedure will change the address on the gateway and all reachable units.

**Note**
If a dual-node cluster is part of a local redundancy setup, use the logical IP addresses.

The following table describes the options to the changeSite.pl utility. If you are using an external LDAP server for user authentication, you must also set the necessary LDAP parameters, as described below. For more details on these parameters, see Configuring Prime Network to Communicate with the External LDAP Server, page 7-10.
Chapter 18      Using RHCS/ADG Gateway Server High Availability

Oracle Active Data Guard (ADG) Geographical Redundancy

Step 1
If you will reset LDAP information, reconfigure them first from the Prime Network Administration GUI client. See Configuring Prime Network to Communicate with the External LDAP Server, page 7-10.

Step 2
Log into the primary gateway server as network user.

Step 3
Change to the correct directory:
# cd $ANAHOME/Main/ha

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-force</td>
<td>Allow manual change to registry settings. (Because this script runs as part of a failover or switchover, the -force option is required when running the script from the command line.)</td>
</tr>
<tr>
<td>-newgwip new-gateway-ip</td>
<td>IP address of the gateway that is running after the failover or switchover.</td>
</tr>
<tr>
<td>-newdbip new-database-ip</td>
<td>IP address of the database that running after the failover or switchover.</td>
</tr>
<tr>
<td>-oldgwip old-gateway-ip</td>
<td>IP address of the gateway that was running prior to the failover or switchover.</td>
</tr>
<tr>
<td>-olddbip old-database-ip</td>
<td>IP address of the database that was running prior to the failover or switchover.</td>
</tr>
<tr>
<td>[ -newldapurl new-ldap-url ] [ old-ldap-url ]</td>
<td>(LDAP only) URL for the LDAP server that will be used by the running gateway (new-ldap-url), and the URL that was used by the gateway that was running prior to the failover or switchover (old-ldap-url). Use the following format: ldap://host.company.com:port</td>
</tr>
<tr>
<td>[ -newldapprefix new-ldap-prefix ] [ old-ldap-prefix ]</td>
<td>(LDAP only) First part of the LDAP DN (which is used to uniquely identify users) for the new and old LDAP server. Both new-ldap-prefix and old-ldap-prefix should be entered exactly as shown below: CN (The actual format is CN=Value, which specifies the common name for specific users. =Value will be automatically populated with Prime Network usernames.)</td>
</tr>
<tr>
<td>[ -newldapsuffix new-ldap-suffix ] [ old-ldap-suffix ]</td>
<td>(LDAP only) Second part of the LDAP distinguished name, which specifies the location in the directory for both the new and old LDAP servers. Both new-ldap-suffix and old-ldap-suffix should use the following format, CN=Users,DC=LDAP_server,DC=company,DC=com</td>
</tr>
<tr>
<td>[ -newldapisssl new-ldap-is-ssl ] [ old-ldap-is-ssl ]</td>
<td>(LDAP only) Encryption protocol to be used for communication between the running Prime Network gateway server and the new LDAP server (new-ldap-is-ssl), and the protocol that was used between the old gateway and LDAP servers (old-ldap-is-ssl).</td>
</tr>
</tbody>
</table>
Step 4  
Run the following command:
```
# perl changeSite.pl -force -newgwip new-gw-ip -newdbip new-db-ip
   -oldgwip old-gw-ip -olddbip old-db-ip
   [-newldapurl new-ldap-url -oldldapurl old-ldap-url]
   [-newldapprefix new-ldap-prefix -oldldapprefix old-ldap-prefix]
   [-newldapsuffix new-ldap-suffix -oldldapsuffix old-ldap-suffix]
   [-newldapisssl new-ldap-is-ssl -oldldapisssl old-ldap-is-ssl]
```

The following is an example of a changeSite.pl session. In this example the following is being changed:
- The original gateway and database IP address was 10.56.56.57.
- The site was switched over to the standby gateway (10.56.56.74) and database (10.56.56.41).

For some reason, the IP addresses were not correctly changed to reflect the new addresses. The utility forces the IP addresses to be changed to 10.56.56.74 for the gateway and 10.56.56.41 for the database. In this example the system is not using LDAP, so those parameters are not included.

```
csi-exy% cd $ANAHOME/Main/ha
csi-exy% perl changeSite.pl -force -newgwip 10.56.56.74 -newdbip 10.56.56.41 -oldgwip 10.56.56.57 -olddbip 10.56.56.57
Thu Apr 14 16:08:22 2011 --[INFO]: 'Forced change of gw address from 10.56.56.57 to 10.56.56.74....'
Thu Apr 14 16:08:22 2011 --[INFO]: 'changing uplinks for gw AVM0'
Thu Apr 14 16:08:22 2011 --[INFO]: 'changing uplinks for unit AVM0s'
Thu Apr 14 16:08:22 2011 --[INFO]: 'changing gw ip and haservice for unit AVM99s'
Thu Apr 14 16:08:22 2011 --[INFO]: 'changing registry on units'
Thu Apr 14 16:08:37 2011 --[INFO]: 'changing localhost entry for gw AVM99'
Thu Apr 14 16:08:37 2011 --[INFO]: 'Forced change of db server address from 10.56.56.57 to 10.56.56.41....'
Thu Apr 14 16:08:37 2011 --[INFO]: 'changing db server ip for gw AVM66'
Thu Apr 14 16:08:38 2011 --[INFO]: 'changing db server ip for gw persistency.xml'
Thu Apr 14 16:08:38 2011 --[INFO]: 'changing db server ip for template persistency.xml'
Thu Apr 14 16:08:38 2011 --[INFO]: 'changing db server ip for unit persistency.xml'
Thu Apr 14 16:08:38 2011 --[INFO]: 'Forced change of NCCM address from 10.56.56.57 to 10.56.56.41....'
new IP address is: 10.56.56.41
jdbc.properties file has been updated to change to new IP address
Thu Apr 14 16:08:39 2011 --[INFO]: '->Done'
```

Changing the Gateway IP Address on a Single Unit (switchUnit.pl)

If any of the units do not reflect the updated gateway and database IP address after a site-to-site failover or switchover, use the switchUnit.pl utility to do so manually. This procedure will change the address only on the unit from which it is run.

Note  
If a dual-node cluster is part of a local redundancy setup, use the logical IP addresses.

For any unit that does not reflect the updated gateway and database IP addresses:

Step 1  
Log into the unit as network user.

Step 2  
Change to the correct directory:
```
# cd $ANAHOME/Main/ha
```
Step 3 Run the following command:

```
# perl switchUnit.pl new-gw-ip old-gw-ip new-db-ip old-db-ip
```
PART 4

Basic VNE Administration
VNE Administration: VNE Lifecycle and Creating VNEs

These topics provide information about advanced VNE administration tasks:

- What Are VNE Communication and Investigation States?, page 19-1
- Choosing a VNE Scheme, page 19-5
- Adding VNEs, page 19-11
- Viewing and Editing VNE Properties, page 19-28
- Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-44
- Controlling Concurrent VNE Telnet Logins (Staggering VNEs), page 19-45

Additional VNE administration tasks are described in:

- Basic AVM and VNE Administration Tasks, page 4-1
- Troubleshooting VNE Modeling, page 20-1
- VNE Updates, page 21-1

What Are VNE Communication and Investigation States?

VNE states describe to what degree the VNE has discovered and modeled a device, and the disposition of the communication between the VNE and the device it models. This information is very granular and can help you pinpoint why a device is not completely modeled or why it is unreachable.

There are two types of VNE states:

- VNE communication states convey the status of communication between devices and VNEs, and VNEs and the gateway server. The states and their GUI decorators are listed in VNE Communication States, page 19-3. Prime Network generates a Service event whenever a VNE’s communication state changes.

- VNE investigation states represent the different degrees to which the VNE has successfully discovered and modeled a network element. In other words, it gives you an idea of the quality and stability of the device inventory. These states and their GUI decorators are listed in VNE Investigation States, page 19-4. Because investigation states frequently change, Prime Network does not generate a Service event whenever a VNE’s investigation state changes (although you can configure it to do so; see Registry Settings for VNE Discovery Timeout and Investigation State Reporting, page 20-23).
Both the communication and investigation states are displayed in text format in Prime Network Vision when you open a device properties window, as shown in Figure 19-1.

**Figure 19-1  VNE Communication and Investigation States (in Prime Network Vision)**

![VNE Communication and Investigation States](image)

**Note**  If the VNE was stopped, you will see a message and a refresh button at the top of the properties window. If the VNE was restarted, refreshing the window will repopulate the information. However, if the VNE is still down, refreshing the window will result in an error message. To start the VNE, see Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-44.

If you want more information about the communication state, click **VNE Status** to get information on the status of:

- Protocols the device uses to communicate with the VNE.
- Traps and syslog forwarding from the device to the VNE.

This information is helpful for troubleshooting device reachability problems. For more information, see VNE Communication States, page 19-3.
VNE Communication States

VNE communication states convey the status of two types of connections, both of which are needed for Prime Network to successfully manage a device:

- Communication status between the VNE and the device it is monitoring (management issues).
- Communication status between the VNE and the gateway (agent issues).

Management communication—between a VNE and a device—is where problems normally occur. Devices and VNEs communicate using SNMP, Telnet, ICMP and notification protocols such as traps and sylogs—all of which determine whether a device is truly reachable. Prime Network runs tests tailored to each (enabled) protocol to determine the seriousness of a reachability problem. By default, Prime Network does not mark a device as Device Unreachable unless all of the enabled device management protocols are unresponsive, and the device is not generating sylogs or traps. You can adjust the settings that control when a device is considered unreachable. For information on how to do this, and details about how Prime Network determines reachability for different protocols, see How Prime Network Determines Protocol Reachability, page 24-3.

When a VNE’s communication state changes, Prime Network generates a Service event which you can view in Prime Network Events and Vision. An event is generated for newly-started VNEs only when all protocols have been tested. Reachability-related events are also correlated to each other and to any relevant tickets on the managed device. New events will also be correlated to the relevant ticket.

If a Service event indicates a possible problem, check the event details to see if there is a genuine problem with the device. For example, a Device Unreachable event could signal a device protocol problem, or it may indicate that a VNE was shutdown as part of normal maintenance.

<table>
<thead>
<tr>
<th>State Name</th>
<th>Description</th>
<th>Badge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Not Loaded</td>
<td>The VNE is not responding to the gateway because it was stopped, or it was just created. This communication state is the equivalent of the Defined Not Started investigation state.</td>
<td>None</td>
</tr>
<tr>
<td>VNE/Agent Unreachable</td>
<td>The VNE is not responding to the gateway. This can happen if the unit or AVM is overutilized, the connection between the gateway and unit or AVM was lost, or the VNE is not responding in a timely fashion. (A VNE in this state does not mean the device is down; it might still be processing network traffic.)</td>
<td>🚧</td>
</tr>
</tbody>
</table>

Table 19-1 describes all of the possible VNE communication states. It also shows the GUI decorator for each state, where applicable. For information on troubleshooting communication state issues, see Steps to Troubleshoot VNE Communication State Issues, page 20-3.

The 🚧 icon indicates a network element has been deleted (or moved). The state will show N/A for Cloud VNEs because Cloud VNEs do not represent a real network element (see Unmanaged Segments and Cloud VNEs, page 23-1).
What Are VNE Communication and Investigation States?

Table 19-1  VNE Communication States (continued)

<table>
<thead>
<tr>
<th>State Name</th>
<th>Description</th>
<th>Badge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting</td>
<td>The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state. Because the investigation state decorator (the hourglass) will already be displayed, a special GUI decorator is not required.</td>
<td>None</td>
</tr>
<tr>
<td>Device Partially Reachable</td>
<td>The element is not fully reachable because at least one protocol is not operational. Note This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see VNE Management Communication Policies and How To Change Them, page 24-1.</td>
<td>None</td>
</tr>
<tr>
<td>Device Reachable</td>
<td>All element protocols are enabled and connected. Note This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see VNE Management Communication Policies and How To Change Them, page 24-1.</td>
<td>None</td>
</tr>
<tr>
<td>Device Unreachable</td>
<td>The connection between the VNE and the device id down because all of the protocols are down (though the device might be sending traps or syslogs). Note This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see VNE Management Communication Policies and How To Change Them, page 24-1.</td>
<td>None</td>
</tr>
<tr>
<td>Tracking Disabled</td>
<td>The reachability detection process is not enabled for any of the protocols used by the VNE (specifically, the trackreachability registry key is not set to true; see Customizing Protocol Reachability Testing, page 24-7). The VNE will not perform reachability tests nor will Cisco Prime Network generate reachability-related events. In some cases this is desirable; for example, tracking for Cloud VNEs should be disabled because Cloud VNEs represent unmanaged network segments. Because this is a user-defined mode (rather than an error or transitional mode), Cisco Prime Network does not display a decorator for this state. To troubleshoot a VNE that is in this state, check the VNE Status Details window; see Troubleshooting VNE Communication State Issues, page 20-1.</td>
<td>None</td>
</tr>
</tbody>
</table>

VNE Investigation States

VNE investigation states describe how successfully a VNE has modeled the device it represents. These states describe all of the possibilities in the VNE life cycle, from when the VNE is added to Prime Network, through the device modelling, until the VNE is stopped. Table 19-2 describes all of the possible VNE investigation states. It also shows the GUI decorator for each state, where applicable.

At any time you can restart the VNE discovery process by restarting the VNE (see Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-44). If you want to rediscover only a certain element within a device, go to the Prime Network Vision GUI client, open the device inventory, and right-click the element and choose Pull Now.

For troubleshooting information, see Troubleshooting VNE Modeling, page 20-1.

The icon indicates a network element has been deleted (or moved). The state will show N/A for Cloud VNEs because Cloud VNEs do not represent a real network element (see Unmanaged Segments and Cloud VNEs, page 23-1).
Choosing a VNE Scheme

VNE schemes determine what data should be retrieved for each device, along with the commands and protocols Prime Network should use to collect that data. The scheme settings are arranged in an inheritance tree and incorporated into the configuration registry to support default values at any

Table 19-2  VNE Investigation States

<table>
<thead>
<tr>
<th>State Name</th>
<th>Description</th>
<th>Badge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined Not Started</td>
<td>A new VNE was created (and is starting); or an existing VNE was stopped. In this state, the VNE is managed and is validating support for the device type. (This investigation state is the equivalent of the Agent Not Loaded communication state.) A VNE remains in this state until it is started (or restarted).</td>
<td>None</td>
</tr>
<tr>
<td>Unsupported</td>
<td>The device type is either not supported by Prime Network or is misconfigured (it is using the wrong scheme, or is using reduced polling but the device does not support it). To extend Cisco Prime Network functionality so that it recognizes unsupported devices, use the VNE Customization Builder. See the <em>Cisco Prime Network 3.9 Customization User Guide</em>.</td>
<td></td>
</tr>
<tr>
<td>Discovering</td>
<td>The VNE is building the model of the device (the device type was found and is supported by Cisco Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery timeout.</td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td>The VNE has a stable model of the device. Modeling may not be fully complete, but there is enough information to monitor the device and make its data available to other applications, such as activation scripts. A VNE remains in this state unless it is stopped or moved to the maintenance state, or there are device errors.</td>
<td>None</td>
</tr>
<tr>
<td>Currently Unsynchronized</td>
<td>The VNE model is inconsistent with the device. This can be due to a variety of reasons; for a list of these reasons along with troubleshooting tips, see Troubleshooting VNE Investigation State (Discovery) Issues, page 20-14.</td>
<td></td>
</tr>
</tbody>
</table>
| Maintenance             | VNE polling was suspended because the VNE was manually moved to this state (by right-clicking the VNE and choosing Actions > Maintenance). The VNE remains in this state until it is manually restarted. A VNE in the maintenance state has the following characteristics:  
  * It does not poll the device or process traps and syslogs.  
  * It maintains the status of any existing links.  
  * It responds to VNE reachability requests.  
  * It passively participates in correlation flow issues (but is not an initiator).  
  The VNE is moved to the Stopped state if: it is VNE is moved, the parent AVM is moved or restarted, the parent unit switches to a standby unit, or the gateway is restarted. |       |
| Partially Discovered    | The VNE model is inconsistent with the device because a required device command failed, even after repeated retries. A common cause of this state is that the device contains an unsupported module. To extend Cisco Prime Network functionality so that it recognizes unsupported modules, use the VNE Customization Builder. See the *Cisco Prime Network 3.9 Customization User Guide*. |       |
| Shutting Down           | The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device.                                                                                                                                                 |       |
| Stopped                 | The VNE process has terminated; it will immediately move to Defined Not Started.                                                                                                                                                                      | None  |
Choosing a VNE Scheme

level—and the option to inherit or override default settings—on the basis of device vendor, type, model, version etc. The scheme settings can be changed at a very granular level, such as specific device instances or specific aspects of inventory within devices. For example, different polling frequencies can be set for different port types within a device.

If you chose the wrong scheme when you created the VNE, you will have to delete and recreate the VNE.

You can also supplement what is modeled by creating new soft properties. These allows you to model additional attributes and create new threshold crossing alarms. For more information on the Soft Properties Manager, see the Cisco Prime Network 3.9 Customization User Guide.

When creating a VNE, choose a scheme that is based on the device family and on the technologies you want Prime Network to manage. This enables you to define different behavior for different devices. For example, some devices poll only with SNMP, while other devices poll with Telnet. Soft properties and activation scripts are also attached to a specific scheme.

Note

When you create a VNE, Prime Network provides a drop-down list of available schemes. The list includes a “default” choice. If you choose default, Prime Network sets the scheme to Product.

Prime Network uses the following schemes:

- **Product**—This scheme is used for all device types in this release, except for Cisco CRS and Cisco 3750ME devices.
- **IpCore**—This scheme is used only for routers serving as Provider (P) or Provider Edge (PE) devices.

The difference between the two schemes is that IpCore assumes that the device is used as part of an MPLS VPN network containing P and PE devices. Prime Network therefore models these VNEs slightly differently. Use Product for all other instances, including customer edge (CE) devices. The Product scheme assumes that no MPLS or VRF configuration exists and thus does not retrieve it.

These schemes provide users with the flexibility to specify the registrations (device commands, or methods the VNE uses to query the device for information) that the VNEs modeling their routers are to use. You can designate a VNE as a core router by setting it to work with the IpCore scheme, or as an edge router by setting it to work with the Product scheme.

Table 19-3 identifies the technologies supported by each scheme.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="#">ACL</a></td>
<td>Product</td>
</tr>
<tr>
<td><a href="#">ATM</a></td>
<td>Yes</td>
</tr>
<tr>
<td>6PE and 6VPE-based IPv6 Connectivity</td>
<td>Yes</td>
</tr>
<tr>
<td>6RD</td>
<td>Yes</td>
</tr>
<tr>
<td>ATM PW</td>
<td>No</td>
</tr>
<tr>
<td>Backup Pseudowire</td>
<td>No</td>
</tr>
<tr>
<td><strong>BFD</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>BGP</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 19-3 **Technology Support Based on Schemes**
<table>
<thead>
<tr>
<th>Technology</th>
<th>Scheme</th>
<th>Product</th>
<th>IpCore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier Supporting Carrier (CSC)</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>CDP</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CEM Group</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CFM</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CGN</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Clocking Enhancements</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DSx</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EFP</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Ethernet</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ethernet Channel</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ethernet IEEE 802.3 Dot1Q/VLAN</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ethernet LMI</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ethernet OAM</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Frame Relay</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GRE</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HDLC</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hierarchical VPLS</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>IMA</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IP Routing</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IP and ARP</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPoDWDM</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>IPSec^1</td>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IPSLA Responder</td>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IPv6</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IRB/BVI</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ISIS</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ISIS IGPv6</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>L3 VPN and VRF</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>LAG (IEEE 802.3ad)</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LLDP</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Local Switching</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MLACP</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MLPPP</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MP-BGP</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>MPLS</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Choosing a VNE Scheme

Chapter 19  VNE Administration: VNE Lifecycle and Creating VNEs

Table 19-3  Technology Support Based on Schemes (continued)

<table>
<thead>
<tr>
<th>Technology</th>
<th>Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Product</td>
</tr>
<tr>
<td>MPLS P2MP TE</td>
<td>No</td>
</tr>
<tr>
<td>MPLS TE-Tunnel (including FRR)</td>
<td>No</td>
</tr>
<tr>
<td>MPLS TP</td>
<td>No</td>
</tr>
<tr>
<td>MST-AG/REP-AG</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF</td>
<td>Yes</td>
</tr>
<tr>
<td>POS</td>
<td>Yes</td>
</tr>
<tr>
<td>PPP</td>
<td>Yes</td>
</tr>
<tr>
<td>PTP 1588</td>
<td>Yes</td>
</tr>
<tr>
<td>PWE3, L2 VPN (Martini)</td>
<td>No</td>
</tr>
<tr>
<td>PW VCCV</td>
<td>No</td>
</tr>
<tr>
<td>Q-in-Q (IEEE 802.1ad)</td>
<td>Yes</td>
</tr>
<tr>
<td>REP</td>
<td>Yes</td>
</tr>
<tr>
<td>SBC</td>
<td>No</td>
</tr>
<tr>
<td>SL-XLAT</td>
<td>No</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>Yes</td>
</tr>
<tr>
<td>STP/MSTP/PVST</td>
<td>Yes</td>
</tr>
<tr>
<td>SVI</td>
<td>No</td>
</tr>
<tr>
<td>SynCE</td>
<td>Yes</td>
</tr>
<tr>
<td>TDM</td>
<td>Yes</td>
</tr>
<tr>
<td>TDM PW</td>
<td>No</td>
</tr>
<tr>
<td>VC Switching</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN Bridging</td>
<td>Yes</td>
</tr>
<tr>
<td>VPLS</td>
<td>No</td>
</tr>
<tr>
<td>VRRP</td>
<td>No</td>
</tr>
<tr>
<td>VTP (VLAN Trunk and Tunneling)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. Currently this technology is supported only for XR 12K and ASR 1000
Table 19-4 identifies the schemes that are supported by device type.

**Table 19-4  Schemes Used by Device Type**

<table>
<thead>
<tr>
<th>Device Types</th>
<th>Scheme</th>
<th>Product</th>
<th>IpCore</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Appliances</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance 5550 Series</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td><strong>Application Networking Appliances</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco ACE 4700 Series Application Control Engine Appliances</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td><strong>Gateways</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco AS5300 Series Universal Gateways</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td><strong>Routers</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco 800 Series Routers</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Cisco 1000 Series Routers</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Cisco 1600 Series Routers</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Cisco 1700 Series Modular Access Routers</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Cisco 1800 Series Integrated Services Routers</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Cisco 2500 Series Routers</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Cisco 2600 Series Multiservice Platform Routers</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Cisco 2800 Series Integrated Services Routers</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Cisco 2900 Series Integrated Services Routers</td>
<td>X</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Cisco 3600 Series Multiservice Platform Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 3700 Series Multiservice Access Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 3800 Series Integrated Services Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 4700 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 7200 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 7300 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 7400 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 7500 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 7600 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 10000 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco 12000 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco XR 12000 Series Routers</td>
<td>X(^1)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco CRS Carrier Routing System (CRS-1 and CRS-3)</td>
<td>—</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 901 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 903 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 5000 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1000 Series Routers</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Choosing a VNE Scheme

Table 19-4  Schemes Used by Device Type (continued)

<table>
<thead>
<tr>
<th>Device Types</th>
<th>Scheme</th>
<th>IpCore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 9000 Series Aggregation Services Routers</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco MWR 2900 Series Mobile Wireless Routers</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Switches</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Nexus 1000v Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Catalyst 2900 Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco ME 3400 Series Ethernet Access Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Catalyst 3500 XL Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Catalyst 3550 Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Catalyst 3560 Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco ME 3600X Series Ethernet Access Switches</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco Catalyst 3750 Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Catalyst 3750 Metro Series Switches</td>
<td>—</td>
<td>X</td>
</tr>
<tr>
<td>Cisco ME 3800X Series Carrier Ethernet Switch Routers</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco Catalyst 4000 Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Catalyst 4500 Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Catalyst 4900 Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco ME 4900 Series Ethernet Switch</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Nexus 5000 Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Catalyst 6500 Series (CatOS) Switches</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco Catalyst 6500 Series (Cisco IOS) Switches</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco ME 6500 Series Ethernet Switches (6524)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco Nexus 7000 Series Switches</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco SCE 2000 Series Service Control Engine</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td><strong>Optical Networking</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Carrier Packet Transport (CPT) 50</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Carrier Packet Transport (CPT) 500</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Carrier Packet Transport (CPT) 600</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td><strong>Unified Computing and Servers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Computing System</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td><strong>Generic Devices</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generic devices</td>
<td>X</td>
<td>—</td>
</tr>
</tbody>
</table>

1. The product scheme is supported Cisco XR 12000 Gigabit Switch Routers.
Adding VNEs

You can add VNEs manually if desired, but Prime Network provides a variety of VNE auto-add features that will distribute VNEs between units and AVMs. The auto-add feature calculates in advance the predicated memory consumption of a VNE based on its role and type, and balances AVM memory as the VNEs are added. You can also monitor the VNEs as the auto-add feature creates them and distributes them across the system.

Methods for Adding VNEs

Prime Network can choose the best unit and AVM for a VNE. The general rule is that if you want Prime Network to decide where the VNE should go, start from the All Servers branch (that is, right-click All Servers and choose the operation).

Table 19-5 briefly describes the various methods and scenarios for which they are suitable. You can use a combination of methods at the same time. In all of these cases, you can let Prime Network choose the best unit and AVM, or you can specify them yourself.

<table>
<thead>
<tr>
<th>Method</th>
<th>Useful when:</th>
<th>For instructions, see:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clone an existing VNE</td>
<td>You want to create VNEs with most or all of the same properties as an existing VNE. (You can also modify the properties later.)</td>
<td>Cloning VNEs, page 19-14</td>
</tr>
<tr>
<td>Create a CSV file of properties and then use it to create VNEs</td>
<td>You want to create many VNEs with different properties, and the property information is stored in a CSV file.</td>
<td>Creating VNEs Using a CSV File, page 19-17</td>
</tr>
<tr>
<td>Create a VNE “from scratch” by going through all of the properties. VNE first.</td>
<td>You are adding a new device type or upgrading to a different VNE driver file, and you want to test it before deploying it.</td>
<td>Creating VNEs for New Device Types, page 19-21</td>
</tr>
<tr>
<td>Create VNEs based on existing devices using the Network Discovery feature</td>
<td>You want to create many VNEs based on existing devices in your network.</td>
<td>Creating VNEs Using the Network Discovery Feature, page 19-23</td>
</tr>
</tbody>
</table>

How VNE Auto-Add Works

When you use the VNE auto-add feature—that is, you create VNEs from the All Servers branch—Prime Network will choose the appropriate unit and AVM for the VNE. If you decide you want to choose your own AVM, you can still do that using auto-add because all available units and AVMs are displayed in a drop-down list. If you want the VNEs on a specific unit, right-click the unit to perform the operation, and Prime Network will choose the appropriate AVM. Prime Network does this by finding safe target AVMs. 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).

Note

If Prime Network is installed with Cisco Prime Central, be sure to use a device’s SYSNAME as its VNE name. This allows the device to be recognized across the common inventory. Also, do not use None or All as the SYSNAME, because those names have internal meaning to Cisco Prime Central.
Adding VNEs

• It is not experiencing any memory consumption problems.

When you finish defining the VNE properties, the VNEs are listed in the Queued VNEs tab (under All Servers). As the VNEs are assigned to AVMs, they disappear from that tab.

If Prime Network cannot locate an appropriate AVM is not identified, it waits 2 minutes, and attempts to find a suitable AVM again. It will continue retrying until an AVM is found.

Note that even when you use the auto-add feature, before the VNEs are created, you can choose a unit or AVM for a drop-down list in the VNE properties dialog.

Figure 19-2 illustrates the VNE auto-add process.

Figure 19-2  VNE Auto-Add

Before You Create VNEs

The following table provides a list of steps you should perform before adding a VNE.

Note

For troubleshooting help, see Troubleshooting VNE Modeling, page 20-1 and Device Reachability, page 24-1.


2. Gather all prerequisite information:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Device management IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Device name</td>
</tr>
</tbody>
</table>
### Adding VNEs

3. Perform all mandatory configurations on the network element so that it can be properly modeled and managed by Prime Network.

<table>
<thead>
<tr>
<th>For these settings:</th>
<th>See:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS, Cisco IOS XE, and CatOS devices</td>
<td>Cisco IOS, Cisco IOS XE, and CatOS Devices—Required Settings, page A-2</td>
</tr>
<tr>
<td>Cisco IOS XR devices</td>
<td>Cisco IOS XR Devices—Required and Recommended Settings, page A-3</td>
</tr>
<tr>
<td>Devices you will add using SSH</td>
<td>Cisco StarOS Devices—Required Settings, page A-5</td>
</tr>
<tr>
<td>SNMP traps setup</td>
<td>SNMP Traps and Informs—Required Device Settings, page A-8</td>
</tr>
<tr>
<td>Syslogs setup</td>
<td>Syslogs—Required Device Settings, page A-13</td>
</tr>
<tr>
<td>For configurations where the traps and syslogs source IP address is different from the VNE IP address</td>
<td>IP Address Configuration for Traps, Syslogs, and VNEs, page A-14</td>
</tr>
<tr>
<td>Nexus OS devices:</td>
<td>Cisco Carrier Packet Transport Devices, page A-15</td>
</tr>
</tbody>
</table>
4. (Optional) Get deployment information and recommendations, such as best practices for assigning VNEs to AVMs by contacting your Cisco representative.

**Cloning VNEs**

A clone VNE inherits all of the properties of an existing VNE. This includes cloning the Device Package being used by the existing VNE. You only have to specify a different name and IP address. Prime Network will choose the best unit and AVM for the VNE, but you can override this with your own choice. Once you have created the clone VNEs, you can still edit their properties before creating them.

**Before You Begin**

Make sure you have performed any necessary tasks that are described in Before You Create VNEs, page 19-12. This will ensure that the VNE is properly modeled and updated.

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose the appropriate launch point, depending on whether you want to use the auto-add feature:</td>
</tr>
<tr>
<td><strong>To create VNEs where:</strong></td>
<td><strong>Start the clone operation from this point in the GUI client:</strong></td>
</tr>
<tr>
<td>Prime Network chooses the unit and AVM</td>
<td>From All Servers in the navigation area, click All VNEs tab.</td>
</tr>
<tr>
<td>Prime Network chooses the AVM but you choose the unit</td>
<td>From desired unit in the navigation area, click Unit’s VNEs tab.</td>
</tr>
<tr>
<td>You choose the unit and AVM</td>
<td>From desired unit in the navigation area, click the desired AVM</td>
</tr>
</tbody>
</table>

**Step 2** | In the VNEs table, find the VNE type that you want to replicate. |

**Step 3** | Right-click the VNE you want to replicate and choose **Clone > Clone VNE** or **Clone > Clone Multiple VNEs**. |

In Figure 19-3, the user is creating several clone VNEs based on the VNE with the key 10.56.118.53. Because the action was performed while the All Servers branch is selected, Prime Network will choose the appropriate unit and AVM.
Step 4  Create the clone VNE(s).

a. In the Add VNEs from Clone dialog box, click the Add Cloned VNE icon (see Figure 19-4).

Figure 19-4  Creating a Clone VNE Using Auto-Add—Creating the Clones

A Clone VNE dialog box is displayed. It contains all of the properties of the target VNE except for the VNE name and IP address.

b. Enter the new VNE name and IP address. When finished, click OK.

Note  If Prime Network is installed with Cisco Prime Central, be sure to use a device’s SYSNAME as its VNE name. This allows the device to be recognized across the common inventory. Also, do not use None or All as the SYSNAME, because those names have internal meaning to Cisco Prime Central.

c. Repeat this step to create additional clones of the VNE. As you create more clones, they are added to the dialog box.
Step 5

To edit the VNE properties before creating the VNEs (for example, to specify a unit or AVM, use a different scheme, and so forth), right-click the VNE and select **Edit VNE** (see Figure 19-5). If you want, you can specify the unit and AVM you want the VNE to use.

![Image: Figure 19-5 Creating a Clone VNE Using Auto-Add—Viewing and Editing the Clones](image)

**Step 6**

Click **Finish**. To check the status of the VNEs:

a. For auto-added VNEs (the unit or AVM was selected by Prime Network), select **All Servers** branch and click the **Queued VNEs** tab. If it is empty, the VNEs have been assigned.

b. To find the VNE’s assignment, click the **All VNEs** tab and check the unit column.

c. Go to the unit and click the **Unit’s VNEs** tab to check the AVM.

*Figure 19-6* shows two new VNEs that were added to the gateway but are using AVM auto-assignment. Their assignment is pending.
Prime Network starts investigating the network element and builds a live model of the network element, including its physical and logical inventory, its configuration, and its status. Prime Network also creates the registry information of the new VNE in the unit. After a few minutes, verify that the VNE status is Up.

### Creating VNEs Using a CSV File

Using a CSV file to add VNEs is helpful when you have a large number of VNEs to create and you want to organize your customizations using a spreadsheet template. Prime Network will choose the unit and AVMs for the VNEs. The new VNEs will use the latest installed DP (the newest DP that is installed on the gateway or unit). If there are any errors, Prime Network will clearly display them. If any fields are left blank, Prime Network uses the defaults specified in Table 19-6.

#### Format of a CSV File

The CSV file supports all of the entry names listed in Table 19-6. A general guideline is that you should supply the following entries in your file, at a minimum:

```
elementName,ip,SNMPEnabled,SnmpVersionEnum,adminStatusEnum,SchemeName,avm,unitIP,ICMPPollingRate,ICMPEnabled,PollingGroup,TrapSyslogSources,TelnetSequence,telnetEnabled
```

The following is the text of a sample CSV file. This CSV file is also provided on the gateway server at `NETWORKHOME/Main/scripts/BulkVNEImportExample.csv`.

```
elementName,ip,SNMPEnabled,SnmpVersionEnum,adminStatusEnum,SchemeName,avm,unitIP,ICMPPollingRate,ICMPEnabled,PollingGroup,TrapSyslogSources,TelnetSequence,telnetEnabled
```

Adding VNEs

m1,1.1.1.1,TRUE,1,0,ipcore,,,50000000,TRUE,slow,,","prompt,#","TRUE
m2,1.1.1.2,TRUE,2,1,product,,,856000,FALSE,default,,#,TRUE
m3,1.1.1.3 ,TRUE,2,1,,,,","129.5.6.2,55.23.6.5,9.5.2.1","text,,",FALSE
m4,1.1.1.4,TRUE,1,0,,FALSE,,121.2.3.4,,TRUE
m5,1.1.1.5,TRUE ,1,0, ipcore ,,5600000,FALSE ,slow,121.2.3.4,,">,admin,#",FALSE

Table 19-6  Supported Values for CSV File (Creating VNEs)

<table>
<thead>
<tr>
<th>CSV Entry</th>
<th>Supported Values</th>
<th>Default Setting and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Properties</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>elementName</td>
<td>string or IP address</td>
<td>Mandatory field(^1)</td>
</tr>
<tr>
<td>Note</td>
<td>If Prime Network is installed with Cisco Prime Central, be sure to use a device’s SYSNAME as its VNE name. This allows the device to be recognized across the common inventory. Also, do not use None or All as the SYSNAME, because those names have internal meaning to Cisco Prime Central.</td>
<td></td>
</tr>
<tr>
<td>ip</td>
<td>vne IP address</td>
<td>Mandatory field</td>
</tr>
<tr>
<td>elementClassEnum</td>
<td>0=AuditDetect, 1=Generic SNMP, 2=Cloud, 3=ICMP</td>
<td>0 (AutoDetect)</td>
</tr>
<tr>
<td>SchemeName</td>
<td>default (=product), product, ipcore</td>
<td>product</td>
</tr>
<tr>
<td>adminStatusEnum</td>
<td>0=Disabled (do not start VNE), 1=Enabled (start VNE)</td>
<td>1 (start VNE)(^2)</td>
</tr>
<tr>
<td>avm</td>
<td>avm ID</td>
<td>(null) (Use auto-add)</td>
</tr>
<tr>
<td>unitIP</td>
<td>unit IP address</td>
<td>(null) (Use auto-add)</td>
</tr>
<tr>
<td><strong>SNMP Properties</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMPEnabled</td>
<td>TRUE=Enabled, FALSE=Disabled</td>
<td>TRUE</td>
</tr>
<tr>
<td>SnmpVersionEnum</td>
<td>0=SNMPv1, 1=SNMPv2, 2=SNMPv3</td>
<td>1 (SNMPv1)</td>
</tr>
<tr>
<td>SNMPReadCommunity</td>
<td>string</td>
<td>public</td>
</tr>
<tr>
<td>SNMPWriteCommunity</td>
<td>string</td>
<td>private</td>
</tr>
<tr>
<td>SnmpV3AuthenticationProfile</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>SnmpV3AuthenticationPassword</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>SnmpV3AuthenticationProtocolEnum</td>
<td>0=md5, 1=sha</td>
<td>(null)</td>
</tr>
<tr>
<td>SnmpV3EncryptionPassword</td>
<td>string</td>
<td>(null)</td>
</tr>
</tbody>
</table>
### Table 19-6  Supported Values for CSV File (Creating VNEs) (continued)

<table>
<thead>
<tr>
<th>CSV Entry</th>
<th>Supported Values</th>
<th>Default Setting and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnmpV3EncryptionTypeEnum</td>
<td>0=des, 1=aes128, 2=aes192, 3=aes256</td>
<td>(null)</td>
</tr>
</tbody>
</table>

#### Telnet/SSH Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>TelnetEnabled</td>
<td>TRUE=Enabled, FALSE=Disabled</td>
<td>FALSE</td>
</tr>
<tr>
<td>TelnetProtocolEnum</td>
<td>0=Telnet, 1=SSHv1, 2=SSHv2</td>
<td>0 (Telnet)</td>
</tr>
<tr>
<td>TelnetPortNumber</td>
<td>port-number</td>
<td>23 (Telnet), 22 (SSHv1/v2)</td>
</tr>
<tr>
<td>TelnetSequence</td>
<td><em>sequence</em></td>
<td>(null)</td>
</tr>
<tr>
<td>SshCipherEnum</td>
<td>0=DES, 1=3DES, 2=Blowfish</td>
<td>1 (3DES)</td>
</tr>
<tr>
<td>SshAuthenticationEnum</td>
<td>0=password</td>
<td>0 (password)</td>
</tr>
<tr>
<td>SshV1Username</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>SshV1Password</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>SshV2Username</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>SshV2Password</td>
<td>string</td>
<td>(null)</td>
</tr>
</tbody>
</table>

#### XML Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLPortNumber</td>
<td>port-number</td>
<td>38751 (Telnet), 52 (SSL)</td>
</tr>
<tr>
<td>XmlProtocolEnum</td>
<td>0=Telnet, 1=SSL</td>
<td>0 (Telnet)</td>
</tr>
<tr>
<td>XMLEnabled</td>
<td>TRUE=Enabled, FALSE=Disabled</td>
<td>FALSE</td>
</tr>
<tr>
<td>XMLSequence</td>
<td>string</td>
<td>(null)</td>
</tr>
</tbody>
</table>

#### HTTP Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPPortNumber</td>
<td>port-number</td>
<td>80</td>
</tr>
<tr>
<td>HttpProtocolEnum</td>
<td>0=HTTP, 1=HTTPS</td>
<td>0 (HTTP)</td>
</tr>
<tr>
<td>HTTPEnabled</td>
<td>TRUE=Enabled, FALSE=Disabled</td>
<td>FALSE</td>
</tr>
<tr>
<td>HTTPManagementPath</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>HTTPAuthenticationRequired</td>
<td>TRUE=Required, FALSE=Not required</td>
<td>FALSE</td>
</tr>
<tr>
<td>HTTPUserName</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>HTTPPassword</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>TL1Enabled</td>
<td>TRUE=Enabled, FALSE=Disabled</td>
<td>FALSE</td>
</tr>
<tr>
<td>TL1PortNumber</td>
<td>port-number</td>
<td>(null)</td>
</tr>
<tr>
<td>TL1Username</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>TL1Password</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>TL1PortNumber</td>
<td>port-number</td>
<td>(null)</td>
</tr>
<tr>
<td>ClientAuthEnum</td>
<td>0=password, 1=public</td>
<td>0 (password)</td>
</tr>
</tbody>
</table>
Adding VNEs

Before You Begin

Make sure you have performed any necessary tasks that are described in Before You Create VNEs, page 19-12. This will ensure that the VNE is properly modeled and updated.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select All Servers &gt; Add Multiple VNEs &gt; Using Default Values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Add Multiple VNEs dialog box:</td>
</tr>
<tr>
<td></td>
<td>a. Click the Import VNEs from File icon as shown in Figure 19-7.</td>
</tr>
</tbody>
</table>

### Table 19-6 Supported Values for CSV File (Creating VNEs) (continued)

<table>
<thead>
<tr>
<th>CSV Entry</th>
<th>Supported Values</th>
<th>Default Setting and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientPrivateKey</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>ServerAuthEnum</td>
<td>0=none, 1=save-first-auth, 2=preconfigured</td>
<td>2 (preconfigured)</td>
</tr>
<tr>
<td>ServerPublicKey</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>FingerPrint</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>ServerAuthDataTypeEnum</td>
<td>0=fingerprint, 1=public-key</td>
<td>0 (fingerprint)</td>
</tr>
<tr>
<td>KeyExchange</td>
<td>string</td>
<td>(null)</td>
</tr>
<tr>
<td>MAC</td>
<td>0=sha1, 1=md5, 2=sha1-96, 3=md5-96</td>
<td>(null)</td>
</tr>
<tr>
<td>Cipher</td>
<td>0-3DES, 1=AES-128, 2=AES-192, 3=AES-256</td>
<td>(null)</td>
</tr>
<tr>
<td>HostKeyAlgo</td>
<td>0=DSA, 1=RSA</td>
<td>(null)</td>
</tr>
<tr>
<td>IsActionNotAllowed</td>
<td>TRUE=Not allowed, FALSE=Allowed</td>
<td>(null)</td>
</tr>
</tbody>
</table>

### ICMP Properties

<table>
<thead>
<tr>
<th>ICMPEnable</th>
<th>TRUE=Enabled, FALSE=Disabled</th>
<th>FALSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMPPollingRate</td>
<td>number (milliseconds)</td>
<td>(null)</td>
</tr>
</tbody>
</table>

### Polling Properties

<table>
<thead>
<tr>
<th>PollingGroup</th>
<th>slow, default</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdaptivePollingSettingEnum</td>
<td>0=Prime Network Settings, 1=Device Type Settings, 2=Local Settings</td>
<td>1 (Device Type Settings)</td>
</tr>
</tbody>
</table>

### Events Properties

| TrapSyslogSources            | ~IP address[,IP address,...] | (null) |

1. For existing VNEs, you cannot overwrite the VNE name or IP address using a CSV file. To change a VNE name or IP address you must delete the existing VNE and create a new one.
2. If you use auto-add, the VNE will automatically be started regardless of this setting.
3. These settings are not used by VNEs provided with the initial release of Prime Network 3.8. Future Device Packages will introduce new device support for devices that will use this feature.

New VNEs are started automatically as described in the VNE Lifecycle section.
Adding VNEs

Figure 19-7 Creating VNEs from a CSV File—Selecting the CSV File

Step 3

To edit any VNE properties before creating the VNEs (for example, to specify a unit or AVM, use a different scheme, and so forth), right-click the VNE and select Edit VNE (see Figure 19-5).

Note

You can still add individual VNEs using the Clone VNE icon shown in Figure 19-4 on page 19-15.

Step 4

To check the status of the VNEs:

a. For auto-added VNEs (the unit or AVM was selected by Prime Network), select All Servers branch and click the Queued VNEs tab. If it is empty, the VNEs have been assigned.

b. To find the VNE’s assignment, click the All VNEs tab and check the unit column.

c. Go to the unit and click the Unit’s VNEs tab to check the AVM.

Prime Network starts investigating the network element and builds a live model of the network element, including its physical and logical inventory, its configuration, and its status. Prime Network also creates the registry information of the new VNE in the unit. After a few minutes, verify that the VNE status is Up.

Creating VNEs for New Device Types

When you create a VNE for a new device type, you should create a single VNE and test it to ensure its settings are correct. You can then clone it as described in Cloning VNEs, page 19-14.

Before You Begin

Make sure you have performed any necessary tasks that are described in Before You Create VNEs, page 19-12. This will ensure that the VNE is properly modeled and updated.

Step 1

Choose the appropriate launch point, depending on how much control you want over the unit and AVM:

<table>
<thead>
<tr>
<th>To create the VNE(s) where:</th>
<th>Start from this point in the GUI client:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Network chooses the unit and AVM</td>
<td>All Servers &gt; New VNE</td>
</tr>
<tr>
<td>Prime Network chooses the AVM but you choose the unit</td>
<td>Unit &gt; New VNE</td>
</tr>
<tr>
<td>You choose the unit and AVM</td>
<td>Unit &gt; AVM &gt; New VNE</td>
</tr>
</tbody>
</table>
Step 2  The New VNE dialog box is displayed, opened to the General tab. The following table lists the tabs in the VNE properties window and where you can get more information on the fields in those tabs.

<table>
<thead>
<tr>
<th>VNE Tab</th>
<th>Description</th>
<th>Described in:</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Enter general information such as VNE name, IP address, and scheme. By default, Prime Network uses the newest DP installed on the gateway or unit. If you are creating a single VNE, you can specify a different DP from the drop-down list. The VNE name and IP address are mandatory (Cloud VNEs do not require an IP address). <strong>Note</strong> If Prime Network is installed with Cisco Prime Central, be sure to use a device’s SYSNAME as its VNE name. This allows the device to be recognized across the common inventory.</td>
<td>VNE General Settings, page 19-29</td>
</tr>
<tr>
<td>SNMP</td>
<td>Specifies SNMP information and credentials to support polling and device reachability. The fields displayed in the dialog box depend on the protocol you select.</td>
<td>VNE SNMP Settings, page 19-31</td>
</tr>
<tr>
<td>Telnet/SSH</td>
<td>Enables Telnet and SSH for device reachability and investigation, including the Telnet sequence and SSH prompts. The fields displayed in the dialog box depend on the protocol you select.</td>
<td>VNE Telnet/SSH Settings, page 19-32</td>
</tr>
<tr>
<td>XML</td>
<td>Enables XML for device reachability and investigation.</td>
<td>VNE XML Settings, page 19-38</td>
</tr>
<tr>
<td>HTTP</td>
<td>Enables HTTP. <strong>Note</strong> These settings are not used by VNEs provided with the initial release of Prime Network 3.8. Future Device Packages will introduce new device support for devices that will use this feature.</td>
<td>VNE HTTP Settings, page 19-39</td>
</tr>
<tr>
<td>ICMP</td>
<td>Enables ICMP and the ICMP polling rate (in seconds) for device reachability testing.</td>
<td>VNE ICMP Settings, page 19-39</td>
</tr>
<tr>
<td>Polling</td>
<td>Associates a VNE with a previously created polling group or allows you to customize different polling settings according to the type of VNE information you want (status, configuration, and so forth); and lets you specify VNE adaptive polling.</td>
<td>VNE Polling Settings, page 19-40</td>
</tr>
<tr>
<td>Events</td>
<td>Specifies other IP addresses on which the VNE should listen for syslogs and traps. (This is useful when devices have components using IP addresses that are different from the management IP address, especially if the device driver cannot automatically detect these additional addresses.)</td>
<td>VNE Events Settings, page 19-42</td>
</tr>
</tbody>
</table>

Step 3  Click Finish. Check the status of the VNEs in the VNEs table. For auto-added VNEs:

a. Select All Servers branch and click the Queued VNEs tab. If it is empty, the VNEs have been assigned.

b. To find the VNE’s assignment, click the All VNEs tab and check the unit column.

c. Go to the unit and click the Unit’s VNEs tab to check the AVM.
Prime Network starts investigating the network element and builds a live model of the network element, including its physical and logical inventory, its configuration, and its status. Prime Network also creates the registry information of the new VNE in the unit. After a few minutes, verify that the VNE status is Up.

Creating VNEs Using the Network Discovery Feature

The network discovery tool allows administrator and configurator users to automatically discover the devices that exist in the network, and then to create a virtual Network Element (VNE) for each discovered device to be managed with Prime Network. Use of the network discovery tool significantly speeds up the process of importing your devices into Prime Network so that they can be managed.

Network discovery is supported on the following device operating systems: IOS, IOS-XR, IOS-XE, NX-OS, CATOS, JUNOS.

Before You Begin

Make sure of the following:

- You have performed any necessary tasks that are described in Before You Create VNEs, page 19-12. This will ensure that the VNE is properly modeled and updated.
- The gateway running the discovery process must be able to reach the target devices using the management protocols (SNMP and Telnet/SSH).

The Network Discovery workflow is as follows:

**Step 1**
Access the Network Discovery tool, as follows:
Choose **Tools > Network Discovery** in Cisco Prime Network Administration.

or

Enter the following URL in your web browser:
https://gateway_IP_address:8043/prime-network-web/index.html#pageId=discovery_settings_page

**Step 2**
Create a discovery profile. The profile includes all the discovery settings that will determine how the system locates, identifies, and communicates with the devices in the network. To do this, click **New** in the Discovery Profiles page. Your discovery profile is saved with a unique name so that it can be reused at a later stage. See Discovery Profiles, page 19-24 for details.

**Step 3**
Start the network discovery by selecting the discovery profile and clicking **Run**.

**Step 4**
View the results of the network discovery, which indicate which devices were discovered and whether or not further credential information is required before creating VNEs. To do this, choose **Network Discovery > Discovery Results**. See Network Discovery Results, page 19-26 for details.

**Step 5**
Select the devices you want to manage with Prime Network and create VNEs for these devices.

**Step 6**
Monitor the status of the VNE creation in the Discovery Results tab or in Prime Network Administration.
Discovery Profiles

Before starting the network discovery process, you need to provide information that will allow the system to locate and discover the devices in your network and then to create a VNE for each discovered device. Your discovery settings are saved in a discovery profile. This discovery profile can be reused at a later stage so that you do not need to define new settings each time you perform network discovery.

When creating a discovery profile, you first specify the technique(s) to be used to discover the network. The most common discovery technique is Ping Sweep, which pings all the IP addresses in a specified subnet. You can choose a different discovery technique based on protocol data, depending on the protocols used in your network.

After specifying the discovery technique(s), you provide information that is required to create VNEs for the discovered devices, including the credentials that will be needed to connect to the devices, and the method the system should use to identify the management IP address.

Lastly, you have the option to define filters to include/exclude specific devices from the network discovery results. For example, you might have a subset of devices in the specified subnet that you do not want to manage, so you could filter these out of the results.

Table 7 lists the parameters to be defined before initiating the discovery process.

Table 7  Discovery Profile Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the discovery profile.</td>
</tr>
<tr>
<td>Discovery Technique</td>
<td>The discovery technique to be used to discover the devices in the network. The most commonly used technique is Ping Sweep. Click on Techniques Based on Protocol Data to see the other discovery techniques. To select a discovery technique, click the plus icon next to the technique, check the Enable check box, and then enter the required information. You have the following options:</td>
</tr>
<tr>
<td>Ping Sweep—Enter the starting IP address and subnet mask to specify a range of IP addresses. The system will ping all the IP addresses in this range and will discover the devices from which it receives a reply.</td>
<td></td>
</tr>
<tr>
<td>Protocol Data Techniques (CDP, Router, Address Resolution, Border Gateway or OSPF)— Specify the seed device IP address and the number of hops away from the seed device the system should look for devices to discover.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
You can specify multiple techniques in order to locate and discover the largest number of devices.

**Note**
When both BGP and OSPF are specified in the same discovery profile, the seed devices specified for each protocol will be combined for each protocol. For example, if you specify 192.0.2.1 as a seed device for BGP and 192.0.2.2 as a seed device for OSPF, you will see both 192.0.2.1 and 192.0.2.2 listed for both BGP and OSPF when you edit the profile. To avoid this, you can create separate discovery profiles – one using BGP and one using OSPF for discovery.
Credential Settings
Specifies the pool of credentials that the system can use to communicate with the devices during the VNE creation process. At minimum, you must specify SNMP v2/v3 credentials and Telnet/SSH credentials. The system will define a device as “Reachable” if the device is accessible using the defined credentials.

Management IP Selection Method
This setting tells Prime Network how to identify which of the device’s IP addresses should be used as the management IP address:

- Discovered IP—The IP address used to discover the device.
- Loopback—The priority for selecting the IP address if Prime Network uses this as selection method is:
  - Highest IP address of a loopback interface
  - Highest IP address of an Ethernet interface
  - Highest IP address of a Token Ring interface
  - Highest IP address of a Serial Interface
- System Name—Prime Network performs a DNS lookup on the system name specified and verifies the validity of the IP address of the device. On successful validation, the verified IP address becomes the preferred management IP address for this device. If validation was not successful, the original IP address used to discover the device will be the management IP address.
- DNS Reverse Lookup—Prime Network performs a reverse DNS lookup followed by a forward lookup on the IP address specified and verifies the validity of the IP address of the network element. On successful validation, the verified IP address becomes the preferred management IP address for this network element, otherwise the original address will be used.

Filters
(Optional) Enables you to filter the results that are displayed for the discovery. The filters include:

- System Location—Filter by physical/geographic location of the device (as specified in the SYSTEM-MIB). If your network devices are configured with the system location, you can use this filter option.
- IP—Filter by IP address.
- System Object ID—Filter by device type (as specified in the SYSTEM-MIB).
- DNS Filter—Filter by domain name. The system resolves the name of the device from the DNS server and filters the results.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Settings</td>
<td>Specifies the pool of credentials that the system can use to communicate with the devices during the VNE creation process. At minimum, you must specify SNMP v2/v3 credentials and Telnet/SSH credentials. The system will define a device as “Reachable” if the device is accessible using the defined credentials.</td>
</tr>
<tr>
<td>Management IP Selection Method</td>
<td>This setting tells Prime Network how to identify which of the device’s IP addresses should be used as the management IP address:</td>
</tr>
<tr>
<td>Filters</td>
<td>(Optional) Enables you to filter the results that are displayed for the discovery. The filters include:</td>
</tr>
<tr>
<td>System Location</td>
<td>Filter by physical/geographic location of the device (as specified in the SYSTEM-MIB). If your network devices are configured with the system location, you can use this filter option.</td>
</tr>
<tr>
<td>IP</td>
<td>Filter by IP address.</td>
</tr>
<tr>
<td>System Object ID</td>
<td>Filter by device type (as specified in the SYSTEM-MIB).</td>
</tr>
<tr>
<td>DNS Filter</td>
<td>Filter by domain name. The system resolves the name of the device from the DNS server and filters the results.</td>
</tr>
</tbody>
</table>
Network Discovery Results

The Network Discovery Results tab enables you to view the status and the results of the network discovery process. The table in the upper half of the Discovery Results tab lists all the network discovery jobs and provides summary information for each one. Select a network discovery job in the table to display full details of the network discovery results in the lower half of the page.

If a device is discovered in the network and deemed reachable, a VNE can be created for that device so that it can be managed in Prime Network. If a device has credential errors, you can change the credentials and run the discovery again. Alternatively, you can create that VNE manually in Prime Network Administration.

After VNEs are created for the discovered devices, the system automatically assigns them to AVMs.

Discovery Jobs

Each time network discovery is initiated, a job is created. The Network Discovery Results table lists the discovery jobs and provides information and status for each one, as described in Table 8.

To see the latest status, please click the Refresh button to refresh the display.

Table 8 Network Discovery Results Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name provided by the system for the discovery job, derived from the discovery profile name plus a unique ID.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the executed discovery. The status can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Completed</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Stopped</td>
</tr>
<tr>
<td></td>
<td>• Aborted</td>
</tr>
<tr>
<td>Note</td>
<td>Icons next to the Name field provide an at-a-glance view of the discovery job status. See Table 9.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Start time of the network discovery job.</td>
</tr>
<tr>
<td>End Time</td>
<td>End time of the network discovery job.</td>
</tr>
<tr>
<td>Discovery Profile</td>
<td>Name of the discovery profile in which the discovery settings were defined.</td>
</tr>
<tr>
<td>Reachable</td>
<td>The number of discovered devices that are reachable and manageable using the specified credentials.</td>
</tr>
<tr>
<td>Filtered</td>
<td>The number of devices that were filtered from the discovery results.</td>
</tr>
<tr>
<td>Credential Error</td>
<td>The number of devices that were identified in the network but cannot be managed using the specified credentials.</td>
</tr>
</tbody>
</table>

The status of the network discovery is reflected in the icons displayed next to the job name, as described in Table 9.
Adding VNEs

Detailed Discovery Results

The detailed results are displayed in three tabs in the bottom half of the Discovery Results page:

- **Reachable**—Lists the devices detected in the network that can be reached and are available for management by Prime Network. For each device, you have the option to change the polling approach and/or the scheme before creating the VNE for that device.

To start the VNE creation process, select the required device(s) and click **Create VNEs**. You can monitor the status in the Status column:

- **Found**—The device has been discovered.
- **In Progress**—VNE creation process has started.
- **Queued**—VNE has been created but has not yet been assigned to an AVM. These VNEs are listed in Prime Network Administration in the Queued VNEs tab under All Servers.
- **Naming Conflict**—A VNE with the same name already exists in the system.
- **IP Conflict**—A VNE with the same IP address already exists in the system.
- **Assigned**—The VNE has been created and assigned to an AVM.

- **Credential Errors**—Lists the devices detected in the network for which additional credential information is required before VNEs can be created.
- **Filtered**—Lists the devices that were filtered out of the discovery results.

### Table 9  Discovery Job Status Icon Reference

<table>
<thead>
<tr>
<th>Status</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running</td>
<td>✔️</td>
<td>The job is running and there are no credential errors.</td>
</tr>
<tr>
<td></td>
<td>🟢</td>
<td>The job is running and there are credential errors.</td>
</tr>
<tr>
<td>Completed</td>
<td>✔️</td>
<td>The job is completed and there are no credential errors.</td>
</tr>
<tr>
<td></td>
<td>🟢</td>
<td>The job is completed and there are credential errors.</td>
</tr>
<tr>
<td>Stopped</td>
<td>🟢</td>
<td>The job is stopped.</td>
</tr>
<tr>
<td>Aborted</td>
<td>✖️</td>
<td>The job is aborted.</td>
</tr>
</tbody>
</table>
Viewing and Editing VNE Properties

Prime Network Administration enables you to view and edit the properties of a VNE in a unit, such as the status or Telnet settings. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

**Note**
For troubleshooting help, see Troubleshooting VNE Modeling, page 20-1 and Device Reachability, page 24-1.

To view the properties of a VNE:

**Step 1** Expand the All Servers branch, then select the required AVM in the navigation tree.

**Step 2** Open the VNE Properties dialog box by right-clicking the required VNE in the VNE Properties table, then choose **Properties**.

<table>
<thead>
<tr>
<th>VNE Tab</th>
<th>Description</th>
<th>Described in:</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Contains general information such as VNE name, IP address, scheme, and VNE driver file and version being used by the VNE. To change the driver a VNE is using, see Changing the Device Package a VNE Is Using, page 21-4.</td>
<td>VNE General Settings, page 19-29</td>
</tr>
<tr>
<td>SNMP</td>
<td>Specifies SNMP settings to support polling and device reachability.</td>
<td>VNE SNMP Settings, page 19-31</td>
</tr>
<tr>
<td>Telnet/SSH</td>
<td>Enables Telnet and SSH for device reachability and investigation.</td>
<td>VNE Telnet/SSH Settings, page 19-32</td>
</tr>
<tr>
<td>XML</td>
<td>Enables XML for device reachability and investigation.</td>
<td>VNE XML Settings, page 19-38</td>
</tr>
<tr>
<td>HTTP</td>
<td>Enables HTTP. <strong>Note</strong> These settings are not used by VNEs provided with the initial release of Prime Network 3.8. Future Device Packages will introduce new device support for devices that will use this feature.</td>
<td>VNE HTTP Settings, page 19-39</td>
</tr>
<tr>
<td>ICMP</td>
<td>Enables ICMP and the ICMP polling rate for device reachability testing.</td>
<td>VNE ICMP Settings, page 19-39</td>
</tr>
<tr>
<td>Polling</td>
<td>Associates a VNE with a previously created polling group or allows you to customize different polling settings according to the type of VNE information you want (status, configuration, and so forth); and lets you specify VNE adaptive polling.</td>
<td>VNE Polling Settings, page 19-40</td>
</tr>
<tr>
<td>Events</td>
<td>Specifies other IP addresses on which the VNE should listen for syslogs and traps.</td>
<td>VNE Events Settings, page 19-42</td>
</tr>
</tbody>
</table>

To edit VNE properties, see Editing VNE Properties, page 19-43.
### VNE General Settings

To view a VNE’s General properties, right-click the VNE in the Servers drawer and select **Properties**. By default it opens to the General tab. **Table 19-10** describes the fields in the VNE General properties dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification Area</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the VNE, which will be used as a unique key in Prime Network. It is also used for commands that manipulate the VNE.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If Prime Network is installed with Cisco Prime Central, be sure to use a device’s SYSNAME as its VNE name. This allows the device to be recognized across the common inventory. You cannot change a VNE name once you have created the VNE. To change the name you must delete and add a new VNE.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Device management IP address of the network element.</td>
</tr>
<tr>
<td>Type</td>
<td>Defines the protocol Prime Network will use to model the element, and the extent to which you want the element to be modeled. In the drop-down list, choose the VNE device type:</td>
</tr>
<tr>
<td></td>
<td>- Auto Detect—Use this type if SNMP is enabled on the element. Prime Network will use SNMP to gather all available inventory information.</td>
</tr>
<tr>
<td></td>
<td>- Generic SNMP—Use this type if SNMP is enabled on the element, and either Prime Network does not support the element, or Prime Network does support the element but you only want basic information to be modeled. Prime Network will use SNMP to gather the most basic inventory information that is normally provided by all network elements. See Notes on Generic SNMP VNEs, page 19-30.</td>
</tr>
<tr>
<td></td>
<td>- Cloud—Use this type for an unmanaged network segment. Specific Cloud configuration is provided on a per-project basis. All other tabs will be disabled. See Unmanaged Segments and Cloud VNEs, page 23-1.</td>
</tr>
<tr>
<td></td>
<td>- ICMP—Use this type if ICMP is enabled on the element, and either Prime Network does not support the element, or Prime Network does support the element but you only want basic information to be modeled. Prime Network will use ICMP to gather the most basic inventory information that is normally provided by all network elements, and will perform reachability testing only. ICMP VNEs can connect to other VNEs using static links. If you want to connect ICMP VNEs using physical links, you must configure the ICMP VNE’s MAC address, as described in Notes on ICMP VNEs, page 19-39.</td>
</tr>
<tr>
<td>Scheme</td>
<td>Defines the VNE modeling components investigated during the discovery process and then populated in the VNE model. This enables the administrator to define different behavior for some network elements; for example, some network elements poll only with SNMP, and other network elements poll with Telnet. Soft properties and activation scripts are also attached to a specific scheme. By default, the VNE inherits the VNE scheme from the default scheme. Where more than one scheme exists in the network, the VNE loads the selected scheme.</td>
</tr>
<tr>
<td></td>
<td>- Default—Sets the scheme to Product.</td>
</tr>
<tr>
<td></td>
<td>- Product—This scheme is used for all device types in this release, except for Cisco CRS and Cisco 3750ME devices.</td>
</tr>
<tr>
<td></td>
<td>- IpCore—This scheme is used only for routers serving as Provider (P) or Provider Edge (PE) devices. For more information, see Choosing a VNE Scheme, page 19-5.</td>
</tr>
</tbody>
</table>
Notes on Generic SNMP VNEs

The generic SNMP VNE is a VNE that is not related to any vendor, can represent any vendor (with certain limitations), and provides lightweight management support for network devices. A generic SNMP VNE does the following:

- Provides basic management capabilities for a device with the following technologies:
  - IP (restricted to basic IP only; does not include modeling of IPsec, MPLS, or routing protocols)
  - Ethernet switching
  - 802.1q
- Supports these inventory items:
  - Physical inventory (specific port types only)
  - Routing table
  - ARP table
  - Default bridge
  - IP interfaces
- Supports these topologies:
  - Physical Layer Connectivity

### Table 19-10 Fields in the VNE General Tab (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial State Area</strong></td>
<td></td>
</tr>
</tbody>
</table>
| State               | Sets the initial disposition of the VNE. Normally you should set it to Stop, especially if you want to verify the VNE configuration, or if you know the VNE is very complex and might need extra processing to complete the loading procedure. **Note** If you use auto-add, the VNE will automatically be started.  
  - Stop—The VNE is not loaded. This is the default state.  
  - Start—The VNE is loaded and starts collecting data.  
  To move an existing VNE to the maintenance state, see Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-44. |
| **VNE Location**    |
| Unit                | IP address of the unit that hosts the AVM for the VNE.                      |
| AVM                 | AVM ID associated with this VNE.                                           |
| **VNE Driver Details** |
| Version             | (Existing VNEs only) Version of the VNE device driver being used.           |
| Device Package Name | For existing VNEs, this is the 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. See How to Find Out if New Support is Available, page 21-2.  
  For new VNEs, this is a drop-down list that displays all available Device Packages. By default, the VNE uses the latest DP that is installed on the gateway or unit. After creating the VNE, you can update it to use new driver files as described in Changing the Device Package a VNE Is Using, page 21-4. |
| Driver File Name    | (Existing VNEs only) Name of the VNE device driver being used (this driver corresponds to the DP that is listed). |
MAC-based ethernet topologies

If a VNE is identified as unsupported (because its type was not recognized), Prime Network gives the VNE a status of Unsupported. You can either leave the VNE as Unsupported or load it as a Generic SNMP VNE.

Every VNE in agentdefaults/da has the entry “load generic agent for unsupported device type,” where you can set the value as true or false (the default). If the value is true, it sets 1.3.999.3 as the property. It looks for this property in agentdefaults/da/deviceTypes and finds sheer/genericda. It then skips the investigation of the device software versions and builds the VNE (generic SNMP) from the default version.

VNE SNMP Settings

To view a VNE’s SNMP settings, right-click the VNE in the Servers drawer and select Properties, and click the SNMP tab. Table 19-11 describes the fields in the VNE SNMP properties dialog box.

<table>
<thead>
<tr>
<th>Table 19-11</th>
<th>Fields in the VNE SNMP Tab</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>SNMP Version Area</td>
<td></td>
</tr>
<tr>
<td>Enable SNMP</td>
<td>If checked, enables the SNMP communication protocol so that the user can work with it. A VNE can have SNMP enabled or disabled at any time; however, when the Auto Detect check box is checked (in the General tab), it cannot be disabled.</td>
</tr>
<tr>
<td>SNMP V1/V2 Settings (activated using SNMP V1 or SNMP V2)</td>
<td>\begin{itemize} \item Read: SNMP read community status, public (default) or private, as defined by the user. \item Write: (Optional) SNMP write community status, public or private (default), as defined by the user. \end{itemize}</td>
</tr>
<tr>
<td>SNMP V3 Settings (activated if using SNMP V3)</td>
<td>\begin{itemize} \item Authentication: Type of authentication to be used: \begin{itemize} \item No—Authentication is not required (default). \item md5—Uses Message Digest 5 (MD5) for the authentication mechanism. \item sha—Uses Secure Hash Algorithm (SHA) for the authentication mechanism. \end{itemize} \item User: Authentication username. \item Password: Authentication password. This field is enabled if you choose md5 or sha. \end{itemize}</td>
</tr>
<tr>
<td>Encryption</td>
<td>Type of encryption method to be used. These choices are disabled if you choose No authentication. \begin{itemize} \item No—Encryption is not required (default). \item des—Uses Data Encryption Standard (DES) for encryption. \item aes128—Uses 128-bit Advanced Encryption Standard (AES) for authentication. \item aes192—Uses 192-bit AES for authentication. \item aes256—Uses 256-bit AES for authentication. \end{itemize} \item Password: Encryption password. This field is enabled if you choose des, aes128, aes192, or aes256 encryption.</td>
</tr>
</tbody>
</table>
VNE Telnet/SSH Settings

To view a VNE’s Telnet/SSH settings, right-click the VNE in the Servers drawer and select Properties, and click the Telnet/SSH tab.

You can find out if a VNE is using Telnet or SSH (along with the specific version) by opening the device properties window and click VNE Status. The VNE Status Details window provides details about the protocols. (You can open the device properties window from both Prime Network Administration (right-click the VNE and choose Inventory) and Prime Network Vision (right-click the device and choose Inventory.)

Table 19-12 describes the fields in the VNE Telnet/SSH properties dialog box.

For examples of how to enter Telnet or SSH prompt information, see Telnet and SSH Login Sequences: Notes and Examples, page 19-35. For more information on SSHv2 host key algorithms, also see Notes on SSHv2 Public Key and Private Key File Formats, page 19-37.

Table 19-12  Fields in the VNE Telnet/SSH Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables the communication protocol so Prime Network will investigate the network element. Checking this check box activates the other fields in this tab.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Type of protocol to be used: Telnet (default), SSHv1, or SSHv2. <strong>Note</strong> By default, when a VNE opens a Telnet session with a network element in order to model and monitor the element, the Telnet session remains open for 5 minutes, even if the VNE is idle (did not query the device during the session). After 5 minutes, the VNE closes the session and reopens it when it needs to query the device. If you would like to change this configuration, contact your Cisco account representative.</td>
</tr>
</tbody>
</table>
| Port    | Port the protocol will use. This field is prepopulated depending on your protocol choice. If you are not using the default port, enter the appropriate port number.  
  - 23—Default port for Telnet.  
  - 22—Default port for SSHv1 or SSHv2. |
### Table 19-12 Fields in the VNE Telnet/SSH Tab (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prompt and Run</td>
<td>The network element’s expected prompt, and the string Prime Network should send to the network element (when the expected prompt is detected). The table shows the current settings; you can change the settings using the controls below the table. Entering a string in the Prompt field activates the Run field. After making your entries in the Prompt and Run fields, check <strong>Mask</strong> if you do not want the password entered as clear text. Finally, click <strong>Add</strong> to add them to the login sequence. Click <strong>Remove</strong> to remove any lines. Use the up and down controls to the right of the table to change the order. <strong>Note</strong> After an SSH session is established between the VNE and the device, the VNE starts the login sequence. This sequence is usually shorter than the corresponding Telnet login sequence, as the username or password might have been sent as a step in establishing the SSH session (see the example in Telnet and SSH Login Sequences: Notes and Examples, page 19-35).</td>
</tr>
<tr>
<td>If you selected Telnet:</td>
<td>Telnet prompt information. The sequence (the order of the commands) must end with a line that includes only the prompt field. Prime Network VNEs can handle partial device prompts as well. For examples, see Telnet and SSH Login Sequences: Notes and Examples, page 19-35. The Prompt field should contain the prompt expected from the device; the Run field should contain the response to the expected prompt. When entering the Run information, you must confirm the entry in the Confirm field. The values in Run and Confirm are displayed as clear text if you have not checked the Hide the Run value while typing check box.</td>
</tr>
<tr>
<td>If you selected SSH V1 or V2:</td>
<td>SSH prompt information. This sequence is usually shorter than the corresponding Telnet login sequence, because the username or password may already be sent during the process of establishing the SSH session. We recommend that you first use any SSH client application (such as UNIX SSH or OpenSSH) to determine the device SSH login sequence, and then enter that information.</td>
</tr>
<tr>
<td>Mask</td>
<td>Masks the password so it is not displayed as clear text in the Run and Confirm fields.</td>
</tr>
<tr>
<td>Add and Remove</td>
<td>Used to manipulate the order of the prompt and run strings.</td>
</tr>
</tbody>
</table>

**SSHv1 Area (activated if using SSHv1)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Device name.</td>
</tr>
<tr>
<td>Password</td>
<td>Device password.</td>
</tr>
<tr>
<td>Cipher</td>
<td>Encryption algorithm to be used. By default, all methods are used.</td>
</tr>
<tr>
<td></td>
<td>• DES—Use the Data Encryption Standard algorithms.</td>
</tr>
<tr>
<td></td>
<td>• 3DES—Use the Triple Data Encryption Standard algorithm.</td>
</tr>
<tr>
<td></td>
<td>• Blowfish—Use the blowfish algorithms.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication method; currently password is the only supported method.</td>
</tr>
</tbody>
</table>
### Table 19-12 Fields in the VNE Telnet/SSH Tab (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSHv2 Area (activated if using SSHv2)</td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td>SSHv2 username.</td>
</tr>
<tr>
<td>Client Authentication</td>
<td>Client-driven authentication method to be used.</td>
</tr>
<tr>
<td>password</td>
<td>Use a password to authenticate the client. Enter the password in the Password field.</td>
</tr>
</tbody>
</table>
| public-key                 | Optionally, use public key authentication, which uses a key pair system in which the client application is configured with the secret private key, and the device is configured with the public (non-secret) key (of this pair). To create a pair of keys:  
1. In the Private Key field, click ... to import the private key from a file. You cannot manually enter they key, but you can edit a key that you import from file. If you change it to the wrong key, you will see an error message.  
2. In the Public Key area, generate the public key in any of the following ways:  
   - Click ... to import the public key from a file.  
   - Manually enter a public key.  
   - Click Generate to autogenerated a public key. |
| Server Authentication      | Server authentication method to be used.                                   |
| none                       | No server authentication. (This method does not do any authentication and is not recommended, because it poses a security risk for “man-in-the-middle” attacks.) |
| save-first-auth            | Uses the public key that was used for the first connection attempt with the server. This method assumes the first connection was legitimate. (A security risk exists if the connection was compromised.) After the first connection, the server authentication method is changed to preconfigured, and the public key data is inserted as the preconfigured data. |
| preconfigured              | Uses the server public key or fingerprint that was configured in the application event before the first connection was attempted. This is the default and is the recommended method. Selecting this method activates the Finger Print or Public Key field.  
Select one of the following (and be sure to read the description, provided later in this table, of the Host Key Algorithm field):  
   - Finger Print—Uses a short checksum of the server public key (this serves the same purpose, but is much shorter).  
   - Public Key—Uses the public key in one of the permitted formats (see Notes on SSHv2 Public Key and Private Key File Formats, page 19-37). Click ... to import the public key from a file. |

By default, the SSHv2 Key, MAC, ciphers, and host key algorithms\(^1\) are allowed (enabled):  
- Key exchange: DH-group1-sha1, DH-group1-exchange-sha1  
- MAC algorithm: SHA1, MD5, SHA1-96, MD5-96  
- Ciphers: 3DES, AES-128, AES-192, AES-256, Blowfish, Arcfour  
- Host Key Algorithm: DSA, RSA

For information on how to change these settings, see Device Communication Security: SSH and SNMPv3, page 13-4.

---

\(^1\) You can select multiple algorithms by pressing Ctrl while choosing a method. If more than one is selected, the application will try to use all of the algorithms until one is accepted by the server. There is no priority in the way the algorithms are tried.
When you add a VNE, Prime Network uses the specified communication protocol to connect to the network element and gather modeling and status information. You must provide the information Prime Network will need: the characters and order of the network element’s expected prompts, and the string Prime Network should send to the network element in response (so that you can get to enable mode for Cisco IOS and Cisco IOS XE devices, and XML mode for Cisco IOS XR devices).

**Note**
VNEs can understand partial and complete device prompts.

After an SSH session is established between the VNE and the device, the VNE starts the SSH login sequence. This sequence is usually shorter than the corresponding Telnet login sequence.

This topic provides two examples (with complete procedures) that show how to enter Telnet sequences:
- Telnet Login Sequence for a Cisco IOS Device: Example, page 19-35
- Telnet Sequence for a Cisco IOS XR Device: Example, page 19-36

A Telnet sequence (the order of the commands) must end with a line that includes only the enable prompt (for Cisco IOS and Cisco IOS XE devices) or the router CLI prompt (for Cisco IOS XR devices). Not all device families will have the same Telnet sequence; this is especially true for Cisco IOS devices. For RAD ACE-2300 devices, because SNMP is used for device modeling, we recommend disabling Telnet to avoid unnecessary queries.

**Telnet Login Sequence for a Cisco IOS Device: Example**

This sample procedure describes how you could enter a Telnet sequence for a hypothetical Cisco IOS device or Cisco IOS XE device.

**Step 1**
Check the **Enable** check box to activate the Telnet prompt fields.

**Step 2**
Enter the expected device prompt and response:

**Note**
To verify a device’s Telnet sequence, open a Telnet session to the device and copy the information. The following is an example.

a. Enter **Password:** in the Prompt field.

**Note**
If you do not want the password displayed in clear text, check **Mask**.

b. Enter **Rivers39** in the Run field.

c. Click **Add**.

**Step 3**
Enter the device prompt and the command required to place the device in enable mode:

a. Enter **R3745** in the Prompt field.

b. Enter **enable** in the Run field.

c. Click **Add**.
Step 4  Enter the enable mode password information:
   a. Enter **Password:** in the Prompt field.

   ![Note]
   If you do not want the password displayed in clear text, check **Mask**.

   b. Enter `!Tribal41_` in the Run field.

   c. Click **Add**.

Step 5  Enter the enable prompt information:
   a. Enter `R3745#` in the Prompt field.

   ![Note]
   VNEs can also understand partial prompts. For example, if you enter the string `#` instead of `R3745#`, the VNE will still be able to recognize the expected prompt.

   Leave the Run field blank.

   b. Click **Add**.

---

**Telnet Sequence for a Cisco IOS XR Device: Example**

This sample procedure describes how you could enter a Telnet sequence for a hypothetical Cisco IOS XR device.

Step 1  Check the **Enable** check box to activate the Telnet prompt fields.

Step 2  Enter the expected device prompt and response:

   ![Note]
   To verify a device’s Telnet sequence, open a Telnet session to the device and copy the information. The following is an example.

   a. Enter **Username:** in the Prompt field.

   b. Enter `crs1-oak` in the Run field.

   c. Click **Add**.

Step 3  Enter the device password information:

   ![Note]
   Enter **Password:** in the Prompt field.

   ![Note]
   If you do not want the password displayed in clear text, check **Mask**.

   d. Enter `sunFlower108!` in the Run field.

   e. Click **Add**.
Step 4 Enter the device prompt:

a. Enter EC-A# in the Prompt field.

Note For devices with multiple processors (such as Cisco CRS), the prompt comprises the active CPU plus the device name (for example, RP/0/RSP0/CPU0:EC-A#). A CPU failover could change the prompt and report a different CPU. In these cases, you should insert a prompt that specifies only the device name (for example, EC-A#). (Also, as with Cisco IOS, VNEs can also understand partial prompts. For example, if you enter the string # instead of EC-A#, the VNE will still be able to recognize the expected prompt.)

Leave the Run field blank.

b. Click Add.

Notes on SSHv2 Public Key and Private Key File Formats

There are several file formats for public and private RSA and DSA keys. The same key can be written differently according to the format that is used.

This application officially supports the openSSH format. For more details, see http://www.openssh.com/manual.html.

Make sure that the keys you provide as input parameters are in this format. If they are not, you need to convert them to the open SSH format before applying them.

Use Case Example: When working with Cisco IOS, the public key is retrieved using the show crypto key mypubkey command. This format is not compatible with the OpenSSH format, and is not supported. There are several ways to convert the format.

The easiest solution is to use public key scan by the (free) openSSH application to retrieve the public key in the supported format. For more details, see http://www.openssh.com/manual.html.

Another option is to convert the files to the required format either manually or by using a script.

The following are examples of valid file formats.

RSA - private key
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDvdpW8ItfbSp/hTbWZJqCPmjRyh9S+EpTV0Aq3fnGpFPTR+
........
TiOfhiuX5+M1cTaE/lf8sScj6jE9AOHpShBrnDU/0A==
-----END RSA PRIVATE KEY-----

DSA private key
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQDNGo+l2XW+W+YtVnKSYbKXr6qkJH9nOl+
........
7wO4+FR9af0RjDusrQrL
-----END DSA PRIVATE KEY-----

DSA public key
ssh-dss AAAAB3...HfuNYu+ DdGY7njEYrN++iWs= aslehr@aslehr-wxp01

RSA - public key
ssh-rsa AAAAB3...lot more_qc8Hc= aslehr@aslehr-wxp01
VNE XML Settings

To view a VNE’s XML properties, right-click the VNE in the Servers drawer and select Properties and click the XML tab. XML is used by some devices such as those that use Cisco IOS XR. Table 19-13 describes the fields in the VNE XML properties dialog box.

Table 19-13 Fields in the VNE XML Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables the XML communication protocol so Prime Network will investigate the network element. Checking this check box activates the other fields in this tab.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Type of protocol to be used: Telnet (default) or SSL. Note: By default, when a VNE opens a Telnet session with a network element in order to model and monitor the element, the Telnet session remains open for 5 minutes, even if the VNE is idle (did not query the device during the session). After 5 minutes, the VNE closes the session and reopens it when it needs to query the device. If you would like to change this configuration, contact your Cisco account representative.</td>
</tr>
</tbody>
</table>
| Port          | Port the protocol will use. This field is prepopulated depending on your protocol choice. If you are not using the default port, enter the appropriate port number.  
  - 38751—Default port for Telnet.  
  - 38752—Default port for SSL. |
| Prompt and Run| The network element’s expected Telnet or SSL prompt, and the string Prime Network should send to the network element (when the expected prompt is detected). The table shows the current settings; you can change the settings using the controls below the table. Entering a string in the Prompt field activates the Run field. After making your entries in the Prompt and Run fields, check Mask if you do not want the password entered as clear text. Finally, click Add to add them to the login sequence. Click Remove to remove any lines. Use the up and down controls to the right of the table to change the order. Note: After an SSH session is established between the VNE and the device, the VNE starts the login sequence. This sequence is usually shorter than the corresponding Telnet login sequence, as the username or password might have been sent as a step in establishing the SSH session (see the example in Telnet and SSH Login Sequences: Notes and Examples, page 19-35).  
The sequence (the order of the commands) must end with a line that includes only the prompt field. The Prompt field should contain the prompt expected from the device; the Run field should contain the response to the expected prompt. When entering the Run information, you must confirm the entry in the Confirm field. The values in Run and Confirm are displayed as clear text if you have not checked the Hide the Run value while typing check box. |
| Mask          | Masks the password so it is not displayed as clear text in the Run and Confirm fields. |
| Add and Remove| Used to manipulate the order of the prompt and run strings. |
VNE HTTP Settings

To view a VNE’s HTTP settings, right-click the VNE in the Servers drawer and select Properties, and click the HTTP tab.

*Note*
These settings are not used by VNEs provided with the initial release of Prime Network 3.8. Future Device Packages will introduce new device support for devices that will use this feature.

Table 19-14 describes the fields in the VNE HTTP properties dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables the HTTP communication protocol so Prime Network will investigate the network element. Checking this check box activates the other fields in this tab.</td>
</tr>
<tr>
<td>Enable HTTPS</td>
<td>Enables the secure HTTP communication protocol.</td>
</tr>
<tr>
<td>Port</td>
<td>Port the protocol will use. By default, HTTP uses port 80.</td>
</tr>
<tr>
<td>Management Path</td>
<td>HTTP URL to use to connect the device.</td>
</tr>
<tr>
<td>Use Authentication</td>
<td>Enables requiring credentials for HTTP to log in to the device.</td>
</tr>
</tbody>
</table>

VNE ICMP Settings

To view a VNE’s ICMP settings, right-click the VNE in the Servers drawer and select Properties, and click the ICMP tab. Table 19-15 describes the fields in the VNE ICMP properties dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Instructs Prime Network to use the ICMP communication protocol to verify that the network element is reachable. You can enable or disable ICMP polling at any time by checking or unchecking the check box (except for ICMP type VNEs, which require this setting to be enabled).</td>
</tr>
<tr>
<td>Polling Rate</td>
<td>Polling rate in seconds. If ICMP is enabled, this is a required field.</td>
</tr>
</tbody>
</table>

Notes on ICMP VNEs

ICMP VNEs are used to test the reachability to a device. For ICMP VNEs, Prime Network does not poll the device to create a physical and logical inventory. But to connect the ICMP VNE to another VNE and visualize a link on the map, the ICMP VNE must have a port in its physical inventory. Therefore, when Prime Network creates an ICMP VNE, it creates a physical inventory model that contains only an Ethernet port.

You can use static links to connect ICMP VNEs to other VNEs.

Prime Network will autodiscover physical links between the ICMP VNE and other VNEs if the following conditions are met:
- The real MAC address of the port is configured for the ICMP VNE.
- The port on the ICMP VNE is a routed port and terminates the Layer 2 domain.
To specify a MAC address for an ICMP VNE, use the following procedure.

**Step 1** Log into the gateway as *network user* and change to the Main directory by entering the following command. (*network user* is the operating system account for the Prime Network application, created when Prime Network is installed; for example, *network39*.)

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

**Step 2** Configure the MAC address for the VNE. For the gateway, *unit-IP* should be 0.0.0.0. For units, the *unit-IP* should be the unit’s IP address.

```
# ./runRegTool.sh -gs gateway-IP set unit-IP site/sheericmp/base/product/software versions/default version/spec/dcs/com.sheer.metrocentral.coretech.common.equipment.dc.Chassis/ethMacAddress mac-address
```

**Step 3** Restart the VNE.

---

### VNE Polling Settings

To view a VNE’s Polling settings, right-click the VNE in the Servers drawer and select **Properties**, and click the Polling tab. This tab is disabled if you chose ICMP as the VNE type (in the General tab). In addition to controlling the intervals at which a network element is polled, this dialog box specifies the adaptive polling settings, which specify how a VNE should respond to high device CPU usage.

**Note** If you want to apply polling settings at a global level (rather than per VNE), create a polling group that can then be applied across VNEs. See **VNE Polling Groups and Slow Polling**, page 22-23.

Table 19-16 describes the fields in the VNE Polling properties dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Method</td>
<td></td>
</tr>
<tr>
<td>Polling approach for model updates</td>
<td>Specifies whether to use normal or reduced polling. The reduced polling mechanism polls a device only when a configuration change syslog is received (which results in less polling overall). You can verify whether a device supports reduced polling by clicking the <strong>Supported on selected devices only</strong> link. By default, reduced polling is disabled and devices are polled according to the standard methods. For more information see <strong>Reduced Polling</strong>, page 22-2.</td>
</tr>
<tr>
<td>Prime Network default for device type</td>
<td>Use the dependency level that is the default for this device type.</td>
</tr>
<tr>
<td>Reduced polling (event-based)*</td>
<td>Poll the device when an event is received from the device. This results in less overall device polls.</td>
</tr>
<tr>
<td>Regular polling</td>
<td>Do not poll the device when an event is received from the device; instead use the normal polling mechanisms. This results in more device polls, overall.</td>
</tr>
</tbody>
</table>
Polling Parameters

Group  Use polling rates from one of the polling groups listed in the drop-down list. This allows you to apply polling rates more globally, to devices of similar type. By default, Prime Network uses Group (not Instance), and the polling group named default (which is provided out-of-the-box).

**Note** You can create new polling groups that will appear in the drop-down list by using the procedure in VNE Polling Groups and Slow Polling, page 22-23.

Instance  Uses a user-specified polling rate created by changing the polling rates of any one of the built-in polling intervals displayed in the dialog box. When you select Instance, the Polling Intervals and Topology areas are activated. These settings are applied to only this VNE.

**Note** A polling rate that is not changed inherits its settings from the group specified in the drop-down list.

Polling Intervals Area (activated if using Instance)

**Note** We recommend that you use the default settings for these polling intervals. Setting the fields below the default values can result in an overload of the Prime Network unit or polled device.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Polling rate for status-related information, such as network element status (up or down), port status, administrative status, and so on. This is typically the most frequently polled information, reflecting the current operational and administrative state of the element and its components. The default setting is 180 seconds.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Polling rate for configuration-related information, such as VC tables, scrambling, and so on. These reflect more dynamic element configuration such as forwarding, routing, and switching tables. The default setting is 900 seconds.</td>
</tr>
<tr>
<td>System</td>
<td>Polling rate for system-related information, such as network element name, network element location, and so on. These reflect element configurations that are less dynamic in nature. The default setting is 86400 seconds.</td>
</tr>
</tbody>
</table>

Topology Area (activated if using Instance)

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 1</td>
<td>Polling rate of the topology process as an interval for the Layer 1 counter. This is an ongoing process. The default setting is 90 seconds.</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Polling rate of the topology process as an interval for the Layer 2 counter. This process is available on demand. The default setting is 30 seconds.</td>
</tr>
</tbody>
</table>
Chapter 19  VNE Administration: VNE Lifecycle and Creating VNEs

Viewing and Editing VNE Properties

Table 19-16  Fields in the VNE Polling Tab (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Network</td>
<td>Uses the default settings for controlling VNE adaptive polling (see Adaptive</td>
</tr>
<tr>
<td>Settings</td>
<td>Polling, page 22-15).</td>
</tr>
<tr>
<td>Device Type</td>
<td>(Default) Uses the VNE adaptive polling settings specified for this device</td>
</tr>
<tr>
<td>Settings</td>
<td>type (as delivered with Prime Network). If no setting exists for the device</td>
</tr>
<tr>
<td></td>
<td>type, the Prime Network Settings are used.</td>
</tr>
<tr>
<td>Local Settings</td>
<td>Overrides the default settings and uses the values specified in the Upper</td>
</tr>
<tr>
<td></td>
<td>and Lower Threshold fields. Any values you specify here are used only for</td>
</tr>
<tr>
<td></td>
<td>this VNE instance.</td>
</tr>
<tr>
<td></td>
<td>• To enter your own adaptive polling settings, click Local Settings and enter</td>
</tr>
<tr>
<td></td>
<td>the thresholds. The changes are not applied until you check the Enable</td>
</tr>
<tr>
<td></td>
<td>check box.</td>
</tr>
<tr>
<td></td>
<td>• To turn off adaptive polling for the VNE, click Local Settings and uncheck</td>
</tr>
<tr>
<td></td>
<td>the Enable check box.</td>
</tr>
<tr>
<td>Upper Threshold</td>
<td>When CPU usage exceeds this value, the adaptive polling mechanism is triggered.</td>
</tr>
<tr>
<td></td>
<td>(See Figure 22-6 on page 22-16.)</td>
</tr>
<tr>
<td>Lower Threshold</td>
<td>When CPU usage drops below this value, the VNE moves to normal polling and</td>
</tr>
<tr>
<td></td>
<td>related alarms are cleared.</td>
</tr>
</tbody>
</table>

VNE Events Settings

For troubleshooting help, see Troubleshooting VNE Modeling, page 20-1 and Device Reachability, page 24-1. Also make sure you performed all necessary device configuration tasks in Before You Create VNEs, page 19-12.

To view a VNE’s Event settings, right-click the VNE in the Servers drawer and select Properties, and click the Events tab. These settings allow you to configure the VNE to listen to additional IP addresses. Existing addresses that are being listened to are listed on the right; you can enter a new address on the left. This is useful when devices have components using IP addresses that are different from the management IP address, especially if the device driver cannot automatically detect these additional addresses.

For example, traps and syslogs maybe dropped if any of the VNEs managed by Prime Network are configured in such a way that the following addresses are different:

• The traps and syslogs source IP address
• The VNE IP address (entered when the VNE was created and displayed in the VNE properties)

To avoid missing any traps or syslogs, configure the VNE to receive traps and syslogs using both IP addresses. For Cisco IOS XR devices, if the device has a configured virtual IP address and the VNE was added using that address, the device can receive the traps and syslogs through the virtual IP address. You do not need to configure the source for the SNMP traps and syslogs. For more information, see Recommended and Optional SNMP Settings for Cisco IOS XR Devices, page A-11.

Table 19-17 describes the fields in the VNE Events properties dialog box.
Viewing and Editing VNE Properties

After entering the address and clicking Add, the new IP address is listed under Event-Generating IP Addresses. When the VNE is saved, it will begin listening for events at the new IP address.

Editing VNE Properties

You can edit all VNE settings except for the scheme. When you change the settings, you must restart the VNE for your changes to take effect. You must have Administrator privileges (user access role) to use this function in Prime Network Administration.

To update the VNE to use a newer Device Package, right-click the VNE and select Update VNE Driver Package.

For troubleshooting help, see Troubleshooting VNE Modeling, page 20-1 and Device Reachability, page 24-1. Also make sure you performed all necessary device configuration tasks in Before You Create VNEs, page 19-12.

You cannot change the name of a VNE. You must delete the VNE and create a new one.

Note

For deployment information and recommendations, such as best practices for assigning VNEs to AVMs, contact your Cisco account representative.

To edit a VNE:

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

Step 2 Open the VNE Properties dialog box by right-clicking the required VNE in the VNE Properties table, then choose Properties.

Step 3 Edit or view the properties as required. Information that is dimmed cannot be edited. The settings that are available for editing depend on the VNE type. (For example, for Cloud VNEs, you can only edit General settings; for ICMP type VNEs, you cannot edit Polling settings.) If a field is dimmed, meaning you cannot edit it, to change the setting you must delete and recreate the VNE.

Step 4 Details about the fields in the VNE properties tabs are described in these topics:

- VNE General Settings, page 19-29
- VNE SNMP Settings, page 19-31
- VNE Telnet/SSH Settings, page 19-32
- VNE ICMP Settings, page 19-39
- VNE Polling Settings, page 19-40
- VNE Events Settings, page 19-42
Step 5 After making your required changes, click **Apply** and **OK**. The VNE properties are updated with your entries.

Step 6 Stop and restart the VNE as described in Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-44.

---

### Changing VNE Status and Lifecycle (Start, Stop, Maintenance)

You can use the Prime Network Administration GUI to start or stop a VNE, or move a VNE to maintenance mode. When you change the status of a VNE, the VNE persistency information is retained. Persistency information is data that is stored for later use. (For information on the VNE persistency mechanism, see Persistency Overview, page 26-1.)

Restarting a VNE also reinitiates the discovery process. If you want to rediscover only a certain element within a device, go to the Prime Network Vision GUI client, open the device inventory, and right-click the element and choose **Poll Now**.

To change a VNE’s status, select the VNE and choose one of the following from the right-click **Actions** menu.

- **Start**—Starts the VNE process and triggers its discovery process. The VNE will move through a status of Starting Up to Up. When the VNE is Up, its process is running and it is reachable.

- **Stop**—Stops the VNE process. The VNE will move through a status of Shutting Down to Down. In the GUI, the Maintenance indicator in the AVMs window will display **false**. (If you stop a VNE that was in maintenance mode, its Maintenance indicator will change to **false**. This is also true if the VNE is moved, if its parent AVM is moved or stopped, if the gateway is restarted, or if it is on a unit that is switched to a standby unit.)

- **Maintenance**—Stops some VNE functionality so that you can perform maintenance operations without affecting the overall functionality of the active network. This is useful during planned outages such as software upgrades, hardware modifications, or cold reboots. For more details about what a VNE in the maintenance state does or does not do, see Table 19-2 on page 19-5.

You do not need to restart a VNE after a device is upgraded. The VNE will gather the new information at its next scheduled poll. However, if you change VNE software, you must restart the VNE for your changes to take effect; see VNE Updates, page 21-1.

The following table shows the badge used to indicate that a VNE is in maintenance mode.

<table>
<thead>
<tr>
<th>Badge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="maintenance_badge" /></td>
<td>Indicates that a VNE is in maintenance mode in Prime Network Vision (and when pressed in a toolbar, moves a VNE to maintenance mode). In Prime Network Administration, the AVMs window will show the VNE Maintenance indicator as <strong>true</strong>.</td>
</tr>
</tbody>
</table>

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To change the state of a VNE or move it to maintenance mode:

- **Step 1** Expand the All Servers branch, and select the required AVM in the navigation tree.

- **Step 2** Select the required VNE in the VNEs Properties table.
### Step 3
Perform one of the following actions:

- To start the VNE, right-click **Actions > Start**, or click **Start** in the toolbar. A confirmation message is displayed. Click **OK**. An Up status is eventually displayed in the VNEs Properties table. You might see a Starting Up status if the gateway is overloaded or if the VNE is still being loaded. If the AVM hosting the VNE is in a Down status, the VNE status remains Starting Up until the VNE is brought up.

- To stop the VNE, right-click **Actions > Stop**, or click **Stop** in the toolbar. A confirmation message is displayed. Click **OK**. A Down status is eventually displayed in the VNEs Properties table. You might see a Shutting Down status while processes are shutting down.

- To place the VNE in maintenance mode, right-click **Actions > Maintenance**, or click **Maintenance** in the toolbar. A confirmation message is displayed. Click **OK**. A Maintenance status is displayed in the VNEs Properties table.

---

### Controlling Concurrent VNE Telnet Logins (Staggering VNEs)

The VNE staggering mechanism controls the rate at which VNEs initiate Telnet/SSH connections across a network managed by Prime Network. This prevents degraded performance on TACACS servers, which can result when there are many concurrent connections.

The mechanism is implemented across the following Prime Network components:

- A gateway service that controls whether VNEs on the unit are permitted to initiate Telnet login sequences. It does this by controlling the number of concurrent connections, and distributing those connections based on how AVMs and VNEs are allocated. The service runs on AVM 99 on the gateway server and units. If there are multiple unit servers, it runs in a distributed fashion across all units. The service ensures that the requests are distributed (it does not specifically monitor the TACACS server).

- A VNE service that requests login permission from its unit server’s management service.

- A Telnet protocol service that requests authorization before initiating a login sequence with a device (Telnet and SSH login requests).

When the gateway receives a Telnet authorization request, it queues the requests in a FIFO (first in, first out) manner. If the gateway denies the request, the VNE communication state is changed to Device Partially Managed and a System event is generated (discovery can be prolonged if the VNE is not granted permission). In addition, the VNE Status Details window is updated to say the gateway denied the service. The VNE will continue to request the login, and once a connection is permitted, the VNE communication state changes accordingly and a clearing System event is generated.

### Enabling the VNE Staggering Mechanism

This service is disabled by default; in other words, all VNEs are allowed to initiate login sequences. To enable it, use the following procedure:

### Step 1
Log into the gateway as **network user** and change to the Main directory by entering the following command. (**network user** is the operating system account for the Prime Network application, created when Prime Network is installed; for example, **network39**.)

```
# cd $ANAHOME/Main
```
Step 2  Configure the VNE service. You should perform this procedure on the gateway machine.

a. Start the service on all VNEs in a unit.
   
   ```
   # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
   site/mcm/services/agentbootstrap/VLAA/enable true
   ```

b. Configure the protocol to request authorization before initiating a login:
   
   ```
   # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
   site/agentdefaults/da/ip_default/protocols/telnet/authorizedlogin true
   ```

c. Restart the AVMs on the unit.

Step 3  Configure the gateway service. You should perform this procedure on the gateway machine.

a. Configure the parameters that control the connections.
   
   - Specify the number of permitted concurrent logins:
     
     ```
     # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
     avm99/services/vneLoginSupervisor/allowedConcurrentLoginsNum logins
     ```
     
     We recommend an initial concurrent login setting of 1000:
     
     ```
     # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
     avm99/services/vneLoginSupervisor/allowedConcurrentLoginsNum 1000
     ```

   - Specify the amount of time allotted for the VNE to successfully log in. If exceeded, the login is disallowed. (This allows the next VNE in the queue to proceed with its login.)
     
     ```
     # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
     avm99/services/vneLoginSupervisor/vneFinishedLoginTimeout milliseconds
     ```
     
     We recommend an initial setting of 5000 milliseconds (5 seconds):
     
     ```
     # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
     avm99/services/vneLoginSupervisor/vneFinishedLoginTimeout 5000
     ```

b. Start the gateway service
   
   ```
   # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
   avm99/services/initlevel5/vneLoginSupervisor
   com.sheer.system.os.services.vne.login.VneLoginSupervisorServiceImpl
   ```

c. Restart AVM 99 on all units.
   
   ```
   # runall.csh networkctl -avm 99 restart
   ```

Disabling the VNE Staggering Mechanism

To disable it, use the following procedure:

Step 1  Log into the gateway as network user and change to the Main directory by entering the following command. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

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

Step 2  Configure the VNE service. You should perform this procedure on the gateway machine.

a. Stop the service on all VNEs in a unit.

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/mcvm/services/agentbootstrap/VLAA/enable false

b. Configure the protocol to request authorization before initiating a login:

# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/agentdefaults/da/ip_default/protocols/telnet/authorizedlogin false

c. Restart the AVMs on the unit.

Step 3

Configure the gateway service. You should perform this procedure on the gateway machine.

a. Stop the gateway service

# ./runRegTool.sh -gs 127.0.0.1 unset 0.0.0.0
avm99/services/initlevel5/vneLoginSupervisor
com.sheer.system.os.services.vne.login.VneLoginSupervisorServiceImpl

b. Restart AVM 99 on all units.

# runall.csh networkctl -avm 99 restart
Troubleshooting VNE Modeling

These topics provide procedures to help you troubleshoot VNE modeling problems.

- Troubleshooting VNE Communication State Issues, page 20-1
- Troubleshooting VNE Investigation State (Discovery) Issues, page 20-14
- Opening a Bug Report, page 20-24

Additional VNE administration tasks are described in:

- Basic AVM and VNE Administration Tasks, page 4-1
- VNE Administration: VNE Lifecycle and Creating VNEs, page 19-1
- VNE Updates, page 21-1

Troubleshooting VNE Communication State Issues

These topics help you understand what determines a VNE’s communication state and how to troubleshoot a problematic state.

- What Determines the VNE Communication State (Device Reachability)?, page 20-1, describes agent and management communication, and how together their state determines the overall communication state of a VNE.
- Steps to Troubleshoot VNE Communication State Issues, page 20-3, describes what to do if a VNE is in an unexpected communication state. Troubleshooting for investigation states is provided in Troubleshooting VNE Investigation State (Discovery) Issues, page 20-14.

What Determines the VNE Communication State (Device Reachability)?

Figure 20-1 illustrate the two aspects that determine a VNE’s communication state: agent communication, which describes reachability between the Prime Network gateway server and the VNEs, and management communication, which describes the reachability between a Prime Network VNE and the network device it is modeling. Both must function in order for Prime Network to properly model and manage a device.
Chapter 20      Troubleshooting VNE Modeling

Troubleshooting VNE Communication State Issues

Management communication is the more challenging domain because it is far more common for devices to become unreachable than for a VNE to go down. There can be many scenarios: perhaps only the Telnet protocol is down but everything else is fine; or all protocols are down but the device is still “alive” (sending syslogs and traps); or all protocols down, and the device is not even generating traps or syslogs. To provide the most accurate reachability status, Prime Network does the following:

- Tracks protocol health by performing reachability tests that are tailored to the different types of protocols.
- Provides different management communication policies that you can choose, depending on how more or less strictly you want to track protocol health.
- Allows you to fine-tune both of the above to fit the needs of your network.
- Provides detailed information for troubleshooting purposes.

For details about how Prime Network does all of the above, see Device Reachability, page 24-1.

The most common management problem is when Prime Network reports that a VNE communication state is Device Partially Reachable because at least one protocol is not operational (this is the default behavior for protocol reporting and can be changed; see VNE Management Communication Policies and How To Change Them, page 24-1).

Table 20-2 provides information about the fields in the VNE Status Details window, and suggestions for troubleshooting steps based on the information you see.

See Device Reachability, page 24-1, for more information on management communication policies, including the following:

- How to change management communication policies
- How Prime Network determines protocol reachability
- How to customize protocol reachability testing
- How to troubleshooting SSH and Telnet connectivity issues
Steps to Troubleshoot VNE Communication State Issues

The following steps provide an overall procedure for responding to an unexpected VNE communication state.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>See:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify the current VNE communication (and investigation) states in Prime Network Vision.</td>
<td>Step 1: Check the Communication State, page 20-3</td>
</tr>
<tr>
<td>2</td>
<td>Check the VNE Status Details window to find out if any protocols are failing and why; and check the management communication policy that is being used. (These policies determine when a VNE is moved to Device Partially Reachable, and they allow you to decide how more or less strictly you want to track protocol health.) You can optionally check the System event to see if it can provide any new information.</td>
<td>Step 2: Check the VNE Status Details Window for Protocol and Connectivity Information, page 20-6</td>
</tr>
<tr>
<td>3</td>
<td>Test the protocol connectivity.</td>
<td>Step 3: Troubleshoot the Connectivity Issue, page 20-12</td>
</tr>
</tbody>
</table>

Prime Network uses a variety of protocols to determine device reachability as described in How Prime Network Determines Protocol Reachability, page 24-3. Probably the most common communication problem is when the VNE communication state changes to Device Partially Reachable, which normally indicates that at least one protocol is experiencing a problem. On the other hand, it could mean the VNE was stopped or moved to maintenance mode.

Step 1: Check the Communication State

Step 1

From the Prime Network Vision map view, double-click the icon in which you are interested. This opens the device properties window.

Note

You can also launch the device properties window from Prime Network Administration by right-clicking the VNE and choosing Inventory.
Step 2  Check the current Communication State (as shown in Figure 20-2).

Figure 20-2  VNE Communication State (in Prime Network Vision)

The 📁 icon indicates a network element has been deleted (or moved). Check Table 20-1 for an explanation of the state and how to proceed.
# Table 20-1  VNE Communication States and Troubleshooting Tips

<table>
<thead>
<tr>
<th>State Name</th>
<th>Description</th>
<th>Badge</th>
</tr>
</thead>
</table>
| Agent Not Loaded      | The VNE is not responding to the gateway because it was stopped, or it was just created. This communication state is the equivalent of the Defined Not Started investigation state. To troubleshoot a VNE in this state, check the VNE, AVM, and unit status using Prime Network Administration. Although a System event is generated whenever the communication state changes, when a VNE is started, an event is generated only after:  
- All protocols have been tested and a new problem is found (one that was not previously reported).  
- A problem that was found has been resolved.  
- If the VNE was stopped, you will see a message and a refresh button at the top of the properties window. If the VNE was restarted, refreshing the window will repopulate the information. However, if the VNE is still down, refreshing the window will result in an error message. To start the VNE, see Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-44. | None     |
| VNE/Agent Unreachable | The VNE is not responding to the gateway. This can happen if the unit or AVM is overutilized, the connection between the gateway and unit or AVM was lost, or the VNE is not responding in a timely fashion. (A VNE in this state does not mean the device is down; it might still be processing network traffic.) To troubleshoot a VNE in this state:  
1. Check the VNE, AVM, and unit status using Prime Network Administration and check the amount of available memory.  
2. Use the diagnostics tool to check memory usage, GC, and CPU usage; see Obtaining Diagnostic Information Using Graphs, page 9-6.  
3. Examine the AVM to see if a specific VNE is causing the problem. See VNE or AVM reachability issues are often due to CPU-related resource problems.                                                                                   |          |
| Connecting            | The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state. Because the investigation state decorator (the hourglass) will already be displayed, a special GUI decorator is not required.                                                                 | None     |
| Device Partially Reachable | The element is not fully reachable because at least one protocol is not operational. To troubleshoot this state, continue to Step 2: Check the VNE Status Details Window for Protocol and Connectivity Information, page 20-6.  
**Note**  
This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see VNE Management Communication Policies and How To Change Them, page 24-1. |          |
| Device Reachable      | All element protocols are enabled and connected.  
**Note**  
This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see VNE Management Communication Policies and How To Change Them, page 24-1. | None     |
Troubleshooting VNE Modeling

Chapter 20

Troubleshooting VNE Communication State Issues

Step 1

From the VNE properties window (see Figure 20-2 on page 20-4), click VNE Status at the bottom of the properties window to open the VNE Status Details window. Figure 20-3 shows an example of this window. In this case, the VNE is fully functional.

For an example of a VNE with communication problems, see Figure 20-4 on page 20-11.

Table 20-1 VNE Communication States and Troubleshooting Tips (continued)

<table>
<thead>
<tr>
<th>State Name</th>
<th>Description</th>
<th>Badge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Unreachable</td>
<td>The connection between the VNE and the device id down because all of the enabled protocols are down (though the device might be sending traps or syslogs). To troubleshoot this state, continue to Step 2: Check the VNE Status Details Window for Protocol and Connectivity Information, page 20-6.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see VNE Management Communication Policies and How To Change Them, page 24-1.</td>
<td></td>
</tr>
<tr>
<td>Tracking Disabled</td>
<td>The reachability detection process is not enabled for any of the protocols used by the VNE (specifically, the trackreachability registry key is not set to true; see Customizing Protocol Reachability Testing, page 24-7). The VNE will not perform reachability tests nor will Cisco Prime Network generate reachability-related events. In some cases this is desirable; for example, tracking for Cloud VNEs should be disabled because Cloud VNEs represent unmanaged network segments. Because this is a user-defined mode (rather than an error or transitional mode), Cisco Prime Network does not display a decorator for this state. To troubleshoot this state, continue to Step 2: Check the VNE Status Details Window for Protocol and Connectivity Information, page 20-6.</td>
<td>None</td>
</tr>
</tbody>
</table>
Figure 20-3  Information Provided by the VNE Status Details Window

Table 20-2 provides a description of the fields in the window.

Table 20-2  VNE Communication State Information (from VNE Status Details Window)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management State</td>
<td>The current investigation state, which pertains to device modeling (not communication). For an explanation of the Investigation State, Description, and Reduced Polling fields, see Table 20-4 on page 20-21.</td>
</tr>
<tr>
<td>Since</td>
<td>Timestamp of when the management state fields were last updated.</td>
</tr>
</tbody>
</table>
### Table 20-2  VNE Communication State Information (from VNE Status Details Window) (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication State Policy</td>
<td>Policy being used by Prime Network to determine device reachability and when to change the communication state to Device Unreachable.</td>
</tr>
<tr>
<td><strong>notstrict</strong></td>
<td>Change state to Device Unreachable when:</td>
</tr>
<tr>
<td></td>
<td>• All of the enabled protocols are down, and</td>
</tr>
<tr>
<td></td>
<td>• No traps or syslogs were sent by the device for the past 6 minutes.</td>
</tr>
<tr>
<td></td>
<td>Change state to Device Partially Reachable when:</td>
</tr>
<tr>
<td></td>
<td>• All of the enabled protocols are down.</td>
</tr>
<tr>
<td></td>
<td>• Traps or syslogs are being sent by device.</td>
</tr>
<tr>
<td><strong>ensure-management</strong></td>
<td>Change state to Device Unreachable when:</td>
</tr>
<tr>
<td></td>
<td>• All of the enabled protocols are down.</td>
</tr>
<tr>
<td></td>
<td>The status of traps/syslogs is not considered. This is the default policy.</td>
</tr>
<tr>
<td><strong>strict</strong></td>
<td>Change state to Device Unreachable when:</td>
</tr>
<tr>
<td></td>
<td>• At least one of the enabled protocols are down.</td>
</tr>
<tr>
<td></td>
<td>The status of traps/syslogs is not considered. (Because the state goes directly to Device Unreachable, you will never see the Device Partially Reachable communication state when using this policy.)</td>
</tr>
</tbody>
</table>

### Protocol Connectivity

<table>
<thead>
<tr>
<th>State</th>
<th>Functional state of the protocol (see the State Description for more details):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Operational</td>
</tr>
<tr>
<td></td>
<td>• Protocol Partially Functional</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
<tr>
<td></td>
<td>• Unknown (protocol is disabled)</td>
</tr>
</tbody>
</table>
Table 20-2  VNE Communication State Information (from VNE Status Details Window) (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Description</td>
<td>Details about the protocol state. Though problems can be due to a variety of issues, the following messages are grouped together by likely cause.</td>
</tr>
<tr>
<td></td>
<td>• Improper configuration of the VNE or the device. These can normally be solved by verifying that the VNE is using the proper credentials to connect to the device. If that does not solve the problem, proceed to Step 3: Troubleshoot the Connectivity Issue, page 20-12.</td>
</tr>
<tr>
<td></td>
<td>• Protocol failed to login</td>
</tr>
<tr>
<td></td>
<td>• Protocol failed to get first prompt</td>
</tr>
<tr>
<td></td>
<td>• Protocol failed to login when sending leading CR</td>
</tr>
<tr>
<td></td>
<td>• Protocol failed to get expected prompt</td>
</tr>
<tr>
<td></td>
<td>• Protocol failed to initiate login</td>
</tr>
<tr>
<td></td>
<td>• Protocol login authorization refused</td>
</tr>
<tr>
<td></td>
<td>• Protocol login authorization timeout</td>
</tr>
<tr>
<td></td>
<td>• Authentication failed</td>
</tr>
<tr>
<td></td>
<td>• Connectivity issues. Troubleshooting steps for this kind of problem are provided in Step 3: Troubleshoot the Connectivity Issue, page 20-12.</td>
</tr>
<tr>
<td></td>
<td>• Protocol failed to handle connection</td>
</tr>
<tr>
<td></td>
<td>• Protocol failed to connect to host</td>
</tr>
<tr>
<td></td>
<td>• Problem trying to ping host</td>
</tr>
<tr>
<td></td>
<td>• Destination host unreachable</td>
</tr>
<tr>
<td></td>
<td>• A specific command failed (note that the other commands may have successfully completed).</td>
</tr>
<tr>
<td></td>
<td>• Protocol failed to send command</td>
</tr>
<tr>
<td></td>
<td>• Protocol says: Command authorization failed</td>
</tr>
<tr>
<td></td>
<td>• Command execution exception</td>
</tr>
<tr>
<td>State Since</td>
<td>Timestamp of when the protocol information was last updated.</td>
</tr>
<tr>
<td>Using Protocol</td>
<td>(Telnet/SSH Connectivity Only) Whether VNE is using Telnet or SSH. This provides an easy way for operators to check which protocol is being used.</td>
</tr>
</tbody>
</table>
Troubleshooting VNE Communication State Issues

Chapter 20  Troubleshooting VNE Modeling

Table 20-2  VNE Communication State Information (from VNE Status Details Window) (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog/Trap Connectivity</td>
<td>Tells you whether the device is sending traps or syslogs (an indication of whether the device is still “alive”). The format is value (time), where:</td>
</tr>
<tr>
<td></td>
<td>• value—Indicates whether a syslog or trap was (true) or was not (false) received in the last 6 minutes. This field is updated whenever a syslog or trap is received.</td>
</tr>
<tr>
<td></td>
<td>• timestamp—Indicates when the last change occurred. This field is refreshed whenever you open the VNE Status Details window.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>false (Mon Jul 19 23:03:33 PDT 2010) means the VNE has not received any syslogs or traps since the time and date listed.</td>
</tr>
<tr>
<td></td>
<td>true (Tue Jul 20 05:09:25 PDT 2010) means the VNE has been receiving syslogs or traps at least every 6 minutes since the time and date listed.</td>
</tr>
<tr>
<td></td>
<td>If this field is blank, either no syslogs or traps were sent since the VNE was started, or Prime Network is using a management policy that does not track syslogs and traps.</td>
</tr>
<tr>
<td></td>
<td>If syslogs or traps are not arriving, do the following:</td>
</tr>
<tr>
<td></td>
<td>2. Check whether the device is configured to forward traps and syslogs to the unit or gateway that has the running Event Collector. See Managing the Event Collector (AVM 100), page 14-1.</td>
</tr>
</tbody>
</table>
Figure 20-4 shows a VNE Status Details window for a VNE that is only partially reachable.

**Figure 20-4 Communication State Information in VNE Status Details Window**

- The VNE is using Telnet and the Telnet protocol failed to connect to the device because the prompt was incorrect. You should correct the Telnet sequence in the VNE properties; see Editing VNE Properties, page 19-43.
- The VNE is using the ensure-management communication policy which means the device is considered reachable when all enabled protocols are fully functional. So when the Telnet problem is fixed, the VNE should move to the reachable state.
Step 2  Optionally check the System event in Prime Network Events to see if it can provide more details.

**Note**  Keep in mind that if an AVM or unit crashes, Prime Network will not generate a Service event for the communication state change, because event-generating entity (the AVM or unit) is itself down. However, the GUI will display the VNE/Agent Unreachable icon. Any tickets related to the problem (that were sent before the crash) will remain open until the VNE restarts and generates a clearing event. If no related tickets were sent before the crash, check Prime Network Events for other related information.

If you want more information, you can adjust the registry setting so that Prime Network Events generates an elaborated report about state changes. See Table 20-5 on page 20-24.

---

**Step 3: Troubleshoot the Connectivity Issue**

Before you begin these steps, get the following information in order to avoid common mistakes that are made when checking VNE connectivity.

- In Prime Network Administration, get the following information (see VNE Telnet/SSH Settings, page 19-32):
  - The protocol and protocol version.
  - The authentication credentials used by the VNE. (For example, if the VNE uses Telnet, you will need the Telnet sequence.)
- Verify that you are using a machine on the same subnet as that on which the VNE resides. (We recommend you run this procedure from the VNE’s gateway or unit.)

Follow this procedure to troubleshoot the connectivity problem. Some steps may not apply, depending on your configuration.

**Step 1**  Try to ping the device. If you cannot, it is likely a network connectivity issue and you will have to work with your system administrator.

**Step 2**  For Telnet, run the following test to see if the problem is that the device may not recognize `\n` as an end-of-line terminator (a common scenario). You can confirm this problem by opening a Telnet connection to the device and looking for output similar to the following:

```
[64] collector failed to get expected prompt Password: after sending command admin
```

**Step 3**  If you do not see this prompt, proceed to Step 4. If you do see this prompt, use the following procedure to change the end-of-line terminator.

- a. Log into the gateway as `network user` and change to the Main directory by entering the following command. (`network user` is the operating system account for the Prime Network application, created when Prime Network is installed; for example, `network39`.)

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

- b. This example changes the end-of-line terminator to `\r` for an individual VNE; you should check the device and find out what end-of-line terminator to use. In this example, `avmxxx` is the AVM ID, `vne-key` is the VNE name, and `vne-ip` is the VNE IP address:

If the VNE is on the gateway server, the `unit-IP` should be `127.0.0.1`. If the VNE is not on the gateway server, the `unit-IP` should be the unit’s IP address.
Step 4

Try to connect to the device.

a. If you are using SSH, check the version the device is using, and the versions that are supported in connections.

   – Check the SSH version on the device. For Cisco devices, use the `show ip ssh` command. The following example was run on a Cisco 7600:

   ```
c7-npe1-76# show ip ssh
   SSH Enabled - version 2.0
   Authentication timeout: 120 secs; Authentication retries: 3
   c7-npe1-76#
   ```

   – Check the following chart to identify which connection versions are supported.

<table>
<thead>
<tr>
<th>Device SSH Version</th>
<th>Will Support Connections Using:</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH 2.x</td>
<td>SSHv2</td>
</tr>
<tr>
<td>SSH 1.x</td>
<td>SSHv1</td>
</tr>
<tr>
<td>SSH 1.99</td>
<td>SSHv2 and earlier</td>
</tr>
</tbody>
</table>

b. Using the same protocol that is configured on the VNE, open a direct connection to the device.

   **Note** Be sure to perform the test using the same subnet on which the VNE resides (preferably from the same machine). Devices are not always accessible from all subnets.

   – For SNMP, use a MIB browser to the sample SNMP MIBs from the device.

   **Note** When you connect, be sure you select the correct version; many SSH client applications use a default of SSHv2.

   – For Telnet, log into the device from the CLI.

If you cannot connect to the device, the likely source of the problem is something in your local configuration. Possible causes you can investigate are:

- **Device issues:**
  - If the device requires an SSH pseudo-terminal. If a communication snoop reveals an error similar to “client did not request a pseudo terminal,” follow the procedure in Step 5.
  - If you cannot get to the user/password stage, there is probably a device issue, such as an ACL or another configuration that is blocking the access.

- **VNE issues:**
  - If the VNE is using device credentials that are incorrect or unauthorized.
  - If the VNE is using a communication protocol which is not configured on or allowed by the device. (If you are using SSH, see Step 5.)
  - If the VNE cannot access the device from the VNE’s subnetwork. (A configured route to the device may not exist, or there is some other network accessibility issue.) Try this procedure using the VNE’s unit or gateway.
If you can connect to the device, the likely cause of the problem is that the VNE driver was not correctly implemented. Check the Cisco Bug Toolkit for possible open caveats, or open a bug as explained in Opening a Bug Report, page 20-24.

Step 5 Open an SSH Pseudo-terminal, if required by the device (for example, a snoop can reveal an error similar to “client did not request a pseudo terminal”). Edit the registry so that SSH on the VNE requests a pseudo-terminal:

a. Log into the gateway as network user and change to the Main directory by entering the following command. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

   # cd $ANAHOME/Main

b. Edit the VNE’s registry as follows, where avmxxx is the A VM ID, vne-key is the VNE name, and vne-ip is the VNE P address.

   If the VNE is on the gateway server, the unit-IP should be 127.0.0.1.
   If the VNE is not on the gateway server, the unit-IP should be the unit’s IP address.

   # ./runRegTool.sh -gs 127.0.0.1 set unit-IP
   “avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/connection/explicitly-ask-for-pty” true
   # ./runRegTool.sh -gs 127.0.0.1 add unit-IP
   “avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/connection/transport”
   # ./runRegTool.sh -gs 127.0.0.1 set unit-IP
   “avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/connection/transport/pty-support” enable
   # ./runRegTool.sh -gs 127.0.0.1 set unit-IP
   “avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/telnet-over-sshv1/leadingcrenabled” false
   # ./runRegTool.sh -gs 127.0.0.1 set unit-IP “avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/telnet-over-sshv2/leadingcrenabled” false

c. Restart the VNE.

If you need more information about protocols and the tests and settings Prime Network uses to determine reachability, see How Prime Network Determines Protocol Reachability, page 24-3.

Troubleshooting VNE Investigation State (Discovery) Issues

Users with Operator privileges can rediscover complete network elements or individual components within network elements using Prime Network Vision. This is done by right-clicking a device or device component and selecting Poll Now.

Rediscovering an entire device can also be done from the Prime Network Administration GUI client by right-clicking a VNE and selecting Inventory. Figure 20-5 shows the device inventory window with the Poll Now button at the top left. Although the Poll Now button is provided for use by all VNEs, it is specifically useful for VNEs using reduced polling because it provides a quick way to synchronize the VNE model without having to wait for the next polling cycle.
The following steps provide an overall procedure for responding to an unexpected VNE investigation state.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>See:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify the current VNE investigation (and communication) states in Prime Network Vision.</td>
<td>Step 1: Check the Investigation State, page 20-16</td>
</tr>
<tr>
<td>2</td>
<td>Check the investigation state description in the VNE Status Details window, especially if you are seeing the Currently Unsynchronized state. You can optionally check the System event to see if it can provide any new information.</td>
<td>Step 2: Check the VNE Status Details for the Cause of the Modeling Problem, page 20-19</td>
</tr>
</tbody>
</table>
### Troubleshooting VNE Investigation State (Discovery) Issues

**Note**
At any time you can restart the VNE discovery process by restarting the VNE (see Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-44).

#### Step Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3    | If needed, perform these additional steps depending on the information you need:  
- Verify that all required device configuration tasks have been performed.  
- Verify that there are no communication state issues.  
- Change Prime Network so that it generates an elaborated report about state changes.  
- Get more information to provide to the Cisco Technical Assistance Center. |
|      | See:  
Step 3: Additional Troubleshooting Steps for Investigation State Problems, page 20-23 |

#### Step 1: Check the Investigation State

**Step 1**
From the Prime Network Vision map view, double-click the icon in which you are interested. This opens the device properties window.

**Note**
You can launch the device properties window from Prime Network Administration by right-clicking the VNE and choosing **Inventory**.
Step 2  Check the current Investigation State (as shown in Figure 20-6). The various states are described in Table 20-3, which follows the figure.

Figure 20-6  VNE Investigation State (in Prime Network Vision)
### Table 20-3 VNE Investigation States

<table>
<thead>
<tr>
<th>State Name</th>
<th>Description</th>
<th>Badge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined Not Started</td>
<td>A new VNE was created (and is starting); or an existing VNE was stopped. In this state, the VNE is managed and is validating support for the device type. (This investigation state is the equivalent of the Agent Not Loaded communication state.) A VNE remains in this state until it is started (or restarted). In the VNE Status Details window, the description will say <strong>VNE is down</strong>.</td>
<td>None</td>
</tr>
<tr>
<td>Unsupported</td>
<td>The device type is either not supported by Prime Network or is misconfigured (it is using the wrong scheme, or is using reduced polling but the device does not support it). See Table 20-4 on page 20-21 for troubleshooting steps.</td>
<td></td>
</tr>
</tbody>
</table>
| Discovering           | The VNE is building the model of the device (the device type was found and is supported by Cisco Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery timeout. In the VNE Status Details window, the description will say **Initial investigation of the device**. To troubleshoot a VNE that does not move out of this state, perform the following steps:  
1. Verify that all required device configuration tasks have been performed. If they were not, Prime Network cannot properly model the device. See Device Configuration Tasks for VNE Creation, page A-1.  
2. Verify that there are no communication state issues. See Steps to Troubleshoot VNE Communication State Issues, page 20-3. Also see Troubleshooting VNE Communication State Issues, page 20-1.  
3. Verify that the VNE is using the proper scheme. See Choosing a VNE Scheme, page 19-5.  
4. Verify that the device is using the proper polling method. See Finding Out Whether a VNE is Using Reduced Polling, page 22-4.  
The default discovery timeout is 30 minutes but is customizable. To change the timeout, see Registry Settings for VNE Discovery Timeout and Investigation State Reporting, page 20-23. | ![badge] |
| Operational            | The VNE has a stable model of the device. Modeling may not be fully complete, but there is enough information to monitor the device and make its data available to other applications, such as activation scripts. A VNE remains in this state unless it is stopped or moved to the maintenance state, or there are device errors. In the VNE Status Details window, the description will say **Ongoing synchronization with the device**. | None  |
| Currently Unsynchronized | The VNE model is inconsistent with the device. This can be due to a variety of reasons; check the VNE Status Details window can provide more information (see Step 2: Check the VNE Status Details for the Cause of the Modeling Problem, page 20-19). | ![badge] |
Troubleshooting VNE Modeling

Chapter 20

Table 20-3 VNE Investigation States (continued)

<table>
<thead>
<tr>
<th>State Name</th>
<th>Description</th>
<th>Badge</th>
</tr>
</thead>
</table>
| Maintenance      | VNE polling was suspended because it was manually moved to this state. In the VNE Status Details window, the description will say **Device synchronization was suspended by user or system**. The VNE remains in this state until it is manually restarted. A VNE in the maintenance state has the following characteristics:  
  • Does not poll the device, but handles syslogs and traps.  
  • Maintains the status of any existing links.  
  • Does not fail on VNE reachability requests.  
  • Handles events for correlation flow issues. It does not initiate new service alarms, but does receive events from adjacent VNEs, such as in the case of a Link Down alarm.  
  
  The VNE is moved to the Stopped state if: it is VNE is moved, the parent AVM is moved or restarted, the parent unit switches to a standby unit, or the gateway is restarted. | ![badge] |
| Partially        | The VNE model is inconsistent with the device because a required device command failed, even after repeated retries. A common cause of this state is that the device contains an unsupported module. See Table 20-4 on page 20-21 for troubleshooting steps. | ![badge] |
| Discovering      |                                                                                                                                                    |       |
| Shutting Down     | The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device. The VNE Status Details window, the description will say **Device synchronization aborted**. | ![badge] |
| Stopped           | The VNE process has terminated; it will immediately move to Defined Not Started. | None |

Step 2: Check the VNE Status Details for the Cause of the Modeling Problem

Step 1  
From the VNE properties window (see Figure 20-6 on page 20-17), click **VNE Status** at the bottom of the properties window to open the VNE Status Details window and check the investigation state information, comparing it against the information in Table 20-4 on page 20-21.
Figure 20-7  Investigation State Information in VNE Status Details Window
Troubleshooting VNE Investigation State (Discovery) Issues

Table 20-4  VNE Investigation State Information (from VNE Status Details Window)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management State</td>
<td>VNE investigation state. Basic descriptions of all of the investigation states is provided in Table 19-2 on page 19-5.</td>
</tr>
<tr>
<td>Description</td>
<td>Cause of the current investigation state. Registry Settings for VNE Discovery Timeout and Investigation State Reporting, page 20-23. The following is a partial list of messages you may see and how to troubleshoot the problem indicated by the message.</td>
</tr>
</tbody>
</table>

**Unsupported**

**VNE cannot synchronize with the device**—The device type is not supported by Cisco Prime Network (no VNE driver was found for the device). Possible causes:

- The VNE is using the wrong scheme. Verify the device type against the supported schemes in Table 19-4 on page 19-9.

- The VNE is using the reduced polling method, but the VNE does not support that method. To check whether the device type supports reduced polling, use the procedure described in Finding Out Whether a Device Type Supports Reduced Polling, page 22-5.

- Check whether the element is supported in a released device package. See What Are Independent VNE Drivers and Device Packages?, page 21-1.

If the device type is not supported:

- You can add the VNE as Generic VNE or ICMP VNE. These VNE types are specified in the VNE General properties; see Table 19-10 on page 19-29.

- You can add the support using the Prime Network VNE Customization Builder. See the Cisco Prime Network 3.9 Customization User Guide.

To extend Cisco Prime Network functionality so that it recognizes unsupported devices, use the VNE Customization Builder. See the Cisco Prime Network 3.9 Customization User Guide.
Troubleshooting VNE Investigation State (Discovery) Issues

Description (continued)

Currently Unsynchronized

The VNE model is inconsistent with the device. This can be due to a variety of reasons:

- **User initiated device re-synchronization**—A user clicked Poll Now in Cisco Prime Network Vision (or issued a BQL command that performs this operation).

- **Resuming synchronization after maintenance**—The VNE is moving out of a user-induced Maintenance state (a user restarted the VNE).

- **Device CPU is high. Synchronization temporarily suspended**—The adaptive polling mechanism moved the VNE to this state because the device exceeded its maximum CPU usage threshold. For troubleshooting tips see CPU Utilization Problems: Where to Begin, page 22-2.

- **Resuming synchronization after device CPU normalized**—The adaptive polling mechanism is moving the VNE back to its normal polling because device CPU usage has stabilized.

- **System initiated device resynchronization due to missed device configuration changes**—The VNE is using reduced polling and has identified a gap in the configuration log (specifically, the configuration archive buffer), or has failed to identify one or more changes. (VNEs using reduced polling are more sensitive to these changes due to their different polling frequency. For more information, see Reduced Polling, page 22-2.

- **VNE cannot reach the device, Synchronization temporarily suspended**—The device did not respond in a timely fashion. Follow the troubleshooting steps in Steps to Troubleshoot VNE Communication State Issues, page 20-3.

- **Resuming synchronization after device reachability from VNE restored**—The VNE is moving out of an unreachable state.

- **Temporarily missing or failed VNE driver component**—A required, recoverable device command failed. Prime Network retries the command at the next polling cycle, up to 3 retries. (If it fails, the VNE is moved to Partially Discovered.)

- **Device synchronization was suspended by system**—The system temporarily stopped the synchronization process because it suspects the device was reloaded (this prevents the VNE from collecting irrelevant information). The synchronization process will normally restart within 5 minutes.

The Currently Unsynchronized state can also be caused by a communication state issue. See Steps to Troubleshoot VNE Communication State Issues, page 20-3.

Table 20-4 VNE Investigation State Information (from VNE Status Details Window) (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description (continued)</td>
<td>Currently Unsynchronized</td>
</tr>
<tr>
<td><strong>Partially Discovered</strong></td>
<td>Missing or failed VNE driver component—Prime Network could not recognize an element in the device. Consider the following troubleshooting options:</td>
</tr>
<tr>
<td>Check whether the element is supported in a released device package. See What Are Independent VNE Drivers and Device Packages?, page 21-1.</td>
<td></td>
</tr>
<tr>
<td>To extend Cisco Prime Network functionality so that it recognizes unsupported parts of devices, use the VNE Customization Builder. See the Cisco Prime Network 3.9 Customization User Guide.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 20  Troubleshooting VNE Modeling

Troubleshooting VNE Investigation State (Discovery) Issues

Step 2
Optionally, check the System event in Prime Network Events to see if it can provide additional information.

Note
Keep in mind that if an AVM or unit crashes, Prime Network will not generate a Service event for the communication state change, because event-generating entity (the AVM or unit) is itself down. However, the GUI will display the VNE/Agent Unreachable icon. Any tickets related to the problem (that were sent before the crash) will remain open until the VNE restarts and generates a clearing event. If no related tickets were sent before the crash, check Prime Network Events for other related information.

Step 3: Additional Troubleshooting Steps for Investigation State Problems

Step 1
Verify that all required device configuration tasks have been performed. If they were not, Prime Network cannot properly model the device. See Device Configuration Tasks for VNE Creation, page A-1.

Step 2
Verify that there are no communication state issues; specifically, check for a System event in Prime Network Vision. The problem may be due to the fact that the device did not respond in a timely manner.

Step 3
Optionally perform the following tasks:
- Adjust the registry setting so that Prime Network Events generates an elaborated report about state changes. See Table 20-5 on page 20-24.
- Open the device properties window in Prime Network Vision. Place your cursor in the inventory window, and press F2. Click Managed State Aspect and review the information. This information is especially useful when working with the Cisco Technical Assistance Center.

Registry Settings for VNE Discovery Timeout and Investigation State Reporting

Table 20-5 lists registry settings you can change to control the following discovery and state reporting behaviors:

- Whether Prime Network should generate a Service event and long event description when an investigation state changes. This is not done by default because it can affect performance and cause unnecessary concern to operators. (Service events are generated for communication state changes by default.)
• The number of retries for device commands issued during the discovery process, and whether the device command is required.

• Whether Prime Network should use the timeout mechanism or the convergence mechanism to determine when the discovery process is complete. (You can also adjust the length of the discovery timeout.)

Note

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

Table 20-5  Registry Settings for Discovery and Investigation States

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Investigation and Communication State Reporting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>site/agentdefaults/da/investigation-progress/investigation-state-update-event</td>
<td>Generate a Service event (in Prime Network Events) when investigation state changes</td>
<td>false</td>
</tr>
<tr>
<td>site/agentdefaults/da/investigation-progress/investigation-state-result-summary-event</td>
<td>Include an elaborated report about the investigation state change in the Long Description field of the Service event</td>
<td>false</td>
</tr>
<tr>
<td><strong>Device Commands Used for Discovery</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>site/interfacebasedscheme/default registration/error update tolerance</td>
<td>Allowable number of device command failures, after which an error is generated</td>
<td>3</td>
</tr>
<tr>
<td>site/interfacebasedscheme/default registration/required</td>
<td>Designate the device command as required for evaluating an investigation state (insert this after the device command key name)</td>
<td>false</td>
</tr>
<tr>
<td><strong>VNE Discovery Period Controls</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>site/agentdefaults/da/investigation-progress/max-delay-before-managed-state-in-milliseconds</td>
<td>Timeout for VNE discovery process (in milliseconds) (ignored if convergence is being used)</td>
<td>1800000 (30 minutes)</td>
</tr>
<tr>
<td>site/agentdefaults/da/investigation-progress/convergence</td>
<td>Use the VNE convergence mechanism to control discovery</td>
<td>false</td>
</tr>
</tbody>
</table>

**Opening a Bug Report**

After performing the troubleshooting steps in the previous sections, if you still have a problem, you may consider opening a bug (or enhancement request).

**Before You Open a Bug**

1. Verify that the network element, event, script, etc. is supported by checking these documents:
   - *Cisco Prime Network 3.9 Reference Guide*
   - *Addendum: Additional VNE Driver Support for Cisco Prime Network 3.9* (this document is released when the first DP becomes available; see *What Are Independent VNE Drivers and Device Packages?*, page 21-1.)
Note

If the device is not supported, you can add the support using the Prime Network VNE Customization Builder. See *Cisco Prime Network 3.9 Customization User Guide*. Also, this guide contains an extended procedure for finding out which traps and syslogs are not supported and how to troubleshoot them.

2. Make sure you have tried all of the troubleshooting steps provided in these topics:
   - Troubleshooting VNE Communication State Issues, page 20-1
   - Steps to Troubleshoot VNE Communication State Issues, page 20-3
   - Troubleshooting VNE Investigation State (Discovery) Issues, page 20-14

3. Provide all of the necessary details for the bug report (reproduce the problem if necessary).

**Information You Must Provide**

1. Describe the actual behavior versus the expected behavior. For example, “Module serial numbers are missing from Vision.”
2. Describe how to recreate the error scenario.
3. Provide the following device details:
   - Device type.
   - Device operating system (including service and patches applied on the NE).
   - Device configuration information. If possible, attach a running config.
   - For device physical modeling issues, details on the physical module.
   - For device logical modeling issues, details on the service.
4. Collect the following Prime Network information:
   - Pertinent AVM log files from `NETWORKHOME/Main/logs`.
   - List of VNE drivers that are installed.
   - Prime Network version. From the gateway, run `networkctl status` and note the version and build number that are displayed at the top of the status message.
   - Patch level details. You can use this command:
     ```
     checkPatchInstallation.pl -v -p
     ```
5. For physical model issues, provide screen captures (of the Prime Network GUI clients and the EMS) that show the discrepancies.
6. For NBI-related issues, provide the IMO or BQL citation.
Opening a Bug Report
VNE Updates

You can obtain updates to VNEs that provide device support enhancements and bug fixes, in addition to support for completely new devices. The following topics describe how you can obtain and install these VNE updates:

- What Are Independent VNE Drivers and Device Packages?, page 21-1
- How to Find Out if New Support is Available, page 21-2
- Identifying VNE Driver Packages That Are Installed on the Gateway, page 21-3
- Identifying Which Driver a VNE Is Using, page 21-4
- Downloading and Installing New Driver Files, page 21-5
- Changing the Device Package a VNE Is Using, page 21-4
- Uninstalling a Device Package, page 21-7
- Troubleshooting Driver Installations, page 21-8

Note

When you upgrade a device’s operating system (such as installing a Cisco Catalyst OS update), you do not need to restart the VNE. When the VNE polls for configuration information, it will detect the changes and will restart itself. When the VNE reloads, it will update any required registry information, such as the VNE registry path.

What Are Independent VNE Drivers and Device Packages?

Independent VNE drivers are individual driver jar files that contain new or enhanced support for a device, such as software versions, physical and logical entities, syslogs, traps, and activation scripts. These are released outside of a major or minor release of Prime Network. A complete set of independent VNE drivers is provided with base releases of Prime Network.

Updates to driver jar files are packaged together and delivered in Device Packages (DPs). As newer versions become available, DPs are placed on the Prime Network Software Download site on Cisco.com. The new support is documented in the Addendum: Additional VNE Driver Support for Cisco Prime Network 3.9 (which becomes available when the first DP is released). Once you download a Device Package you can install it and then restart the VNE to apply the new driver file.

New drivers are installed using the ivne script. After new drivers are downloaded, the gateway server copies the new driver information to all units.

You can also customize which driver versions are used by VNEs by choosing a different DP using the Update VNE Driver Package from the VNE’s right-click menu.
Device Package and VNE Driver Jar File Versions

VNE driver jar files are cumulative and contain all the enhancements that are provided in earlier versions. All jar files use the following versioning scheme:

Vendor-JarType-VNEJarVersion.jar

*JarType* can be Modules, Commons, or device-specific. For example:

<table>
<thead>
<tr>
<th>Jar File Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco-Commons-v1.0.0.0.jar</td>
<td>First release of jar file with support common to all Cisco devices.</td>
</tr>
<tr>
<td>Cisco-Modules-v1.0.0.0.jar</td>
<td>First release of jar file with support common to all Cisco modules.</td>
</tr>
<tr>
<td>Cisco-ASR90xx-v2.0.0.0.jar</td>
<td>Second release of jar file with support common to all ASR 9000 Series Aggregation Services Routers. Contains all of the support provided in version 1.0.0.0.</td>
</tr>
<tr>
<td>Cisco-3750ME-v1.0.0.0.jar</td>
<td>First release of jar file with support common to all Cisco Catalyst 3750 Metro Series Switches.</td>
</tr>
</tbody>
</table>

Device Packages always contain the latest version of *all* available jars. Even if a jar is not revised for a DP, it is still included in the latest DP so that all available enhancements are present. Remember that installing the DP on the gateway server is different from applying the new drivers to a VNE; that does not occur until you restart the VNE.

DPs use the following versioning scheme:

PrimeNetwork-A.xTOB.x-DPym.tar

where:

A.xTOB.x: Indicates the range of Prime Network releases in which the device package is supported.

DPym: Indicates the year and month in which the device package is released.

Example: PrimeNetwork-3.8.xTO3.9.x-DP1205.tar

How to Find Out if New Support is Available

The *Cisco Prime Network 3.9 Reference Guide* lists the support provided with the base release. When a new DP is released, the new support is documented in *Addendum: Additional VNE Driver Support for Cisco Prime Network 3.9*, which is a companion document to the reference guide.

In addition, you can find the following DP-specific information at the Prime Network Software Download site:

- A Readme file that describes the DP, including the new support, resolved and open bugs, and links to previous Readmes.
- *Cisco Prime Network 3.9 VNE Device Package Installation Guide* (available when the first DP is released)

Note: These documents are not available until the first Prime Network 3.9 DP is released.
Identifying VNE Driver Packages That Are Installed on the Gateway

The following procedure explains how you can list all of the driver files in a specified DP that are installed on the gateway server in NETWORKHOME/Main/drivers. Many different versions of DP can be installed at one time and many of them may not be being used. Each VNE can use its own instance of the DP for modeling.

By default, when a VNE is restarted, it uses the latest DP installed on the gateway or unit. Using the latest DP means Prime Network will detect the device type and identify the newest DP for that device type (for both Cisco and non-Cisco devices). You can also choose a different driver at a later time as described in Changing the Device Package a VNE Is Using, page 21-4.

Note
To identify which driver version is being used by a VNE, see Identifying Which Driver a VNE Is Using, page 21-4.

Step 1
Log into the gateway as network user. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

Step 2
Start the ivne script and choose the option to list the contents:

```bash
# ivne
```

---

| 1 | Install VNE Device Package from a local directory. |
| 2 | Install VNE Device Package from a Web repository. |
| 3 | List installed Device Packages. |
| 4 | Uninstall a Device Package (DP). |
| 5 | Quit |
---

Step 3
The script displays a submenu that lists the installed DPs. Choose one to list the DP contents.

```bash
|       Select Device Package (DP) to display the included drivers. |
| 1 | CiscoPrimeNetwork-3.9-DP0 |
| 2 | PrimeNetwork-3.8TO3.9-DP1205 |
| 3 | PrimeNetwork-3.8TO3.9-DP1206 |
| 4 | PrimeNetwork-3.8TO3.9-DP1207 |
| 5 | Back |
```

Step 4
The script lists the contents of the specified DP.

Gathering information from /export/home/network39/Main/drivers/

<table>
<thead>
<tr>
<th>Name</th>
<th>Driver File Name</th>
<th>Version</th>
<th>Device Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco-100xx-PN3.9</td>
<td>Cisco-100xx-v3.0.0.0.jar</td>
<td>3.0.0.0</td>
<td>CiscoPrimeNetwork-3.9-DP0</td>
</tr>
<tr>
<td>Cisco-12xxx-PN3.9</td>
<td>Cisco-12xxx-v3.0.0.0.jar</td>
<td>3.0.0.0</td>
<td>CiscoPrimeNetwork-3.9-DP0</td>
</tr>
<tr>
<td>Cisco-3400ME-PN3.9</td>
<td>Cisco-3400ME-v3.0.0.0.jar</td>
<td>3.0.0.0</td>
<td>CiscoPrimeNetwork-3.9-DP0</td>
</tr>
</tbody>
</table>
Identifying Which Driver a VNE Is Using

When a VNE is created, by default it checks the gateway for the most recent DP and uses the applicable driver from that DP. DPs are installed on the gateway server in NETWORKHOME/Main/drivers. You can specify a different DP when you create the VNE, or by updating the VNE (see Changing the Device Package a VNE Is Using, page 21-4).

The VNEs table displays the specific device driver file and version that VNEs are using. Figure 21-1 illustrates the driver jar file information that is shown when you list all VNEs. This information is also provided on the VNE properties page.

To find out if a newer device driver is available, check the Addendum: Additional VNE Driver Support for Cisco Prime Network 3.9. That document becomes available when the Prime Network DP is published. The “New Support” section lists all new functionality that is available via DP. If new support is available, download and install the DP as described in Downloading and Installing New Driver Files, page 21-5.

Changing the Device Package a VNE Is Using

The update function allows you to choose from all DPs that are installed on the gateway or unit and apply the DP’s corresponding jar file to a VNE. You can also choose an earlier DP, effectively rolling back to an earlier version. You must stop and restart the VNE for the changes to take effect. A best practice is to test a new DP on one VNE before applying it to the other device types.

Choosing latest means Prime Network will detect the device type and identify the newest DP for the device type (for both Cisco and non-Cisco devices).

Step 1
If needed, download a copy of the Addendum: Additional VNE Driver Support for Cisco Prime Network 3.9 which lists:

- The support added in a specific DP, by device series.
- The versions of VNE drivers that were with each DP.

Step 2
Right-click a single or group of VNEs and choose Update VNE Driver Package. Prime Network displays all installed DPs along with a latest choice. For example:
Chapter 21  VNE Updates

Steps 3

Step 3 If a latest DP is available and you want that support, download and install it as described in Downloading and Installing New Driver Files, page 21-5.

Step 4 Select a DP and click OK.

Step 5 Restart the VNEs to apply the changes by right-clicking the VNEs and selecting Actions > Stop. When the status changes to Down, right-click the VNEs and select Actions > Start.

---

**Downloading and Installing New Driver Files**

Use this procedure to download and install new driver files to your gateway server. The new drivers are not applied until you restart the VNEs.

**Preparing to Install a New VNE Device Package**

<table>
<thead>
<tr>
<th>Step</th>
<th>See:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Check the documentation for new support, and run a report to identify which VNEs should be updated.</td>
<td>Preparing to Install a New VNE Device Package, page 21-5</td>
</tr>
<tr>
<td>2. Download the Device Package tar file according to the instructions on the download site.</td>
<td>Download the Device Package, page 21-6</td>
</tr>
<tr>
<td>3. Download the DP installation instructions using <code>ivne</code> to install the DP.</td>
<td>Installing the Device Package Using <code>ivne</code>, page 21-6</td>
</tr>
<tr>
<td>4. Apply the new drivers to the VNEs.</td>
<td>Restarting the VNEs to Apply the New Driver Files, page 21-7</td>
</tr>
</tbody>
</table>

---

**Prefering to Install a New VNE Device Package**

**Step 1** Check the *Addendum: Additional VNE Driver Support for Cisco Prime Network 3.9* to find out what support is available, and note the device types you want to update.

**Step 2** If you are not sure what is installed on the gateway server, check it by performing the procedure in Identifying VNE Driver Packages That Are Installed on the Gateway, page 21-3.

**Step 3** Identify the VNEs of that device type. You can do this in several ways; here are two examples:

- Select All Servers and click the All VNEs tab. Click the Element Type column to sort the table, and identify the device type you are looking for.
- For long lists, choose Reports > Run Report > Inventory Report > Hardware Summary (By Selected Property). When you select devices, enter the device type in the search field, and save and print your list.
Download the Device Package

For the current instructions on downloading the DP, use the documentation that is on the download site. This procedure explains how to get the documentation.

**Step 1** Log into Cisco.com

**Step 2** Go to the Prime Network Software Download site and navigate to the Prime Network VNE Drivers.

**Step 3** From the download site, click the hyperlink for the Prime Network 3.9 VNE Device Package Installation Guide (available when the first DP is released).

**Step 4** Follow the instructions in the guide.

---

Installing the Device Package Using ivne

The `ivne` script installs DP on the gateway server. The changes are not applied to the VNEs until they are restarted. If any new drivers depend on the support provided in other driver, those jar files are also installed.

**Step 1** Make sure you have the necessary information, such as the location of the jar file, by checking the procedure in the Prime Network 3.9 VNE Device Package Installation Guide. (You should have downloaded that file as instructed in Download the Device Package, page 21-6.).

**Step 2** Log into the gateway as `network user`. (`network user` is the operating system account for the Prime Network application, created when Prime Network is installed; for example, `network39`.)

**Step 3** Enter the `ivne` command:

```
# ivne
```

```
| 1 | Install VNE Device Package from a local directory.
| 2 | Install VNE Device Package from a Web repository.
| 3 | List installed Device Packages.
| 4 | Uninstall a Device Package (DP).
| 5 | Quit
```

**Step 4** Choose 1 or 2 depending on the location of the driver files:

- Choose 1 to install the DP when they are on a local folder on the gateway server.
- Choose 2 when the DP are on a remote host, such as a web server that is providing central support to multiple gateway servers.

The script creates an installation log file in `NETWORKHOME/Main/drivers/log/ivne-install-log-mmddyy-hHmmss`. 
Chapter 21  VNE Updates

Uninstalling a Device Package

Step 5  Provide the location of the DP files:

<table>
<thead>
<tr>
<th>If you chose...</th>
<th>Provide the location in this format:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (install from tar file)</td>
<td>Enter the full pathname.</td>
</tr>
</tbody>
</table>
| 2 (install from web repository) | Enter the repository address in one of these formats:  
  IP-address/full-pathname-to-DP-repository  
  hostname/full-pathname-to-DP-repository  
  Example: 120.56.57.58/drivers |

**Restarting the VNEs to Apply the New Driver Files**

Click the All VNE tab to view the VNEs table. You can restart individual or groups of VNEs by right-clicking the VNEs and selecting **Actions > Stop**. When the status changes to Down, right-click the VNEs and select **Actions > Start**.

**Uninstalling a Device Package**

A DP uninstallation removes the DP from the gateway. Any VNEs using the DP will have to be updated to use a different DP.

Step 1  Verify that no VNEs are using the DP you plan to uninstall by following the procedure in **Identifying Which Driver a VNE Is Using**, page 21-4.

Step 2  Log into the gateway as **network user**. (**network user** is the operating system account for the Prime Network application, created when Prime Network is installed; for example, **network39**.)

Step 3  Start the **ivne** script and choose the option to uninstall a DP:

```
# ivne
```

| 1 | Install VNE Device Package from a local directory. |
| 2 | Install VNE Device Package from a Web repository. |
| 3 | List installed Device Packages. |
| 4 | Uninstall a Device Package (DP). |
| 5 | Quit |

Step 4  The script displays a submenu that lists the installed DPs. Choose one to list the DP contents.

| 1 | CiscoPrimeNetwork-3.9-DP0 |
| 2 | PrimeNetwork-3.8TO3.9-DP1205 |
| 3 | PrimeNetwork-3.8TO3.9-DP1206 |
| 4 | PrimeNetwork-3.8TO3.9-DP1207 |
| 5 | Back |
Step 5  Select the DP you want to uninstall from the list that is displayed. The script creates an uninstallation log file in `NETWORKHOME/Main/drivers/log/ivne-uninstall-log-mmddyy-hhmmss` and uninstalls the DP.

---

**Troubleshooting Driver Installations**

The following table lists error messages you might encounter when using `ivne` and how to rectify the cause of the problem.

<table>
<thead>
<tr>
<th>ivne Error Message</th>
<th>Details/Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>The repository folder does not contain any driver jar files. Please verify the folder location.</td>
<td>The web repository folder does not exist.</td>
</tr>
<tr>
<td></td>
<td>• Verify that you entered the correct IP address and hostname.</td>
</tr>
<tr>
<td></td>
<td>• Verify that you entered the complete path; for example, enter 120.56.576.58/drivers, instead of 120.56.57.58.</td>
</tr>
<tr>
<td></td>
<td>• Verify whether the web server is down.</td>
</tr>
<tr>
<td>Invalid value for width: 80 at <code>NETWORKHOME/local/scripts/install_ivne.pl</code> line 40</td>
<td>The display window is too narrow to display the ivne command menu. Increase the display window width and rerun the command.</td>
</tr>
</tbody>
</table>
PART 5

Advanced VNE Administration
Customizing VNE Polling

To maintain connectivity between a device and Prime Network, and to keep the model up to date, Prime Network uses a variety of polling methods to maintain a balance between model fidelity (more polling cycles) and high system performance (less polling cycles). Table 22-1 lists the polling methods used by Prime Network, their default behavior, and where you can find more information on each method and how to customize it.

If you are experiencing high CPU usage, see CPU Utilization Problems: Where to Begin, page 22-2.

Table 22-1 Polling Mechanisms Used by Prime Network

<table>
<thead>
<tr>
<th>Polling Mechanism</th>
<th>Description</th>
<th>Default Setting</th>
<th>For information, see:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced polling</td>
<td>Polls the device when a configuration change syslog is received, rather than according to any interval. Changes to the model are updated immediately.</td>
<td>Disabled. Can be enabled per VNE from GUI.</td>
<td>Reduced Polling, page 22-2</td>
</tr>
<tr>
<td>Adaptive polling</td>
<td>When CPU usage is high, introduces an interval between executions of device commands. Changes are updated according to the interval.</td>
<td>Enabled. Can be enabled or disabled per VNE from GUI.</td>
<td>Adaptive Polling, page 22-15</td>
</tr>
<tr>
<td>Polling groups</td>
<td>Executes device commands according to the polling group setting, in a repetitive fashion. You can create new polling groups using Prime Network Administration, and apply them to network elements. Changes are updated according to the polling cycles.</td>
<td>Enabled with two default polling groups, slow and default. Can be controlled from GUI.</td>
<td>VNE Polling Groups and Slow Polling, page 22-23</td>
</tr>
<tr>
<td>Smooth polling</td>
<td>Takes commands in the same polling cycle and spreads their execution throughout the polling cycle using a random number within the polling interval, rather than using a timer-based approach.</td>
<td>Enabled. Can be enabled by editing the registry.</td>
<td>Smooth Polling, page 22-26</td>
</tr>
<tr>
<td>Smart polling</td>
<td>For repetitive queries, introduces a polling protection interval that specifies the minimum amount of time that must pass before a query can be sent to a device a second time.</td>
<td>Disabled. Can be enabled by editing the registry.</td>
<td>Smart Polling (On-Demand Polling), page 22-27</td>
</tr>
</tbody>
</table>
CPU Utilization Problems: Where to Begin

If you suspect ongoing CPU utilization problems, start with these troubleshooting steps:

1. Review the device log files to find any recurring polling spikes that extend for prolonged periods. If the CPU spikes are not occurring at a constant interval, it is likely a network events rather than a device problem.

2. Verify whether other applications (besides Prime Network) are managing the devices, and check those applications for problems before proceeding with Prime Network customizations.

3. If you think the problem resides in Prime Network, analyze the CPU over a 24-hour period as follows:
   - Log onto the device and check the usage for different timelines. (Refer to the operating system documentation that applies to the device type.)
   - Check the audit log for any open sessions that correspond with the usage problems.

4. Read the following topics:
   - Adaptive Polling, page 22-15
   - VNE Polling Groups and Slow Polling, page 22-23

5. Consider disabling MAC-based topology. To disable this topology, use the following registry command, where devicetype is the registry location for the device type. For an example of how to find the devicetype, see Configuring Reduced Polling for All VNEs of the Same Device Type, page 22-8.

   # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/device-type/ipcore/software versions/default version/amsi/topology/ethernet/MacTestEnable" false

   For example, this command disables MAC-based topology for Cisco 7600 routers:

   # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/ciscorouter2/76xx/product/software versions/default version/amsi/topology/ethernet/MacTestEnable" false

Reduced Polling

If a VNE is using the reduced polling mechanism, it polls the device when a configuration change syslog is received. Changes to the model are updated immediately. This polling strategy is useful when configuration changes for devices can be sufficiently obtained from a log of the archived changes, instead of repeatedly polling for the information and forcing the VNE to identify the changes. Thus for certain device types, Prime Network offers the option of using reduced polling. The Prime Network Administration GUI client provides a link that will launch a window listing all device types that support reduced polling, as shown in Figure 22-3 on page 22-6.

In general all types of VNE (except Generic types) make use of the expedited event mechanism. Normally changes are detected by way of syslog or trap notification events, or model changes that are detected through regular polling. Although the notification events provide the source and other helpful information describing the nature of the change, they do not provide enough information to capture the entire scope of the change, and the effect the change can have on other network elements. In these situations, Prime Network uses expedited polling to capture network element status information.
A VNE can move to the Currently Unsynchronized state for a number of reasons, such as the failure of a required, recoverable device command, or because it is moving out of the Maintenance state. A complete list of causes is provided in Table 20-4 on page 20-21. The causes pertaining to reduced polling are as follows:

- The VNE is using reduced polling and has identified a gap in the configuration archive buffer or has failed to identify one or more changes. A gap is identified as follows.
  
  The device configuration archive buffer contains the configuration commands that were executed on the device. For Cisco IOS devices, it is possible for the buffer to overflow when a large number of commands are executed; thus some commands can be lost, a gap is identified, and the VNE is assumed to be out of sync with the device. VNEs using reduced polling are more sensitive to these changes due to their different polling frequency.

- A user clicked Poll Now in Prime Network Vision (or by using the appropriate BQL command) and the VNE is being resynchronized with the device. Although the Poll Now button is provided for use by all VNEs, it is specifically useful for VNEs using reduced polling because it provides a quick way to synchronize the VNE model without having to wait for the next polling cycle.

Figure 22-1 Poll Now Button in Prime Network Vision
The information refresh is similar to the VNE discovery process, the main difference being what triggers the process.

Like any discovery process the VNE refresh has the potential of raising the CPU usage on the device. However, several factors work together to keep CPU usage low: the queueing mechanism that controls command execution, the VNE logic that reuses command results, and adaptive polling’s throttle mechanism that introduces a delay between commands.

The amount of time needed for the VNE refresh depends on many factors, such as device and network latency, and gateway server activities. To help you understand when the refresh is in process and when it has completed:

- The VNE moves to Currently Unsynchronized investigation state and its icon changes to an hourglass (see Figure 22-1).
- You can configure Prime Network to generate a System event when a VNE enters or exits the Currently Unsynchronized state (or any other investigation state). See Table 20-5 on page 20-24.

Basic Procedures and Customizations: Reduced Polling

These topics provide procedures that will help you identify whether reduced polling is being used by a VNE, and how to change the setting:

- Finding Out Whether a VNE is Using Reduced Polling, page 22-4
- Finding Out Whether a Device Type Supports Reduced Polling, page 22-5
- Selecting the Reduced Polling Mechanism for an Individual VNE, page 22-6

Finding Out Whether a VNE is Using Reduced Polling

To find out whether or not a VNE is using reduced polling, check the VNE Status Details window as follows.

**Step 1**
Open the device inventory window from the Prime Network Administration by right-clicking the VNE and choosing **Inventory**.

**Note**
Users with Operator privileges can open the Communications Details window from Prime Network Vision.

**Step 2**
Click **VNE Status** at the bottom of the window to open the VNE Status Details window, and check the reduced polling setting as shown in Figure 22-2.
Finding Out Whether a Device Type Supports Reduced Polling

To find out whether or not a VNE supports reduced polling, check the listing in the VNE properties dialog as follows.

**Step 1** Open the VNE properties window from the Prime Network Administration by right-clicking the VNE and choosing **Properties**.

**Note** Users with Administrator privileges can also open the VNE properties window from Prime Network Vision.

**Step 2** Click the Polling tab and go to the Polling Method area.

**Step 3** Click **Supported on selected devices only** to list the device types that support reduced polling, as shown in Figure 22-3, and verify it against the VNE device type.
Selecting the Reduced Polling Mechanism for an Individual VNE

Prime Network supports reduced polling on certain devices. You can list the device types in the VNE Properties dialog box, as shown in Figure 22-3. If you are not sure whether or not to use reduced polling, select Default for device type. Prime Network will match the device type with the best reduced polling option.

The risk of using reduced polling applies mostly to situations where events are dropped. In that cases, changes may be detected later than they would have if regular polling were being used.

If you try to apply reduced polling to a device type that does not support it, the VNE will stop modeling when it detects the misconfiguration, and it will issue a Device Unsupported Service event. If you look at the event description will explain that the polling method is not supported.

Make sure that devices have been properly configured to receive syslogs. See Syslogs—Required Device Settings, page A-13.

Note
For ASR 5000 Series devices, reduced polling works by polling all the registrations when the config change trap is received from the device. A device does not send the config change trap immediately after the configuration is changed, due to which there will be delay in updating the device configuration in VNE.
To apply reduced polling to an existing VNE:

**Step 1** Verify that the device type supports reduced polling by following the procedure in Finding Out Whether a Device Type Supports Reduced Polling, page 22-5.

**Step 2** Select a device (for example, using Prime Network Vision map view or properties view, or Prime Network PathTracer). Right-click the device and select Properties, then click the VNE button.

For a new VNE, follow the procedure in Adding VNEs, page 19-11, and specify reduced polling when you set the polling options (see VNE Polling Settings, page 19-40). This setting does not affect the initial discovery of the device.

**Step 3** Double-click the VNE to open the VNE Properties dialog box.

**Step 4** Click the Polling tab and go to the Polling Method area.

**Step 5** Select the polling method, as shown in Figure 22-4.

---

**Note** We recommend that you select Default for device type. Prime Network will match the VNE with the most efficient option for modeling the device type. You can override the default but should only do so after careful consideration.

---

**Step 6** If you do not want Prime Network to select the best polling approach, you can specify the reduced polling method, but keep in mind that you should balance model fidelity (more polling cycles) and high system performance (less polling cycles).

a. Verify that the device type supports reduced polling by clicking Supported on selected devices only link.

b. Specify whether you want the VNE to poll the device in response to device events, by selecting a method from the Dependency on Events for Model Updates dropdown list:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default for device type</td>
<td>Allows Prime Network to determine the best polling strategy. Prime Network makes a choice based on the level of support for the device driver, and the recommended offset of model fidelity vs. interference.</td>
</tr>
</tbody>
</table>
Chapter 22 Customizing VNE Polling

Reduced Polling

Step 7

Restart the VNE by right-clicking it and choosing Stop. When the Status changes to Down, right-click the VNE and choose Start.

Advanced Customizations: Reduced Polling

The preferred method for customizing reduced polling settings is to use the GUI client, as described in Selecting the Reduced Polling Mechanism for an Individual VNE, page 22-6. However, for bulk changes, using the GUI is prohibitive since you would have to repeat the same procedure multiple times. The following procedure explains how to customize reduced polling for all VNEs of the same type:

- Configuring Reduced Polling for All VNEs of the Same Device Type, page 22-8

Note

When making changes to all VNEs of the same type, make these changes during a maintenance window so you can test the changes locally and then restart the entire system to apply your changes throughout the system.

In addition, these procedures allow you to further extend the reliability of the reduced polling mechanism by ensuring that no events are missed and that commands are not repeatedly executed:

- Enabling the Reduced Polling Throttling Mechanism, page 22-12
- Enabling the Reduced Polling Fail-safe Option, page 22-14

Configuring Reduced Polling for All VNEs of the Same Device Type

The following procedure explains how to apply reduced polling to a device type rather than to individual VNEs. It includes steps for verifying the setting on a VNE before applying it to a device type. Finally, it also explains how to “undo” the procedure and revert back to the Prime Network defaults for a device type.

Before you set a reduced polling mechanism for a device type, consider the following points.

- Because this is a bulk change, carefully weigh the effect of using reduced polling on all device type instances, including those that will be created in the future. (You can always revert back to the original settings, as described in the procedure at the end of this topic.).
- Your customizations will take precedence over the factory defaults. For example, if you later apply an update that uses a different setting, your changes will override the settings in the update.
- If the device type uses more than one scheme, you must apply the change to both schemes (Product and IpCore).
- Test the changes in a staging setup before moving to the production environment, as you should for any customization that affects multiple VNEs.
- This change requires the `runRegTool.sh` script to perform customization on an unofficial Prime Network registry interface and as such subject to change.

To customize the reduced polling setting for a device type:

**Step 1** Create a new VNE (see Adding VNEs, page 19-11) or modify an existing VNE.

**Step 2** Verify that the Investigation State is Operational. This indicates that the VNE has completed its discovery.

**Figure 22-5 Verifying a VNE Investigation State**

**Step 3** Configured the VNE to use reduced polling.
   a. Verify that the device type supports reduced polling. See Finding Out Whether a Device Type Supports Reduced Polling, page 22-5. If it is not supported, you cannot use this procedure.
   b. Set the VNE’s polling method to reduced polling. See Selecting the Reduced Polling Mechanism for an Individual VNE, page 22-6.

**Step 4** Restart the VNE.

**Step 5** Confirm that the device is properly configured by checking the Device Configuration Tasks for VNE Creation, page A-1, paying special attention to event forwarding and configuration archive logging. If you have to make any device changes, do so and then restart the VNE.
Chapter 22 Customizing VNE Polling

**Step 6** Repeat Step 2 to verify that the VNE is in the Operational investigation state and has completed discovery.

**Step 7** Verify that the device has been properly discovered:

a. Compare the device inventory to the configuration on the device using the GUI client and/or BQL.

b. Check the Cisco Prime Network 3.9 Reference Guide and the Addendum: Additional VNE Driver Support for Cisco Prime Network 3.9 for supported technologies, events, and applications, and make sure they are working as expected. (The addendum becomes available when the first Device Package is released; see What Are Independent VNE Drivers and Device Packages?, page 21-1.)

**Step 8** Restart the VNE.

**Step 9** Get the registry data you will need to apply the changes to the device type. You will use as a basis the VNE you configured in Step 1 through Step 7.

a. Log into the gateway as network user and change to the Main directory by entering the following command. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

   ```
   cd $ANAHOME/Main
   ```

b. Get the device type and scheme details for the VNE from the registry, where unit-IP is the unit IP address, avmxxx is the AVM ID, vne-key is the VNE name:

   ```
   .runRegTool.sh -gs 127.0.0.1 get -key unit-IP "avmxxx/agents/da/vne-key" | grep default | head -n 1
   ```

   If you are running this command from the gateway server, unit-IP should be 127.0.0.1. In this example, the AVM is AVM 600, and the VNE key is c7-npe1-76.

   ```
   .runRegTool.sh -gs 127.0.0.1 get -key 127.0.0.1 "avm600/agents/da/c7-npe1-76" | grep default | head -n 1
   <entry name="default">cisco2/cisco7604/ipcore/software versions/gt 12.2(33)SRE</entry>
   ```

c. Identify the scheme by checking for product or ipcore. In this example, the scheme is ipcore.

   ```
   <entry name="default">cisco2/cisco7604/ipcore/software versions/gt 12.2(33)SRE</entry>
   ```

d. Identify the device type by checking the prefix that appears before the scheme. In this case, the prefix is cisco2/cisco7604.

   ```
   <entry name="default">cisco2/cisco7604/ipcore/software versions/gt 12.2(33)SRE</entry>
   ```

**Step 10** Verify that reduced polling is not enabled on the device type:

```
./runRegTool.sh -gs 127.0.0.1 get -entry unit-IP "site/device-type/reduced-polling"
```

In this example, the device-type is cisco2/cisco7604:

```
./runRegTool.sh -gs 127.0.0.1 get -entry 127.0.0.1 "site/cisco2/cisco7604/reduced-polling" false
```

The output of the command (false) shows that reduced polling is not enabled for this device type.

**Step 11** Change the device type’s default setting so that reduced polling is enabled. If you are running this command on the gateway server, unit-IP should be 0.0.0.0.

```
./runRegTool.sh -gs 127.0.0.1 set unit-IP "site/device-type/reduced-polling" true
```

In this example, the device-type is cisco2/cisco7604:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/cisco2/cisco7604/reduced-polling" true
```
Step 12 For existing VNEs, reinitiate the discovery process to collect the required NE-level data.

a. Generate a list of all affected VNEs. You will have to perform this operation on all unit servers—that is, all avmxxx.xml files that are under NETWORKHOME/Main/registry/ConfigurationFiles/*.

```
# cd $ANAHOME/Main/registry/ConfigurationFiles
# grep "reduced polling" */avm*.xml | more
```

b. Reinitiate the discovery process on all VNEs that are using reduced polling. If you are running this command on the gateway server, unit-IP should be 127.0.0.1.

```
# cd $ANAHOME
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP "avmxxx/agents/da/vne-key/default" agentdefaults/da
```

For our original VNE with AVM 600, and VNE key c7-npe1-76.

```
# ./runRegTool.sh -gs 127.0.0.1 set 127.0.0.1 "avm600/agents/da/c7-npe1-76/default" agentdefaults/da
```

Step 13 Restart Prime Network to apply the override for the device type setting to all VNEs.

Step 14 After Prime Network has restarted, check existing VNEs to ensure the change was applied.

Step 15 Verify the reduced polling settings are also applied to new VNEs:

a. Create a new VNE or modify an existing VNE (see Step 1 and Step 2) and verify that it is Operational.

b. Verify that a VNE is using the new value for reduced polling. If you are running this command on the gateway server, unit-IP should be 127.0.0.1.

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 get -entry unit-IP
"avmxxx/agents/da/vne-key/reduced-polling"
```

In this example, the unit IP address is 10.56.57.72, the AVM is AVM 850, and the VNE key is c3-70.

```
# ./runRegTool.sh -gs 127.0.0.1 get -entry 10.56.57.72
"avm850/agents/da/c3-70/reduced-polling"
true
```

The output of the command (true) shows that reduced polling is enabled on this VNE.

c. Verify that the reduced polling is being used on the VNE because of the default setting for the device type. If you are running this command on the gateway server, unit-IP should be 127.0.0.1.

```
# ./runRegTool.sh -gs 127.0.0.1 get -key unit-IP "avmxxx/agents/da/vne-key" | grep reduced-polling
```
Using the same VNE (c3-70):

```bash
# ./runRegTool.sh -gs 127.0.0.1 get -key 10.56.57.72 "avm850/agents/da/c3-70/" | grep reduced-polling
#
The command gives no output, which indicates that reduced polling is enabled, but not due to a configuration on the specific VNE; therefore, the setting is coming from the default for the device type.
```

To revert to the Prime Network defaults for a device type—in other words, to cancel the override value specified in the previous procedure—use the `unset` command.

**Note**

After setting the reduced-setting key to `true`, do not set it to `false` to “undo” the change. Doing so will instruct the system to use regular polling for the device type. While that may be acceptable, you will still override the default system setting (which is to not specify the reduced-polling key as true or false).

**Step 1**

Get the registry data you will need to apply the changes to the device type (see Step 9 in the previous procedure).

**Step 2**

Run the following command to unset the override on the device type:

```bash
# ./runRegTool.sh -gs 127.0.0.1 unset unit-IP "site/device-type/reduced-polling" true
```

For the previous example, where the `device-type` was `cisco2/cisco7604`, you would use this command:

```bash
# ./runRegTool.sh -gs 127.0.0.1 unset 0.0.0.0 "site/cisco2/cisco7604/reduced-polling"
```

**Step 3**

Verify that reduced polling is not enabled on the device type by repeating Step 10 of the previous procedure.

---

**Enabling the Reduced Polling Throttling Mechanism**

In case VNE that is using reduced polling receives multiple configuration change syslogs from the same device in a short time span, a throttling mechanism can be used to prevent the same command from being executed repeatedly. The throttle mechanism collects all change notifications that are received within a predefined interval, and when the interval expires, the VNE polls the device for updated information at one time. The throttle feature is turned off by default (the interval is set to 0). If a change is not immediately reflected in Prime Network Vision because the throttle is enabled, you can manually update the GUI using the Poll Now button (see Figure 22-1).

The interval should allow enough time for the change to be applied, including being applied to other affected devices. In the following example we change the interval to five minutes. This may not be a suitable interval in the following scenarios:

- If multiple large configuration changes are bulked and run over a period of time, a larger interval might reduce CPU usage.
- If multiple small configurations are run throughout the day, a smaller interval would be appropriate because it would reflect the changes more quickly.

The throttling mechanism should be applied to either specific VNEs or a device types. The following procedures explain how to enable the throttling mechanism for a specific VNE and for all VNEs of the same device type.
Reduced Polling

Changing Settings for a Specific VNE

To check, enable, or disable the throttling mechanism for an individual VNE, use the following procedure.

Step 1
Log into the gateway as network user and change to the Main directory by entering the following command. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

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

Step 2
For a VNE where unit-IP is the unit IP address, avmxxx is the A VM ID, vne-key is the VNE name, use the following commands. If you are running this command on AVMs that are on the gateway server, unit-IP should be 127.0.0.1.

- To check whether throttling is enabled (and an interval is set):
  
  ```
  # ./runRegTool.sh -gs 127.0.0.1 get -entry unit-IP "avmxxx/agents/da/vne-key/evne polling interval"
  ```

- To set the throttling interval to minutes:
  
  ```
  # ./runRegTool.sh -gs 127.0.0.1 set unit-IP "avmxxx/agents/da/vne-key/evne polling interval" minutes
  ```

- To unset (disable) the throttling interval:
  
  ```
  # ./runRegTool.sh -gs 127.0.0.1 unset unit-IP "avmxxx/agents/da/vne-key/evne polling interval"
  ```

For example, this command would set the throttling interval to 5 minutes for a VNE named c7-npe1-76 on AVM 600, and would make the change to the Golden Source registry:

```
# ./runRegTool.sh -gs 127.0.0.1 set 127.0.0.1 "avm600/agents/da/c7-npe1-76/evne polling interval" 5
```

Step 3
Restart the VNE.

Changing Settings for a Device Type

To enable the throttling mechanism for a device type, use this procedure. You will have to restart the gateway server; then your changes will be applied to all VNEs of that device type.

Note
If you change the settings for a device type, you will have to restart Prime Network to apply your changes.

You will need the following information for a VNE of the device type:

- The VNE IP address (for example, 10.56.101.163)
- The AVM number (for example, A VM 751)
- The unit IP address (for example, 10.56.57.72)
To change the settings for a device type:

**Step 1** Log into the gateway as network user and change to the Main directory by entering the following command. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

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

**Step 2** To find the device type registry location, locate the information for a VNE of that device type. Get the registry data you will need to apply the changes to the device type (see Step 9 in the procedure Configuring Reduced Polling for All VNEs of the Same Device Type, page 22-8). For example:

**Step 3** Use these commands to check, set, and unset throttling.

- To check whether throttling is enabled (and an interval is set):
  
  ```
  # ./runRegTool.sh -gs 127.0.0.1 get -entry 127.0.0.1 "site/device-type/evne polling interval"
  ```

- To set the throttling interval to minutes:
  
  ```
  # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/device-type/evne polling interval"
  ```

- To unset (disable) the throttling interval:
  
  ```
  # ./runRegTool.sh -gs 127.0.0.1 unset 0.0.0.0 "site/device-type/evne polling interval"
  ```

For example, if the device-type is cisco2/cisco7604, this command would set the throttling interval to 5 minutes for all Cisco 7604 VNEs (and would make this change to the Golden Source registry):

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/cisco2/cisco7604/evne polling interval" 5
```

**Step 4** Restart the gateway server:

```
# networkctl restart
```

**Enabling the Reduced Polling Fail-safe Option**

Because syslogs are not always reliable, the reduced polling mechanism provides a fail-safe option that polls the device’s complete command history to identify any new configuration commands that were missed as well as to identify what changed so that the model can be updated accordingly. If an event is dropped due to some extreme conditions, it could result in a VNE that is not synchronized with its network element; and if the VNE was using the system interval for polling updates, it could remain unsynchronized for up to 24 hours.

This option is only applicable to VNEs that have a high dependency on events to update the model. It is turned off by default.

The fail-safe option setting should be the same for all devices; that is, it should be enabled or disabled for all devices.
To enable the fail-safe option:

---

**Step 1**  
Try changing the throttling interval as described in Enabling the Reduced Polling Throttling Mechanism, page 22-12. You should test both a shorter and longer interval.

**Step 2**  
Use one of the following commands depending on your device OS. The fail-safe option is disabled (configuration polling is not set) by default:

- For Cisco IOS devices:
  
  ```
  # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
  "site/cisco-router-repository-evne/archive-log-telnet/instrumentation
  services/interval" configuration
  ```

- For Cisco IOS XR devices:
  
  ```
  # ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
  "site/cisco-router-iox-repository-evne/archive-log-telnet/instrumentation
  services/interval" configuration
  ```

**Step 3**  
Restart the gateway server.

---

**Adaptive Polling**

Adaptive polling is a feature that preserves device integrity in extreme network scenarios or when encountering device caveats. When device CPU is exceedingly and consistently high, it introduces an interval between SNMP/CLI commands so that the device can quickly recover. In addition, some devices with exceptionally large configurations can generate very large Telnet responses—literally thousands of output lines. Because these are single, atomic commands, other techniques such as smooth polling cannot be applied.

If this occurs, the adaptive polling mechanism defines a limited terminal length, breaking the response into segments, inserts a delimiter (such as --More--), and does not resume until the VNE sends a space character. This technique is sometimes called *flow control*. During the pause, the network element can address other priorities. This ensures that the network element CPU utilization is not monopolized by Prime Network polling commands. Although the duration of these polling commands will be slightly longer, this is normally a desirable tradeoff.

The XML protocol also supports adaptive polling due to the fact that XML is a protocol that is handled over Telnet. Although adaptive polling is not formally supported over HTTP, because other (non-HTTP) protocols are involved in data collection, an overall improved result is also seen for HTTP.

---

**Note**  
In earlier releases, a postlogin command could be used to specify the terminal length and width. This should no longer be done because these commands have their own dedicated registry entries, as shown in Table 22-3.

---

**Figure 22-6** illustrates the adaptive polling mechanism.

---

**Note**  
In Figure 22-6, the term *slow polling* does not refer to the preconfigured polling group called *slow*, that is described in Table 22-4 on page 22-24.
Figure 22-6  How Adaptive Polling Works

The following steps provide more detail about the adaptive polling algorithm illustrated in Figure 22-6.

1. When a normal polling VNE exceeds the maximum CPU usage threshold value for five consecutive polls, it is moved to slow polling.

   Slow polling introduces a delay is added between sending the commands to the NE. (In SNMP, the delay is between SNMP packets sent to the device; in Telnet or SSH, the delay is between CLI commands sent to the device.) In addition, Telnet responses are divided into smaller parts, separated by a delimiter to adjust throughput.

2. A slow polling VNE can do either of the following, depending on CPU usage polling results:
   - If CPU usage is below the minimum threshold level for two consecutive polls, the VNE returns to normal polling.
   - If CPU usage exceeds the maximum threshold for five additional consecutive polls (a total of ten polls), the VNE moves to CPU-only polling.
      
      All polling is suspended except for CPU usage; however, syslogs and traps continue to be processed. The VNE is moved to the Currently Unsynchronized VNE investigation state.

3. When a CPU-only polling VNE has CPU usage that is below the minimum threshold level for two consecutive polls, it returns to normal polling.

   Figure 22-7 shows the an example of what you will see in Prime Network Events and Prime Network Vision when a VNE is experiencing high CPU usage. (The VNE Status Details window is launched from Prime Network Vision by clicking VNE Status from the device properties window.)
If a VNE keeps moving from normal to slow polling to CPU-only polling, consider adjusting the thresholds that control adaptive polling. See Changing Adaptive Polling Thresholds and Delimiters, page 22-21.

**Note**

If a parent AVM is stopped during this process, the VNE retains its previous polling data. When the AVM is restarted, the VNE continues from the point at which its polling was interrupted. See Instrumentation Persistency, page 26-6.

**Basic Customizations: Adaptive Polling**

These topics provide procedures that explain how to configure adaptive polling using the GUI, and how to turn off adaptive polling:

- Configuring Adaptive Polling Settings Using the GUI Client, page 22-17
- Turning Off Adaptive Polling, page 22-18

**Configuring Adaptive Polling Settings Using the GUI Client**

The following procedure is the preferred method for configuring adaptive polling settings for a VNE. You can specify your settings in the VNE Properties dialog box.

**Step 1**
Select the required gateway or unit and AVM in the navigation tree.

**Step 2**
Right-click the AVM, then choose **New VNE**. The New VNE dialog box is displayed, opened to the General tab. Complete the dialog as described in Creating VNEs for New Device Types, page 19-21. If you are updating an existing VNE, select the VNE and right-click **Properties**.
Step 3 Configure adaptive polling for the VNE by clicking the Polling tab. The adaptive polling settings are at the bottom of the dialog box.

Note The Enable check box must be checked for adaptive polling to be activated.

a. Select the settings you want the adaptive polling mechanism to use.

<table>
<thead>
<tr>
<th>Adaptive Polling Choice</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Network Settings</td>
<td>Use the settings chosen by Prime Network.</td>
</tr>
<tr>
<td>Device Type Settings</td>
<td>Use the settings specified for this device type (as delivered with Prime Network). If no setting exists for the device type, the Prime Network Settings are used.</td>
</tr>
<tr>
<td>Local Settings</td>
<td>Specify your own settings, overriding the defaults. The settings are applied to this VNE only.</td>
</tr>
</tbody>
</table>

b. If you select Local Settings, enter values in the Upper and Lower Threshold fields:
   - Upper Threshold—When CPU usage exceeds this value for 5 polls, the adaptive polling mechanism is triggered. The VNE switches to slow polling or CPU-only polling. (See Figure 22-6 on page 22-16.
   - Lower Threshold—When CPU usage drops below this value for 2 polls, the VNE moves back to normal polling and related alarms are cleared.

Step 4 If you are editing an existing VNE, click Apply and restart the VNE for your changes to take effect.
If you are creating a new VNE, click OK to create the new VNE, or continue with the VNE configuration.

Turning Off Adaptive Polling

Step 1 Select the required gateway or unit and AVM in the navigation tree.
Step 2 Select the VNE and right-click Properties.
Step 3 Uncheck the Enable check box, and save and restart the VNE.

Advanced Customizations: Adaptive Polling

The following advanced procedures explain how to change polling intervals and other adaptive polling delimiters, such as the delays that are introduced between commands:

- Changing the CPU Usage Polling Interval and Other Settings, page 22-19
- Changing Adaptive Polling Thresholds and Delimiters, page 22-21

Note We recommend that you adjust adaptive polling settings using the GUI client, as described in Basic Customizations: Adaptive Polling, page 22-17.
Chapter 22  Customizing VNE Polling

Adaptive Polling

Changing the CPU Usage Polling Interval and Other Settings

The command for retrieving CPU utilization data is sent to the device according to the interval setting in Table 22-2. Therefore, if Prime Network reports a high CPU utilization on a VNE, it means that for last 5 CPU polls, the average CPU utilization has been crossing the recommended threshold.

For example, the CPU usage information for some devices is gathered using the following command (other devices may use SNMP):

```
show processes cpu include CPU utilization
```

Table 22-2 lists the parameters that control how often the data is polled. Complete directory paths to the registry entries are provided in the procedure that follows the table.

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interval</strong></td>
<td>How often (milliseconds) to poll the CPU usage when determining the average usage.</td>
<td><strong>IOS XR</strong> 60000 (1 min)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>IOS</strong> 30000 (30 secs)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cat OS</strong> 30000 (30 secs)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NX-OS</strong> 30000 (30 secs)</td>
</tr>
<tr>
<td><strong>cpu-util-counter-bucket</strong></td>
<td>(Cisco IOS XR only) Parameter for CPU measurement (see examples below)</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>IOS</strong> N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cat OS</strong> N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NX-OS</strong> N/A</td>
</tr>
</tbody>
</table>

**Example for Cisco IOS XR Devices**

As shown in Table 22-2, Prime Network provides a cpu-util-counter-bucket variable to calculate average CPU usage for Cisco IOS XR devices. The following table provides examples of values you might see for the same interval setting, but with different cpu-util-counter-bucket settings.

<table>
<thead>
<tr>
<th>cpu-util-counter-bucket Setting</th>
<th>If <code>interval=1 minute</code>, CPU usage is checked every:</th>
<th>Hypothetical CPU average usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 x <code>interval</code> = 1 minute</td>
<td>10%</td>
</tr>
<tr>
<td>5</td>
<td>5 x <code>interval</code> = 5 minutes</td>
<td>16%</td>
</tr>
<tr>
<td>15</td>
<td>15 x <code>interval</code> = 15 minutes</td>
<td>14%</td>
</tr>
</tbody>
</table>

With a cpu-util-bucket-counter setting of 5, the adaptive polling mechanism would recognize average CPU usage on the device to be 16%.

The following procedures explain how to enable the throttling mechanism for a specific VNE and for all VNEs of the same device type.

**Changing Settings for a Specific VNE**

Use the following procedure to adjust how often CPU utilization is polled by a specific VNE.

Note

Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative. For information on the format of the `runRegTool.sh` script, see Changing Registry Settings Using `runRegTool.sh`, page C-2.
Step 1
Log into the gateway as network user and change to the Main directory by entering the following command. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

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

**Note** In the following examples, the changes are first applied to individual VNEs. We recommend this approach, before applying changes to a device type (which will affect all VNEs of that type).

Step 2
To change the current CPU polling interval for an individual VNE, where avmxxx is the AVM ID, vne-key is the VNE name, and unit-IP is the IP address of the unit where the AVM resides (if you are running this command on AVMs on the gateway server, unit-IP should be 127.0.0.1):

- To change the default polling interval to 60000 milliseconds (60 seconds, the recommended interval for Cisco IOS XR devices):

  ```
  # ./runRegTool.sh -gs 127.0.0.1 set unit-IP "avmxxx/agents/da/vne-key/dcs
  /registrations/com.sheer.metrocentral.coretech.common.dc.ManagedElement/cpu
  usage/instrumentation services/interval" 60000
  ```

- To change the default polling interval to 30000 milliseconds (30 seconds, the recommended interval for Cisco IOS and Cisco Cat OS devices):

  ```
  # ./runRegTool.sh -gs 127.0.0.1 set unit-IP "avmxxx/agents/da/vne-key/dcs
  /registrations/com.sheer.metrocentral.coretech.common.dc.ManagedElement/cpu
  usage/instrumentation services/interval" 30000
  ```

Step 3 (Cisco IOS XR devices only) To change the number of times to poll a device to 15, where avmxxx is the AVM ID on the gateway server, vne-key is the VNE name:

```
# ./runRegTool.sh -gs 127.0.0.1 set 127.0.0.1 "avmxxx/agents/da/vne-key/dcs
/registrations/com.sheer.metrocentral.coretech.common.dc.ManagedElement/cpu
usage/instrumentation services/command/parsing params/cpu-util-counter-bucket" 15
```

Step 4 Restart the VNE for your changes to take effect.

**Changing Settings for A Device Type**

To apply a change to a device type, use this procedure. You will have to restart the gateway server; then your changes will be applied to all VNEs of that device type.

You will need the following information for a VNE of the device type:

- The VNE IP address
- The AVM number
- The unit IP address
To change the adaptive polling settings for a device type:

### Step 1
Log into the gateway as network user and change to the Main directory by entering the following command. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

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

### Step 2
To find the device type registry location, locate the information for a VNE of that device type. Follow the procedure in Step 9 of Configuring Reduced Polling for All VNEs of the Same Device Type, page 22-8.

For example, the following is the typical output you would get from the procedure. The device-type information is in bold.

```xml
<entry name="default">cisco2/catalyst494810GE/product/software versions/gt 12.2(53)SG/ip_default</entry>
```

### Step 3
Use the following command to apply your change to the device type, substituting the location information for device-type (unit-IP is the IP address of the parent unit to the VNE; if you are running this command on the gateway server, unit-IP should be 0.0.0.0):

```bash
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP "site/device-type/dcs/registrations/com.sheer.metrocentral.coretech.common.dc.ManagedElement/cpuusage/instrumentation services/interval" 60000
```

In the following example, a new interval is applied to all Catalyst 494810GE switches (unit-IP is the IP address of the parent unit to the VNE):

```bash
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP "site/cisco2/catalyst494810GE/product/software versions/gt 12.2(53)SG/ip_default/dcs/registrations/com.sheer.metrocentral.coretech.common.dc.ManagedElement/cpuusage/instrumentation services/interval" 60000
```

### Step 4
Restart the gateway server:

```bash
# networkctl restart
```

---

**Changing Adaptive Polling Thresholds and Delimiters**

Table 22-3 describes the registry parameters (and default values) for adaptive polling for Cisco VNEs.

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Indicates whether adaptive polling is enabled on the VNE. Can also be set using the GUI; see VNE Polling Settings, page 19-40.</td>
<td>true</td>
</tr>
<tr>
<td>snmp_delay</td>
<td>Delay (in milliseconds) between SNMP commands that are sent from the VNE to the device.</td>
<td>500</td>
</tr>
<tr>
<td>telnet_delay</td>
<td>Delay (in milliseconds) between Telnet commands that are sent from the VNE to the device.</td>
<td>500</td>
</tr>
<tr>
<td>telnet_delimiter_delay</td>
<td>Delay (in milliseconds) the VNE must wait before sending a space character to the NE, in order to retrieve the next part of a long Telnet response that is delimited.</td>
<td>300</td>
</tr>
</tbody>
</table>
Chapter 22  Customizing VNE Polling

Adaptive Polling

The following procedure explains how to check the current adaptive polling settings for a VNE, and how to adjust a VNE so that adaptive polling problems are handled more conservatively.

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

**Step 1**  Log into the gateway as *network user* and change to the Main directory by entering the following command. (*network user* is the operating system account for the Prime Network application, created when Prime Network is installed; for example, *network39*).

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

**Step 2**  To view the current adaptive polling settings for an individual VNE, where *unit-IP* is the unit IP address for the AVM, *avmxxx* is the AVM ID, *vne-key* is the VNE name, use the following command (if you are running this command on AVMs on the gateway server, *unit-IP* should be 127.0.0.1):

```bash
# ./runRegTool.sh -gs 127.0.0.1 get unit-IP
"avmxxx/agents/da/vne-key/dcs/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/AdaptivePolling/registry-entry"
```

For example, to check the maintenance_tolerance setting for VNE c7-sw7 on AVM 600 on the gateway server:

```bash
# ./runRegTool.sh -gs 127.0.0.1 get 127.0.0.1
"avm600/agents/da/c7-sw7/dcs/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/AdaptivePolling/maintenance_tolerance"
```

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal_length</td>
<td>Terminal length to use when VNE is moved to slow polling.</td>
<td>512</td>
</tr>
<tr>
<td>threshold alarm value</td>
<td>Upper threshold (%) at which to move VNE to slow polling. Can also be set using the GUI; see VNE Polling Settings, page 19-40.</td>
<td>90</td>
</tr>
<tr>
<td>threshold clear value</td>
<td>Lower threshold (%) at which to move VNE to normal polling. Can also be set using the GUI; see VNE Polling Settings, page 19-40.</td>
<td>60</td>
</tr>
<tr>
<td>low_tolerance</td>
<td>When CPU utilization falls below the lower threshold for this number of consecutive polls, move the VNE to normal polling.</td>
<td>2</td>
</tr>
<tr>
<td>upper_tolerance</td>
<td>When upper threshold is crossed this number of consecutive CPU polls, move the VNE to slow polling. (Using the settings in this table and in Table 22-2, this means the VNE would move to slow polling after 5 minutes.)</td>
<td>5</td>
</tr>
<tr>
<td>maintenance_tolerance</td>
<td>When upper threshold is crossed this number of consecutive CPU polls, move the VNE to CPU-only polling. (This number includes the 5 polls in the lower tolerance. See Figure 22-6 on page 22-16 for an example of this configuration.)</td>
<td>10</td>
</tr>
</tbody>
</table>

The following procedure explains how to check the current adaptive polling settings for a VNE, and how to adjust a VNE so that adaptive polling problems are handled more conservatively.

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

**Step 1**  Log into the gateway as *network user* and change to the Main directory by entering the following command. (*network user* is the operating system account for the Prime Network application, created when Prime Network is installed; for example, *network39*).

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

**Step 2**  To view the current adaptive polling settings for an individual VNE, where *unit-IP* is the unit IP address for the AVM, *avmxxx* is the AVM ID, *vne-key* is the VNE name, use the following command (if you are running this command on AVMs on the gateway server, *unit-IP* should be 127.0.0.1):

```bash
# ./runRegTool.sh -gs 127.0.0.1 get unit-IP
"avmxxx/agents/da/vne-key/dcs/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/AdaptivePolling/registry-entry"
```

For example, to check the maintenance_tolerance setting for VNE c7-sw7 on AVM 600 on the gateway server:

```bash
# ./runRegTool.sh -gs 127.0.0.1 get 127.0.0.1
"avm600/agents/da/c7-sw7/dcs/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/AdaptivePolling/maintenance_tolerance"
```
Step 3  
To change the adaptive polling settings for VNE on the gateway server, so that its CPU utilization problems are tracked even more carefully than the default behavior:

- Instead of 5 polls, the VNE moves to slower polling after 3 consecutive polls above the threshold:
  
  
  ```bash
  # ./runRegTool.sh -gs 127.0.0.1 set 127.0.0.1
  "avm600/agents/da/c7-sw7/dcs/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/AdaptivePolling/upper_tolerance" 3
  ```

- Instead of 2 polls, the VNE moves back to normal polling after 5 consecutive polls below the threshold:
  
  ```bash
  # ./runRegTool.sh -gs 127.0.0.1 set 127.0.0.1
  "avm600/agents/da/c7-sw7/dcs/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/AdaptivePolling/lower_tolerance" 5
  ```

- Instead of 90%, the VNE high CPU threshold is 70%:

  **Note**  
  You can also use the GUI client to change the threshold setting, as described in Configuring Adaptive Polling Settings Using the GUI Client, page 22-17.

  ```bash
  # ./runRegTool.sh -gs 127.0.0.1 get 127.0.0.1
  "avm600/agents/da/c7-sw7/dcs/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/AdaptivePolling/threshold_alarm_value" 70
  ```

Step 4  
Restart the VNE to apply your changes.

---

### VNE Polling Groups and Slow Polling

Prime Network VNEs poll the network element in a repetitive fashion according to a predefined time interval, referred as a polling cycle. For queries that affect device CPU, a higher repetition of these queries will result in longer CPU peaks and higher average CPU utilization over time. On the other hand, long intervals may result in changes that are not reflected, and go unnoticed until the next polling interval.

Users can fine-tune the frequency at which information is retrieved from the managed elements, thus controlling the amount of network traffic used by the various VNEs. These intervals are controlled by Prime Network polling groups which are configured using Prime Network Administration.

For example, these are cases where a polling group with a longer polling interval would be useful:

- Define a core-device polling group with a long interval for configuration changes, because core devices seldom undergo configuration changes. Access devices, which are more likely to adjust to service provisioning changes, would have a shorter interval. This enables you to differentiate the same device type based on the device role.

- Define a group for legacy architectures and in-band management, that has an overall long interval (slow polling cycle).

Prime Network provides the preconfigured polling groups default and slow (these groups cannot be deleted). Users can employ these or, alternatively, can define a new polling group, apply customized polling intervals to the group, and assign the polling group to managed elements. The VNE then polls the network element according to the preset values. This ensures polling of devices for different information consistently and in accordance with technical and business requirements.
Table 22-4 identifies the settings for the default and slow polling groups.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Preconfigured Polling Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The polling rate for status-related information, such as device status (up or down), CPU usage, port status, admin status, operational status.</td>
<td>default: 180 seconds (3 minutes)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration: 900 seconds (15 minutes)</td>
</tr>
<tr>
<td>Configuration</td>
<td>The polling rate for configuration-related information, such as IP address, device name and type; communication and investigation state; system name, description, location.</td>
<td>default: 86400 seconds (24 hours)</td>
</tr>
<tr>
<td>System</td>
<td>The polling rate for system-related information, such software version.</td>
<td></td>
</tr>
<tr>
<td>Layer 1</td>
<td>The polling rate of the topology process as an interval for the Layer 1 counter. This is an ongoing process.</td>
<td>default: 90 seconds</td>
</tr>
<tr>
<td>Layer 2</td>
<td>The polling rate of the topology process as an interval for the Layer 2 counter. This process is available on demand.</td>
<td>default: 30 seconds</td>
</tr>
</tbody>
</table>

**How to Create a Customized Polling Groups**

In the following example, a new polling group is created that polls for all device information every 24 hours. The polling group is then applied to a new VNE.

**Step 1** Choose Global Settings > Polling Groups.

**Step 2** Open the New Polling Group dialog box by right-clicking Polling Groups, then choose New Polling Group.

**Step 3** Complete the New Polling Group dialog. Figure 22-8 provides an example of the new 24-hour polling group.
Figure 22-8 Creating a Polling Group Called 24 Hrs Cycle

The following table describes the fields in this dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the polling group.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the polling group.</td>
</tr>
<tr>
<td>Polling Intervals</td>
<td>Number of seconds between collections of status-related information.</td>
</tr>
<tr>
<td>Status</td>
<td>Configuration Number of seconds between collections of configuration-related information.</td>
</tr>
<tr>
<td>Configuration</td>
<td>System Number of seconds between collections of system-related information.</td>
</tr>
<tr>
<td>System</td>
<td>Layer 1 Number of seconds in the topology Layer 1 counter. This is an ongoing process.</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Number of seconds in the topology Layer 2 counter. This process is available on demand.</td>
</tr>
</tbody>
</table>

Step 4  Save the changes by clicking **OK**. The new polling group is displayed in the content area and will be displayed when users create new VNEs.

Step 5  To apply the new polling group to a new VNE, select the required gateway or unit and AVM in the navigation tree.
Step 6 Right-click the AVM, then choose New VNE. The New VNE dialog box is displayed, opened to the General tab.

Step 7 Complete the dialog as described in Creating VNEs for New Device Types, page 19-21. Apply the 24 hrs cycle polling group to the VNE by clicking the Polling tab and selecting 24 hrs cycle from the Polling Parameters Group dropdown list, as shown in Figure 22-9.

Figure 22-9 Applying the 24 Hrs Cycle Polling Group to a VNE

Step 8 Click OK. The new VNE is created, and it will poll the device according to the settings in the 24 hrs cycle polling group.

Smooth Polling

Each VNE uses device registrations (commands) to collect different kinds of data from the associated network element. Each registration specifies the commands required to obtain a specific given item of data, and can be configured with a specific polling interval or logically associated with one of the polling intervals on a per device/VNE basis.

The smooth polling mechanism that takes commands in the same polling cycle, and spreads their execution throughout the polling cycle. Rather than using a timer-based approach (where a large number of commands will be potentially scheduled for execution at the same time), the smooth polling method generates a random number (within the polling interval) for the next execution. This ensures that the commands get executed at least once within the required period, while also reducing the probability that two or more commands will run at the same time. This “smooths out” the load of the management protocols on the network and reduces their impact. Obviously, the longer the polling interval, the more effective smooth polling can be.

Note that smooth polling augments regular polling only after the completion of the first poll. Smooth polling is enabled in Prime Network by default.
How to Enable or Disable Smooth Polling

While it is rare that you will need to change the smooth polling setting, you can disable it if a VNE’s polling intervals are extremely small.

Note

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

Step 1

Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39), and change to the Main directory by entering the following command:

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

Step 2

Issue the appropriate command for a VNE where unit-IP is the unit IP address, avmxxx is the AVM ID, vne-key is the VNE name (if you are running this command on AVMs on the gateway server, unit-IP should be 127.0.0.1):

- To disable smooth polling:
  
  ```
  Note
  Disabling smooth polling will likely result in higher CPU usage.
  ```

  ```
  # ./runRegTool.sh -gs 127.0.0.1 set unit-IP
  "avmxxx/agents/da/vne-key/smoothpollingenabled" false
  ```

- To revert to the default setting (enabled):
  
  ```
  # ./runRegTool.sh -gs 127.0.0.1 unset unit-IP
  "avmxxx/agents/da/vne-key/smoothpollingenabled"
  ```

Step 3

Restart the VNE.

Smart Polling (On-Demand Polling)

When Prime Network receives an incoming notification about a model change, the event provides information about the change but not about other components that may be affected by the change. For this reason Prime Network polls for this information that can affect the VNE model.

Sometimes queries are repeatedly submitted to a device. Common cases for this are when a user opens a Prime Network Path Tracer, window, and when an expedited event is received by Prime Network. To prevent overpolling, the smart polling mechanism uses a polling protection interval that specifies the minimum amount of time that must pass before a query can be sent to a device a second time.

For example, if multiple GUI or BQL users are concurrently using Prime Network Path Tracer, if the paths being viewed have common network elements, the details are collected according to the smart polling interval, and the data is shared without performing duplicate polls.

This example shows how Prime Network uses smart polling when receiving multiple instances of an expedited event:

1. An incoming event notification is classified as an expedited event, so Query A is immediately sent.
2. A few milliseconds later, the same incoming event arrives on an adjacent interface, triggering Query A again.
If the interval was 10 seconds, and the second instance of Query A arrived 7 seconds after the first instance of Query A, the second query would be dropped.

For expedited queries, Prime Network will queue the query to run when the interval is complete. Using the previous example, suppose the first instance of the query arrived at 12:00:00. The second instance arrives at 12:00:07. Because the query is expedited, the second query is queued to run at 12:00:10 (10 seconds after the first query).

If you change the smart polling interval, keep the following in mind:

- If the interval is too short, Prime Network might report false alarms.
- If the interval is too long, Prime Network will not report current data.

Therefore, the interval value should be based on the amount of time required for the network to stabilize after a change.

---

**Note**

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

---

**Step 1**

Log into the gateway as `network user` (where `network user` is the operating system account for the Prime Network application, created when Prime Network is installed; for example, `network39`), and change to the Main directory by entering the following command:

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

**Step 2**

Issue the following command to change the polling-protection-interval for all commands from the default of 0 to `value` milliseconds. (The text that precedes this procedure provides general guidelines for specifying `value`.)

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/instrumentordefaults/baseCommand/polling-protection-interval" value
```

**Step 3**

Restart the gateway server:

```
# networkctl restart
```
Cloud VNEs represent unmanaged network segments that are connected to two or more managed segments. This prevents interruptions to alarm correlations and affected subscribers for the managed segments.

These topics describe how to add and remove links between two ports of two network elements in the network that are connected to some unmanaged network segment through a Cloud VNE. Dynamic links are used to connect these ports to a cloud.

Static links override any existing autodiscovered topology in the system. A static link is identical in all respects to a link that is autodiscovered.

- Unmanaged Segments and Cloud VNEs, page 23-1
- Creating and Deleting Static Links, page 23-8

Unmanaged Segments and Cloud VNEs

Three types of technology simulations are supported for Cloud VNEs: Frame Relay, ATM, and Ethernet. If you want to work with Cloud VNEs with Ethernet support, see Ethernet on Cloud VNEs, page 23-2.

Administrators can create Cloud VNEs that represent:

- A single device to which two or more managed segments of the network can be connected. In this case, the Cloud VNE builds a model with port type and technology that is identical to its adjacent VNEs and virtual forwarding components. Each physical port in a VNE can connect to only one Cloud VNE.
- Multiple unmanaged segments and multiple technologies, as long as each technology is in a different network segment.
- Multiple Cloud VNEs, each one representing a portion of an unmanaged network.

All VNEs can also be configured to connect dynamically to a Cloud VNE. When loading, the VNE gathers whatever data is relevant to the Cloud VNE, and sends the data to it. Upon receiving this information, the Cloud VNE builds the corresponding model to allow the topology to connect the two VNEs.
To create a Cloud VNE, you must do the following:

1. Create the VNE using Prime Network Administration. You only have to provide a name for the VNE. No additional protocols need to be configured for the Cloud VNE. See Adding VNEs, page 19-11.

2. Connect the cloud VNE to a device, which will automatically populate the Cloud VNE with technology and topology information. See Connecting the Cloud VNE to a Device, page 23-3.

---

**Note**

Unmanaged segments must be pure switches; no routing can be involved with the segment.

### Ethernet on Cloud VNEs

When using an Ethernet LAN cloud to represent unmanaged network segments, be aware of the following:

- For Ethernet interfaces with duplicate IPs, see Configuring Duplicate IP Addresses on Ethernet Interfaces, page 23-3.

- Devices on both sides of the cloud must communicate so that a Cloud VNE can build the forwarding information properly; otherwise, their MAC addresses do not appear in each other’s ARP or bridging tables.

- The logic that builds the bridging table assumes that each port in the network has a unique MAC address. If multiple ports with the same MAC address do exist in the network, the Cloud VNE will not function properly.

- The logic that builds the bridging table assumes there all VLANs in the network have different IDs. If multiple VLANs with the same ID do exist on any of the VNEs connected to the cloud, the VLANs will be connected together on the cloud.

- A router with an interface that is an ingress point of a Martini tunnel (with no IP address configuration) cannot be connected to a cloud. A Layer 2 tunnel represents a point-to-point pseudowire in the network.

- The size of the Ethernet Cloud VNE depends on the number of devices, their configurations and the number of VLANs that are connected to it.

- The Layer 2 devices in the unmanaged cloud segment cannot contain VLAN rewrite configurations that are not supported by the Cloud VNE.

- The Cloud VNE does not support the Q-in-Q technology. If VLAN stacking is configured on an unmanaged segment, or if ports with Q-in-Q configuration are connected to the cloud, the cloud might not be able to simulate the behavior of the unmanaged segment.

- The Cloud VNE does not have Spanning Tree Protocol (STP) awareness, so any link from a device to the unmanaged network is assumed to be in a nonblocking state. This might cause the forwarding information calculated by the Cloud VNE to be inaccurate.

- By default, Prime Network does not display VLANs that are present on the device and that cannot be deleted, such as restricted Fiber Distributed Data Interface (FDDI), Token Ring, and other nonEthernet VLANs.

---

**Note**

Most of the Ethernet functionality—namely, MAC and VLAN support—is only available for dynamic links.
Chapter 23  Unmanaged Network Segments (Cloud VNEs) and Dynamic/Static Links

Configuring Duplicate IP Addresses on Ethernet Interfaces

Figure 23-1 provides an example of a configuration of duplicate IP addresses on Ethernet interfaces that are connected to the same Cloud VNE.

Figure 23-1  Duplicate IP Addresses on Ethernet Interfaces

In Figure 23-1, a PE router and two CEs are connected to an unmanaged Ethernet access network, represented by a Cloud VNE.

The PE router is connected to the Cloud VNE through Port1. Two interfaces configured on Port1 are connected to different VRFs (VRF A and VRF B). Both VRF interfaces are configured with the same IP address (10.0.0.1). Each interface is configured with a different VLAN encapsulation (VLAN-ID 3 and VLAN-ID 5), and is connected to a different VLAN in the unmanaged network (VLAN 3 and VLAN 5).

The two CEs are connected to different VLANs in the unmanaged network: CE A is connected to VLAN 3 through Port2, and CE B is connected to VLAN 5 through Port3. Both Port2 and Port3 are access ports (that is, untagged ports with no VLAN encapsulation) and are configured with identical IP addresses (10.0.0.2).

The Cloud VNE creates a similar port for each port connected to it, and two bridges, one per VLAN (that is, a bridge for VLAN 3 and a bridge for VLAN 5). Each bridge contains a forwarding table with the MAC addresses of the ports connected to that VLAN. In this example, the bridge representing VLAN 3 contains MAC1 and MAC2, and the bridge representing VLAN 5 contains MAC1 and MAC3.

Connecting the Cloud VNE to a Device

Each Cloud VNE has a unique agent ID (that is used as the Cloud VNE’s identifier) that cannot be used to access any network element. To connect a regular VNE to a Cloud VNE, the VNE must be configured with the physical port that should be connected, and the agent ID of the Cloud VNE.

When configuring a Cloud VNE for dynamic operation, the cloud model and the topology (that is, the link between the Cloud VNE and the adjacent VNE) are discovered and managed automatically by Prime Network.

To configure the Cloud VNE to operate dynamically, after creating a new Cloud VNE, you must:

1. Identify the OID of the physical port layer of the port that will connect to the Cloud VNE.
2. Connect the ports on the adjacent VNEs to the Cloud VNE.
3. For Cloud VNEs with Ethernet support, configure the Cloud VNE’s permissible subnets.
Before You Begin

If you are creating an Cloud VNE with Ethernet support, read Ethernet on Cloud VNEs, page 23-2.

---

Step 1

Identify the physical port layer OID of the ports that will connect to the Cloud VNE.

a. Perform a GET on the PhysicalRoot to retrieve all the physical models of the VNE up to the physical layer. The GET command can be optimized to retrieve only necessary information using a specific retrieval specification.

The following is an example of an optimized GET command for VNE PE_South:

```xml
<command name="Get">
  <param name="oid">
    <value>{[ManagedElement(Key=PE_South)] [PhysicalRoot]}</value>
  </param>

  <param name="rs">
    <value>
      <key name="imo-view-controller">
        <entry name="depth">10</entry>
        <entry name="register">true</entry>
        <entry name="cachedResultAcceptable">false</entry>
      </key>

      <key name="requiredProperties">
        <key name="com.sheer.imo.IPhysicalRoot">
          <entry name="EquipmentHolders"/>
        </key>

        <key name="com.sheer.imo.IEquipmentHolder">
          <entry name="ContainedEquipmentHolder"/>
          <entry name="ContainedEquipment"/>
        </key>

        <key name="com.sheer.imo.IEquipment">
          <entry name="SupportedPTPs"/>
        </key>

        <key name="com.sheer.imo.IPhysicalTerminationPoint">
          <entry name="ContainedCurrentCTPs"/>
        </key>
      </value>
    </param>

  </command>
```

b. Identify the physical layer (port) OID according to port name or location. You will need For example, from the result of the previous step’s GET command, this would be the physical layer OID of port FastEthernet1/0 in PE_South.

```xml
<IPhysicalRoot>
  <ID type="Oid">{[ManagedElement(Key=PE_South)] [PhysicalRoot]}</ID>
  <EquipmentHolders type="IMObjects_Array">
    <IChassis>
      <ID type="Oid">{[ManagedElement(Key=PE_South)] [PhysicalRoot] [Chassis]}</ID>
      <ContainedEquipmentHolder type="IMObjects_Array">
        ....
        <IEquipmentHolder>
          <ID type="Oid">{[ManagedElement(Key=PE_South)] [PhysicalRoot] [Chassis] [Slot(SlotNum=1)]}</ID>
      </ContainedEquipmentHolder>
    </IChassis>

```
<ContainedEquipment type="IModule">
  <ID type="Oid">{[ManagedElement(Key=PE_South)] [PhysicalRoot] [Chassis] [Slot(SlotNum=1)] [Module]}</ID>
  <SupportedPTPs type="IMObjects_Array">
    <IPortConnector>
      <ID type="Oid">{[ManagedElement(Key=PE_South)] [PhysicalRoot] [Chassis] [Slot(SlotNum=1)] [Module] [Port(PortNumber=FastEthernet1/1)]}</ID>
      <ContainedCurrentCTPs type="IMObjects_Array">
        <IPhysicalLayer>
          <ID type="Oid">{[ManagedElement(Key=PE_South)] [PhysicalRoot] [Chassis] [Slot(SlotNum=1)] [Module] [Port(PortNumber=FastEthernet1/1)] [PhysicalLayer]}</ID>
        </IPhysicalLayer>
      </ContainedCurrentCTPs>
    </IPortConnector>
    <IPortConnector>
      <ID type="Oid">{[ManagedElement(Key=PE_South)] [PhysicalRoot] [Chassis] [Slot(SlotNum=1)] [Module] [Port(PortNumber=FastEthernet1/0)]}</ID>
      <ContainedCurrentCTPs type="IMObjects_Array">
        <IPhysicalLayer>
          <ID type="Oid">{[ManagedElement(Key=PE_South)] [PhysicalRoot] [Chassis] [Slot(SlotNum=1)] [Module] [Port(PortNumber=FastEthernet1/0)] [PhysicalLayer]}</ID>
        </IPhysicalLayer>
      </ContainedCurrentCTPs>
    </IPortConnector>
  </SupportedPTPs>
</ContainedEquipment>

The OID is
{[ManagedElement(Key=PE_South)] [PhysicalRoot] [Chassis] [Slot(SlotNum=1)] [Module] [Port(PortNumber=FastEthernet1/0)] [PhysicalLayer]}

c. Replace / (the slash) in the port name with \slash\ when specifying the OID in the CLI command.
For example, the OID from the preceding step should be changed to:
{[ManagedElement(Key=PE_South)] [PhysicalRoot] [Chassis] [Slot(SlotNum=1)] [Module] [Port(PortNumber=FastEthernet1\slash\0)] [PhysicalLayer]}

Step 2 Connect the ports to the Cloud VNE. For each VNE that represents a device that is connected to the unmanaged network represented by the Cloud VNE, do the following:

a. Log into the gateway as network user.
b. Change to the Main directory:
   
   # cd $ANAHOME/Main
c. Obtain the cloud agentId by running the following command, where cloudAvmId is the ID of the AVM in which the cloud was defined:

   cat registry/avm/cloudAvmId.xml
In the following example, a cloud was defined on AVM 358:

```bash
# cat registry/avm358.xml

<?xml version="1.0" encoding="UTF-8"?>
<key name="avm358">
  <entry name="default">mcvm</entry>
  <entry name="avmkey">AVM 358</entry>
  <key name="agents">
    <key name="da">
      <entry name="default">sheer/cloud/product/software versions/default version</entry>
      <entry name="element type">SHEER_NETWORKS_CLOUD</entry>
      <entry name="deletePersistency">true</entry>
      <entry name="adaptivePollingType">1</entry>
      <key name="creationTime">
        <entry name="time">1311516933201</entry>
      </key>
      <key name="pollingrates">
        <entry name="default">pollinggroups/default</entry>
      </key>
      <key name="amsi">
        <key name="topology">
          <key name="dynamic">
            <key name="permissible-subnet">
              <entry name="subnet">0.0.0.0/0</entry>
            </key>
          </key>
        </key>
        <key name="maintenance">
          <entry name="activated">false</entry>
        </key>
        <key name="ips">
          <entry name="agentId">784</entry>
          <key name="Cloud">
            ...
          </key>
        </key>
      </key>
    </key>
  </key>
</key>
```

### d. From the gateway, run the following CLI commands:

```bash
# ./runRegTool.sh -gs 127.0.0.1 add unit-IP
"avmxxx/agents/da/vne-key/dcs/instance/physical-layer-oid/cloud topology"
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
"avmxxx/agents/da/vne-key/dcs/instance/physical-layer-oid/cloud topology/id=
cloud-agent-ID"
```

The following lists the parameters you must define:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>unit-IP</code></td>
<td>The IP address of the Solaris machine on which the parent AVM resides (for the VNE that will connect to the Cloud VNE). If the AVM is on the gateway server, <code>unit-IP</code> should be <code>127.0.0.1</code>.</td>
</tr>
<tr>
<td><code>avmxxx</code></td>
<td>The ID of the parent AVM (for the VNE that will connect to the Cloud VNE).</td>
</tr>
<tr>
<td><code>vne-key</code></td>
<td>The name of the VNE which will connect to the Cloud VNE.</td>
</tr>
</tbody>
</table>
### Unmanaged Segments and Cloud VNEs

#### Example:

```bash
$ ./runRegTool.sh -gs 127.0.0.1 add 192.168.100.1
"avm900/agents/da/PE_South/dcs/instance/([ManagedElement(Key=PE_South)][PhysicalRoot][Chassis][Slot(SlotNum=1)][Module][Port(PortNumber=FastEthernet1/0)][PhysicalLayer])/cloud topology"
```

The previous example connects a VNE named PE_South (which resides in avm900 on unit 192.168.100.1) with a Cloud VNE that has the agent ID 784. The connection with the Cloud VNE is made using the physical layer of PE_South that has the OID:

```
[[ManagedElement(Key=PE_South)][PhysicalRoot][Chassis][Slot(SlotNum=1)][Module][Port(PortNumber=FastEthernet1/0)][PhysicalLayer]]/cloud topology/id" 784
```

**e. Restart the VNE.**

#### Step 3

If the cloud represents an Ethernet access network, configure the permissible subnets on the Cloud VNE. This will permit IP interfaces to connect to other entities only if the interfaces are on the specified subnets. This minimizes the number of connections the Cloud VNE handles.

---

**Note**

This configuration applies to the Cloud VNE, not to the adjacent VNEs. The most common use case is to configure permissible subnets to allow the connection through all subnets that are connected to the cloud (by configuring 0.0.0.0/0, or 0::0/0 for IPv6).

---

For each Cloud VNE, do the following:

- **a.** Log into the gateway as `network user`.
- **b.** Change to the Main directory:

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

- **c.** From the gateway, run the following CLI commands:

  ```bash
  $ ./runRegTool.sh -gs 127.0.0.1 add unit-IP
  "avmxxx/agents/da/cloud-vne-key/amsi/topology/dynamic/permissible-subnet"
  $ ./runRegTool.sh -gs 127.0.0.1 set unit-IP
  "avmxxx/agents/da/cloud-vne-key/amsi/topology/dynamic/permissible-subnet/subnet"
  permissible-subnet
  ```

---

### Table: Parameter Meaning

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>physical-layer-oid</code></td>
<td>The OID of the VNE port which will connect to the Cloud VNE. This is</td>
</tr>
<tr>
<td></td>
<td>the OID you identified in Step 1 of this procedure.</td>
</tr>
<tr>
<td><code>cloud-agent-ID</code></td>
<td>The agent ID of the Cloud VNE. (This is the Cloud VNE you created in</td>
</tr>
<tr>
<td></td>
<td>Creating VNEs for New Device Types, page 19-21.)</td>
</tr>
</tbody>
</table>

---
Creating and Deleting Static Links

You can create a static link between devices by selecting the two end ports from the device physical inventory in Prime Network Administration. To create a static topological link, you need to supply the exact location of the two end ports (at both ends of the link). The physical hierarchy in which the port is located defines the location of a port, as follows:

Device > [shelf] > module > [submodule] > port

**Note** The link is bidirectional, and needs to be added only once.

**Note** By default, a user can view a link in Prime Network Vision only if both link endpoints are in the user’s device scope. If you want to make links viewable if only one endpoint is in a user’s scope, you must edit the registry as described in Viewing Links in Device Scopes, page 7-17.
The new link is validated after the two ports are selected, but before the link is added. Validation checks:

- The similarity of the connector port types (for example, RJ45 on both sides).
- Layer 2 technology type (for example, ATM OC-3 on both sides).
- The physical layer.
- The operation status of both ports.
- One of the ports is part of another link.

For links between LAGs (IEEE 802.3ad), Prime Network also validates the following:

- The underlying dynamically discovered physical connections do not contradict the new static link.
- Different number of ports configured under the two LAGs.

If validation reveals that one of the ends is part of a static link, you are asked to delete the previous link manually. If validation reveals that one of the ends is part of a dynamic link, the previous link is overridden.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

To create a new static link:

**Step 1** Right-click **Topology** and choose **New Static Link**.

*Note* Any changes made in the Topology window are saved automatically and are registered immediately in Prime Network.

The A Side and Z Side lists enable you to choose the devices and the ports for the static link. When you select a device from the list, the physical inventory of the device is displayed the dialog box.

**Step 2** From the A Side and Z Side lists choose a device. The physical inventory of each device is displayed in the related area of the dialog box.

To delete a static link, right-click the link in the Topology window and choose **Delete**.
Chapter 23  Unmanaged Network Segments (Cloud VNEs) and Dynamic/Static Links

Creating and Deleting Static Links
Device Reachability

Prime Network VNEs communicate with network devices using the SNMP, Telnet, XML, ICMP, and HTTP protocols, and using notification protocols (traps and syslogs). To determine the reachability of specific protocols, Prime Network runs tests tailored to each protocol.

The status of all of these protocols determine whether a device is reachable. By default, Prime Network marks a device as unreachable only when all enabled protocols are down; that is, the protocols are not responding, and the device is not generating syslogs or traps. However, you can customize this behavior to fit your network.

These topics describe how reachability is determined and how you can customize this behavior to fit the needs of your network:

- VNE Management Communication Policies and How To Change Them, page 24-1
- How Prime Network Determines Protocol Reachability, page 24-3
- Customizing Protocol Reachability Testing, page 24-7

VNE Management Communication Policies and How To Change Them

The management communication policy determines when Prime Network changes a VNE communication state to Device Unreachable or Device Partially Reachable. The policies allow you to decide how more or less strictly you want to track protocol health. Figure 20-3 on page 20-7 illustrates how you can find out which management communication policy is being used by a VNE. Table 24-1 describes the supported policies.
Chapter 24  Device Reachability

VNE Management Communication Policies and How To Change Them

Table 24-1  Supported VNE Management Communication Policies

<table>
<thead>
<tr>
<th>Management Policy</th>
<th>Criteria for Determining Device Reachability</th>
</tr>
</thead>
<tbody>
<tr>
<td>notstrict</td>
<td>Device Unreachable state change when:</td>
</tr>
<tr>
<td></td>
<td>• All of the enabled protocols are down,</td>
</tr>
<tr>
<td></td>
<td>• No traps or syslogs were sent by the</td>
</tr>
<tr>
<td></td>
<td>device for the past 6 minutes.</td>
</tr>
<tr>
<td></td>
<td>Device Partially Reachable state change</td>
</tr>
<tr>
<td></td>
<td>when:</td>
</tr>
<tr>
<td></td>
<td>• All of the enabled protocols are down.</td>
</tr>
<tr>
<td></td>
<td>• Traps or syslogs are being sent by</td>
</tr>
<tr>
<td></td>
<td>device.</td>
</tr>
<tr>
<td>ensure-management</td>
<td>(Default) Device Unreachable state change</td>
</tr>
<tr>
<td></td>
<td>when:</td>
</tr>
<tr>
<td></td>
<td>• All of the enabled protocols are down.</td>
</tr>
<tr>
<td></td>
<td>The status of traps/syslogs is not</td>
</tr>
<tr>
<td></td>
<td>considered. (Because the state goes</td>
</tr>
<tr>
<td></td>
<td>directly to Device Unreachable, you will</td>
</tr>
<tr>
<td></td>
<td>never see the Device Partially Reachable</td>
</tr>
<tr>
<td></td>
<td>communication state when using this policy.)</td>
</tr>
<tr>
<td>strict</td>
<td>Device Unreachable state change when:</td>
</tr>
<tr>
<td></td>
<td>• At least one of the enabled protocols</td>
</tr>
<tr>
<td></td>
<td>are down.</td>
</tr>
<tr>
<td></td>
<td>The status of traps/syslogs is not</td>
</tr>
<tr>
<td></td>
<td>considered. (Because the state goes</td>
</tr>
<tr>
<td></td>
<td>directly to Device Unreachable, you will</td>
</tr>
<tr>
<td></td>
<td>never see the Device Partially Reachable</td>
</tr>
<tr>
<td></td>
<td>communication state when using this policy.)</td>
</tr>
</tbody>
</table>

Note

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

By default, Prime Network uses the ensure-management policy. You can check the policy that is being used with the following command:

```
# cd $ANAHOME/Main
# ./runRegTool.sh -gs 127.0.0.1 get 127.0.0.1
"site/agentdefaults/da/dcs/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/Reachability/policy"
```

If you want to change to a different management communication policy, see the instructions in Customizing Protocol Reachability Testing, page 24-7.

Changing the Management Communication Policy and Policy

The following procedure explains how to configure Prime Network to use a different policy to determine device reachability.

Note

All changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.
Use `runRegTool.sh` to make your registry changes, using the following format:

```
runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/agentdefaults/da/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/Reac
tibility/policy" value
```

The following table describes the policy key.

<table>
<thead>
<tr>
<th>Registry Entry (Key)</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy</td>
<td>Management communication policy Prime Network should use. Supported values are strict, ensure-management, or notstrict. For information on the policies, see VNE Management Communication Policies and How To Change Them, page 24-1.</td>
<td>ensure-management</td>
</tr>
</tbody>
</table>

**Step 1** Log into the gateway as network user and change to the Main directory by entering the following command. (network user is the operating system account for the Prime Network application, created when Prime Network is installed; for example, network39.)

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

**Step 2** Change the policy using the following command. This example changes the policy from ensure-management (the default) to strict:

```bash
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/agentdefaults/da/dcs/type/com.sheer.metrocentral.coretech.common.dc.ManagedElement/Reac
tibility/policy" strict
```

**Step 3** Restart Prime Network:

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

## How Prime Network Determines Protocol Reachability

These topics describes the tests Prime Network conducts to check the health of the SNMP, Telnet, XML, ICMP, and HTTP protocols. Settings for all of the protocols are listed in Table 24-3 on page 24-7. You can check Prime Network Vision to get details about the health of each protocol (see Figure 20-3 on page 20-7).

**SNMP**

SNMP connectivity is determined by the IP address of the device. The VNE polls the sysObjectld.0 (which is assumed to be available, simple, and immediate) and waits for a response (such as “1.3.6.1.2.1.1.2.0”). The registry entries that control SNMP reachability testing are provided in Table 24-3 on page 24-7.
The following steps describe how Prime Network checks the health of the SNMP protocol.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>The VNE detects a reachability problem.</td>
</tr>
<tr>
<td>Step 2</td>
<td>The VNE begins an SNMP reachability command cycle (the cycle is represented by <code>reachabilityretry</code>). The number of commands that are sent in each command cycle is determined by the value of <code>retries</code>. In this illustration, <code>retries</code>=3 and <code>timeout</code>=5 seconds.</td>
</tr>
<tr>
<td></td>
<td>a. The VNE sends an SNMP reachability command (a character) to the device. This is the first retry; <code>retry</code>=1.</td>
</tr>
<tr>
<td></td>
<td>b. If the device does not respond within <code>timeout x retry</code> (5 seconds x 1), the SNMP command is repeated. The VNE sends another SNMP reachability command (this is retry 2).</td>
</tr>
<tr>
<td></td>
<td>c. If the device does not respond within <code>timeout x retry</code> (5 seconds x 2), the SNMP command is repeated (this is retry 3).</td>
</tr>
<tr>
<td></td>
<td>This continues until <code>retries</code> SNMP commands have been sent. This completes one reachability command cycle.</td>
</tr>
<tr>
<td>Step 3</td>
<td>The value of <code>reachabilityretries</code> is decremented by 1.</td>
</tr>
<tr>
<td>Step 4</td>
<td>The mechanism waits the period of time specified by <code>reachabilityinterval</code>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>The mechanism repeats the reachability command cycle (Step 2) until <code>reachabilityretries</code> equals</td>
</tr>
<tr>
<td>Step 6</td>
<td>The SNMP protocol is marked Down.</td>
</tr>
</tbody>
</table>

How these values work together is illustrated in Figure 24-1.

**Figure 24-1  SNMP Reachability Testing**

```
reachabilityretries = 2

(reachabilityretry)

Send SNMP reachability command

<table>
<thead>
<tr>
<th>retries = 3</th>
<th>timeout</th>
<th>timeout + timeout</th>
<th>timeout + timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 secs</td>
<td>10 secs</td>
<td>15 secs</td>
<td>reachabilityinterval = 30 secs</td>
</tr>
</tbody>
</table>

Mark SNMP down

(reachabilityretry)

Send SNMP reachability command

<table>
<thead>
<tr>
<th>retries = 3</th>
<th>timeout</th>
<th>timeout + timeout</th>
<th>timeout + timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 secs</td>
<td>10 secs</td>
<td>15 secs</td>
<td>timeout</td>
</tr>
</tbody>
</table>
```

Timeout is incremented according to retries. In this case, `timeout` = 5 seconds and `retries` = 3.
By default, lazyreachability is disabled. This means the default reachability algorithm is proactive—the VNE sends an SNMP request to the device and expects a response. If a response is not received within a certain amount of time, the SNMP protocol is marked as Down. However, if the lazyreachability registry key is enabled, the VNE will not be proactive. Instead, the VNE will wait until a regular query is sent to the device, and if no result is received, the VNE marks the protocol as Down.

**Telnet and XML**

Telnet connectivity is determined by the IP address of the device. The VNE sends a space and carriage return and waits for the device to echo the prompt. The registry entries that control Telnet reachability testing are provided in Table 24-3 on page 24-7.

Prime Network uses these same tests for XML reachability testing. The only difference is that instead of sending a space and a carriage return, the VNE sends a request to sample the serial number of the device.

The following describes the two most common scenario for Telnet problems.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
</table>
| Scenario 1 | A running command times out and the connection to the device is lost. The VNE will attempt to start a new connection with the device.  
1. The VNE sends a message (a space and carriage return) to the device to initiate a login sequence.  
2. Starting from when the login sequence was initiated, if there is no response within logintimeout, the protocol remains marked Down. |
| Scenario 2 | The device is not responding in a timely manner to a bulk command. The VNE will begin monitoring the device as follows.  
1. Starting from when the first bulk request was sent, if there is no response within receivetimeout, the VNE repeats the request.  
2. If there is no response within workingtimeout, the protocol is marked Down. |

**Figure 24-2** illustrates Scenario 2, where a device is not returning timely responses to a bulk command.

Sometimes it is not necessary for the VNE to maintain an open Telnet connection to a device, even if the session is idle. This is illustrated in **Figure 24-3**.
a. The VNE sends Telnet reachability command (keepalive message) to the device. The keepalive message consists of a space and carriage return.

b. If the device does not respond within reachabilityinterval, the protocol is marked Down.

Figure 24-3 Reachability Testing to Retain Telnet Connection

Finally, if an open Telnet session is idle for an amount of time that exceeds idletime, Prime Network closes the connection. If the protocol connection is dropped, it is possible that reachability problems may go undetected by Prime Network until the Telnet connection is needed.

By default, lazyreachability is disabled. This means the default reachability algorithm is proactive—the VNE sends a Telnet request to the device (and a space and a newline character) and expects a response. If a response is not received within a certain amount of time, the Telnet protocol is marked as Down. If the lazyreachability registry key is enabled, the VNE will not be proactive. Instead, the VNE will wait until a regular query is sent to the device, and if no result is received, the VNE marks the protocol as Down.

ICMP

ICMP connectivity is determined by sending a ping to a device and waiting for a reply. The registry entries that control ICMP reachability testing are provided in Table 24-3 on page 24-7.

Due to a system limitation, ICMP packets cannot be sent. ICMP connectivity is therefore determined by attempting to establish a TCP connection on port 7 (Echo).

1. The VNE sends a ping to the device, and the device does not respond within timeout.
2. The first step is repeated retries times.
3. If there is still not response, the ICMP protocol is marked Down, and the VNE starts this process again.
HTTP

HTTP connectivity is determined by trying to log into the device. If the device does not respond within *timeout*, the device is marked as Down.

**Customizing Protocol Reachability Testing**

Table 24-3 lists the registry settings that control how Prime Network tests the SNMP, Telnet, XML, ICMP, and HTTP protocols to ensure reachability. These tests are described in How Prime Network Determines Protocol Reachability, page 24-3.

**Note**

Because many VNEs may be impacted, we recommend that you change these settings during a maintenance window. Avoid setting numbers too low (which can trigger false “unreachable” messages) or too high (which may cause real problems to go undetected).

**Note**

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

**Table 24-3** Registry Settings for Device Protocol Reachability

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trackreachability</td>
<td>Enable reachability detection process for SNMP</td>
<td>true</td>
</tr>
<tr>
<td>timeout</td>
<td>Timeout between each request (in seconds)</td>
<td>5</td>
</tr>
<tr>
<td>retries</td>
<td>Number of retries for each request</td>
<td>3</td>
</tr>
<tr>
<td>reachabilityinterval</td>
<td>Interval for device reachability command (in seconds)</td>
<td>30</td>
</tr>
<tr>
<td>reachabilityretries</td>
<td>Number of retries until a reachability problem is determined</td>
<td>1</td>
</tr>
<tr>
<td>lazyreachability</td>
<td>Send reachability request only when another (regular) query is being sent to the device (a non-proactive manner).</td>
<td>false</td>
</tr>
<tr>
<td><strong>Telnet and XML</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trackreachability</td>
<td>Enable reachability detection process for Telnet or XML</td>
<td>true</td>
</tr>
<tr>
<td>reachabilityinterval</td>
<td>Interval for device reachability command (in seconds)</td>
<td>30</td>
</tr>
<tr>
<td>lazyreachability</td>
<td>Send reachability request only when another (regular) query is being sent to the device (a non-proactive manner).</td>
<td>false</td>
</tr>
<tr>
<td>logintimeout</td>
<td>Timeout for login part (in seconds)</td>
<td>30</td>
</tr>
<tr>
<td>receivetimeout</td>
<td>Timeout for receiving initial device response to a command, or for executing a “more” or other interactive user signal (for responses that have multiple pages or bulk) (in seconds)</td>
<td>20</td>
</tr>
<tr>
<td>workingtimeout</td>
<td>Timeout for not receiving a device response to any commands (in seconds)</td>
<td>60</td>
</tr>
<tr>
<td>idletime</td>
<td>Amount of time where no commands are sent to device, after which to disconnect the Telnet or XML session (in seconds)</td>
<td>300</td>
</tr>
</tbody>
</table>
### Table 24-3  Registry Settings for Device Protocol Reachability (continued)

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ICMP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trackreachability</td>
<td>Enable reachability detection process for ICMP ping</td>
<td>true</td>
</tr>
<tr>
<td>retries</td>
<td>Number of retries for each ICMP ping</td>
<td>1</td>
</tr>
<tr>
<td>timeout</td>
<td>Timeout for not receiving a device response to the ICMP ping (in seconds)</td>
<td>5</td>
</tr>
<tr>
<td><strong>HTTP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trackreachability</td>
<td>Enable reachability detection process for HTTP</td>
<td>true</td>
</tr>
<tr>
<td>lazyreachability</td>
<td>Send reachability request only when another (regular) query is being sent to the device (a non-proactive manner).</td>
<td>false</td>
</tr>
<tr>
<td>timeout</td>
<td>Timeout for login (in seconds).</td>
<td>3</td>
</tr>
<tr>
<td>connectionReuse</td>
<td>Use the same connection to send and receive multiple HTTP requests/responses instead of opening a new connection for each request/response pair. Also known as HTTP keepalive.</td>
<td>true</td>
</tr>
<tr>
<td>authenticationRequired</td>
<td>Require device username and password when using HTTP.</td>
<td>true</td>
</tr>
</tbody>
</table>
VNE Collectors and Command Priorities

The following topics provide a high-level description of how VNE collectors execute the commands required to build a model of a device, and how to customize the way Prime Network executes these commands:

- What Are Collectors and Command Priorities?, page 25-1
- Considerations for Using Fast Commands and Fast Collectors, page 25-2
- Expedited Commands and Activation Scripts and Fast Collectors, page 25-3
- Configuring a Command With the “Fast” Command Priority, page 25-4
- Creating a Fast Collector for a VNE, page 25-5

What Are Collectors and Command Priorities?

Prime Network discovers and models a network element using commands that are called *registrations*. Registrations are forwarded to a VNE’s *collectors*, which are the VNE components that communicate with the physical network element. By default, each VNE is configured to have two collectors: an SNMP collector and a Telnet collector. These collectors can execute only one command at a time. Because many commands are sent to the network element during modeling, each collector maintains a queue of commands. When a collector is busy, any new incoming commands are placed at the end of the queue (FIFO, or first in, first out). When a collector finishes with one command, it executes the next command in the queue in a serial fashion.

In most cases, executing command in a serial fashion is adequate. However, it may not be efficient enough for network elements with large configurations, for the following reasons:

- When modeling begins, the collector receives many commands in a short amount of time. This results in a very long command queue.
- Some commands require extra time to execute (for example, when sampling a routing table for a Cisco CRS-1). The result is that commands at the end of the queue experience long delays before execution. This is particularly problematic for expedited commands and activation script commands (these cases are discussed in Expedited Commands and Activation Scripts and Fast Collectors, page 25-3).

---

**Note**

Slow response could be the result of a high CPU utilization problem. See CPU Utilization Problems: Where to Begin, page 22-2.
Considerations for Using Fast Commands and Fast Collectors

Command Priorities and Command Queues: Normal and Fast

To prevent delays in command execution, Prime Network uses a command priority mechanism. Every command is given one of the following priorities:

- **Fast**—High priority
- **Normal**—Normal priority (the default)

To deal with the two priorities, each collector maintains two queues: a fast queue for the fast commands and a normal queue for the normal commands. When a collector is available it will execute commands in the fast queue first. It will not execute any commands in the normal queue until the fast queue is empty.

Fast Collectors

Even a fast priority command can suffer a delay if, when it is sent, the collector is already busy executing a very large normal priority command.

For this situation, you can configure an additional collector called a fast collector. The fast collector is a special collector that is dedicated to commands in the fast queue. When the fast queue is empty, the fast collector is dormant.

For example, if you configure a fast collector for the Telnet protocol, Prime Network will have:

- One Telnet fast collector that only executes commands in the Telnet fast queue. If the Telnet fast queue is empty, the Telnet fast collector is dormant.
- One Telnet (default) collector that executes commands in both the Telnet normal and fast queues. (Remember that the default collector always executes commands in the fast queue first. If the Telnet fast collector is occupied, the Telnet (default) collector will execute the next command in the fast queue.).

Collectors and Thread Sharing

To decrease the overall number of threads used at the VNE layer, each AVM maintains pools of threads that are shared by the VNEs. VNEs acquire and release the threads as needed, in an asynchronous fashion. One thread pool is dedicated to activation scripts. This thread pool grows dynamically, up to the number of VNEs in the AVM. Each thread is destroyed after 60 seconds of inactivity. Even if you expect a large number of activation scripts to run in parallel, you should see no IO degradation. However, we recommend that you do not run more than 100 concurrent activation scripts on a unit.

Considerations for Using Fast Commands and Fast Collectors

There are obvious benefits of marking commands with a fast priority, and configuring and additional fast collector. But these methods also have some cost and possible risks.

Risks of Using the Fast Command Priority

Only a small number of registration commands should have a fast command priority. If too many commands are marked as fast, the queue for the fast commands can become long, with the following results:

- The purpose of command priorities is defeated because even fast commands have to wait in a queue.
- The normal commands are delayed even further because they are not executed until the (long) fast queue is empty.
Risks of Using Fast Collectors

We recommend that you do not configure an additional fast collector for the following reasons:

- The additional collector can impact system scale performance. In Prime Network, because each collector works in a separate thread, every VNE configured with a fast collector will consume an additional thread. If a large number of VNEs are configured with fast collectors, system performance can be significantly degraded.

- The additional collector could significantly reduce overall management traffic throughput. Every VNE configured with a fast collector opens an additional management connection to a device. Opening multiple connections in parallel can cause a significant increase in NE CPU levels, which can greatly reduce the overall throughput of management traffic.

General Recommendation for Fast Commands and Fast Collectors

For commands that are high priority, mark the command with the fast command priority. Do not configure an additional fast collector unless the command takes an unusually long time to execute.

Expedited Commands and Activation Scripts and Fast Collectors

By default, all expedited commands, activation scripts, and CPU monitoring commands have a fast command priority.

CPU monitoring commands have a fast command priority so that Prime Network can quickly identify and respond to high CPU issues that may affect the device and overall system.

Expedited commands have a fast command priority, but only for their first execution. Normally, expedited command execute with little delay. When it has successfully executed, the expedited command returns to a normal command priority. You should only consider using an additional fast collector if expedited commands are consistently delayed by other commands that require a long time to execute. To find out which commands are expedited, see the specific syslog, trap, and command descriptions in the in the Cisco Prime Network 3.9 Reference Guide and the Cisco Prime Network 3.9 Release Notes.

Activation scripts (which are converted into commands) have a fast command priority by default. However, activation scripts must adhere to a more strict timeout mechanism than expedited commands.

All commands—expedited commands or commands in activation scripts—have a timeout period which begins when command execution starts. But activation scripts have an additional timeout on the gateway. This gateway timeout begins when the commands are sent to the VNE. If a collector is occupied for an extended period, the gateway timeout may expire and the activation will fail.

If activation commands are timing out, consider the following approaches:

- For devices with marginal timeouts (that is, devices for which there is a very small difference between the script timeout and the time required for the longest command to execute), consider slightly increasing the activation script timeout. However, this is not appropriate for complex device configuration commands.

- For very complex devices with commands that require several minutes to execute, consider configuring an additional fast collector. Increasing the timeout is not appropriate because the increase would have to be sizable. This would result in Prime Network taking a long time to detect activation script failures, hence reducing the system throughput.
General Recommendation for Using Fast Collectors with Expedited Commands and Activation Scripts

The default behavior (described earlier) should be sufficient for both activation scripts and expedited commands. Consider an additional fast collector only if commands are experiencing unacceptable delays.

Note
If you decide to configure additional fast collectors, limit it to the smallest possible number of VNEs—in other words, only for VNEs with the most critical need. Also be sure to monitor the system for any effects on device CPU and system scale performance.

Configuring a Command With the “Fast” Command Priority

By default, all commands have a normal command priority and are executed by the collector in a FIFO basis. You can mark a command to have the fast (high) command priority, which means it will be placed in the collector’s fast queue rather than its normal queue. Use the following procedure to edit the command priority in the registry.

Note
We recommend that you do not change any of these settings. Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

Before You Begin

To set a command priority to fast, use the following procedure.

Step 1
Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; an example of network user is network39).

Step 2
Change to the NETWORKHOME/Main directory:

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

Step 3
Issue the following command to configure commands with the fast command priority. The variable registry-path is the path to the command to be configured. For example, for the CPU usage command in Cisco IOS devices, use the following:

```bash
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 "site/registry-path/cpu usage snmp/instrumentationservices/command/priority" fast
```

Step 4
Restart the gateway server:

```bash
# networkctl restart
```
Creating a Fast Collector for a VNE

By default, every protocol has only one collector (that is, no fast collector). You can configure a fast Telnet or SNMP collector for a VNE by editing the registry.

Note
Before you configure a fast collector, try using the fast command priority mechanism. See Configuring a Command With the “Fast” Command Priority, page 25-4.

Note
We recommend that you do not change any of these settings. Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

Before You Begin


To create a fast Telnet or SNMP collector for a specific VNE, use the following procedure.

Step 1
Log into the gateway as network user (where network user is the operating system account for the Prime Network application, created when Prime Network is installed; an example of network user is network39).

Step 2
Change to the NETWORKHOME/Main directory:

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

Step 3
Issue the following command to create a new fast collector for a specific VNE. In the following, avmxxx is the A VM ID, vne-key is the VNE name, and vne-ip is the VNE IP address.

If the VNE is on the gateway server, unit-IP should be 127.0.0.1. If the VNE is on a unit server, unit-IP should be the unit’s IP address.

- To create an SNMP fast collector for the VNE with the ID vne-key:

  ```
  #./runRegTool.sh -gs 127.0.0.1 set unit-IP
  "avmxxx/agents/da/vne-key/ips/vne-ip/protocols/snmp/maxfastcollector" 1
  ```

- To create a Telnet fast collector for the VNE with the ID vne-key:

  ```
  #./runRegTool.sh -gs 127.0.0.1 set unit-IP
  "avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/maxfastcollector" 1
  ```

Step 4
Restart the VNE using Prime Network Administration.

Note
Be sure to monitor the system for any effects on device CPU and system scale performance.
VNE Persistency Mechanism

Persistency is the ability to store information in the unit for later use. These topics describe the VNE persistency mechanism in Prime Network:

- **Persistency Overview, page 26-1**
- **Alarm Persistency, page 26-2**
- **Instrumentation Persistency, page 26-6**
- **Topology Persistency, page 26-7**

**Note**

These topics describe some of the persistency registry settings. Changes to the registry should be performed only with the support of Cisco. For details, contact your Cisco account representative.

**Persistency Overview**

Persistency information is stored across unit, AVM, and VNE restarts. VNE data persists during runtime when a VNE polls data from a device, and the VNE updates the files in the file system for changes in the device’s response according to the persistency variables. When a VNE is started or restarted, the persistency information is read from these files once. Every normal polling or refresh that takes place after the first time will read the data from the device itself and not from the files.

VNE data persistency is lost in the following scenarios (but alarm persistency is saved):

- A user manually moves the VNE to another AVM, or moves the parent AVM to another unit.
- A unit server high availability event occurs, causing a unit to switch over to the standby unit.
- The device the VNE models is reconfigured (for example, a new sysOID or software version change).

The upgrade mechanism automatically clears all persistency files on Prime Network gateways and units. This option does not clear the alarm history that is stored in the Prime Network database.
**Instrumentation Persistency**

Instrumentation persistency is used mainly to:

- Shorten the starting time of VNEs for devices. When the information from the local file system is used, the device’s response time and network latency are eliminated; thus the VNE finishes modeling its first state very quickly.
- Provide information about the old state of the VNE, to initiate alarms if the status has changed while the VNE was unloaded. For example, a Port Down alarm is initiated only if the port status was up and changed to down. This ensures that an alarm is not issued on ports which should be down. By maintaining information about the old state of the port, the system understands whether or not the current state is valid.
- Help lower the CPU load on the device while starting when many polling commands are generated. Also, when persistence data is loaded from the unit, traffic bandwidth between the unit and device is much lower than when the system is loaded using “ordinary” device discovery and modeling.

For more information, see **Instrumentation Persistency, page 26-6**.

**Topology Persistency**

Topology persistency creates topology between devices on startup when the VNE is loaded, instead of performing the entire discovery process. Verification of the links is then performed. For more information, see **Topology Persistency, page 26-7**.

**Alarm Persistency**

Alarm persistency saves information about the VNE components that send alarms. When a VNE sends an alarm, the VNE can save this information (that it has sent an alarm of type X). This information can then be used by the VNE components after restarts to verify whether the VNE needs to send clearing alarms where changes have occurred in the device when the VNE was down. For more information, see **Alarm Persistency, page 26-2**.

**Alarm Persistency**

Alarm persistency enables the system to clear alarms that relate to events that occurred while the system was down. For example, a Link Down alarm is generated, and then the system goes down. While the system is down, a Link Up event occurs in the network, but because the system is down, it does not monitor the network. When the system goes up, the alarm is cleared because the system remembers that a Link Down alarm exists, and the system needs to clear it by sending a corresponding alarm.

Persisting events are held in the AlarmPersistencyManager. Each VNE contains an AlarmPersistencyManager object. Alarms are added to and removed from the AlarmPersistencyManager object in order to maintain the status of an event, whether it exists in the repository or not; that is, whether an up alarm or a clearing alarm has been generated. Two copies of alarm persistency information are maintained: one in the memory, and the other on disk.

At startup, the AlarmPersistencyManager retrieves the events persisted for the containing VNE.

Event data in the files is updated at the following times:

- At shutdown.
- After a change, when an event is added or removed.
- After a specific interval of time has passed. This prevents data from being rewritten to the persistency file when a stream of events is added or removed during a short period of time, because the data is saved only after the specified period of time has elapsed.
Initialization

Alarm persistency is controlled by settings in the registry. Global alarm persistency information is stored in agentdefaults.xml. The major settings are listed in Table 26-1. The settings for these configurable items only apply when trying to retrieve data from the persistency files. Individual event persistency information is described in Configuring Alarm Persistency for a Specific Event, page 26-4.

Note

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

Table 26-1 Default Settings for Alarm Persistency

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Enabled the persistency mechanism for this VNE.</td>
<td>true</td>
</tr>
<tr>
<td>writing-delay</td>
<td>Interval (in milliseconds) between the arrival of a new event or the removal of an existing event, and the writing activity of the persistency file.</td>
<td>300000 (5 minutes)</td>
</tr>
<tr>
<td>max-alarm-age-in-days</td>
<td>How many days an event remains in a persistency file before it becomes obsolete.</td>
<td>7</td>
</tr>
</tbody>
</table>

Retrieving Events

At startup, each VNE calls its AlarmPersistencyManager to load the persisting events. If the file does not exist or is corrupt, no events are loaded. Faulty event objects are not loaded. Events which have been in the file for longer than the configured maximum age are not loaded. No age tests are held during ordinary runtime.

Storing Events

At shutdown, events are saved to the VNE’s event persistency file as a precaution in case the events have not already been saved.

Removing an Event

An event is searched for and removed using the same information which was used to add it. The event is removed from memory because a clearing event (for example, a Link Up alarm) has been generated, and the persistency information is no longer required. After the removal, the AlarmPersistencyManager stores the events after a writing delay, as specified in the registry.

Removing an Event and Clearing an Alarm

The AlarmPersistencyManager is able to search for and remove an event, and send a clearing alarm for the event, if it is found that this information is no longer required because the alarm has been cleared. After an event has been added to or removed from the AlarmPersistencyManager, a delayed message is sent to the AlarmPersistencyManager. Upon its arrival, the message triggers the events to be stored to the file.
Configuring Alarm Persistency for a Specific Event

Alarm persistency can be configured per event using the setting described in Table 26-2. Event-specific persistency information is stored in event-persistency-application.xml.

**Note**

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

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm-persistency</td>
<td>Enable persistency for a specific event.</td>
<td>See Alarm Persistency Default Configuration, page 26-4</td>
</tr>
</tbody>
</table>

In the following LDP Neighbor Loss alarm, the LDP Neighbor Down event marks the alarm as present in the system (persisted), and the LDP Neighbor up event is used to clear the alarm from persistency (unpersist):

```xml
<key name="LDP neighbor loss">
  <entry name="default">event-persistency-application/templates/generic persistency event</entry>
  <key name="sub-types">
    <key name="LDP neighbor down">
      <entry name="alarm-persistency">persist</entry>
    </key>
    <key name="LDP neighbor up">
      <entry name="alarm-persistency">unpersist</entry>
    </key>
  </key>
</key>
```

**Alarm Persistency Default Configuration**

The following alarms are configured to be persistent.

<table>
<thead>
<tr>
<th>Persisted Alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>all ip interfaces down</td>
</tr>
<tr>
<td>ascend link down trap</td>
</tr>
<tr>
<td>bfd connectivity down</td>
</tr>
<tr>
<td>bfd neighbour loss</td>
</tr>
<tr>
<td>bgp link down due to admin</td>
</tr>
<tr>
<td>bgp link down due to oper</td>
</tr>
<tr>
<td>bgp link down vrf due to admin</td>
</tr>
<tr>
<td>bgp link down vrf due to oper</td>
</tr>
<tr>
<td>bgp neighbour loss due to admin</td>
</tr>
<tr>
<td>bgp neighbour loss due to oper</td>
</tr>
<tr>
<td>bgp-neighbour-loss-vrf-due-to-admin</td>
</tr>
</tbody>
</table>
### Table 26-3 Persisted Alarms (continued)

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Alarms</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp-neighbor-loss-vrf-due-to-oper</td>
<td>efp oper down</td>
<td>ospf neighbor down</td>
</tr>
<tr>
<td>bridgeilan ac clear</td>
<td>envmon condition syslog</td>
<td>pim interface down syslog</td>
</tr>
<tr>
<td>bridgeilan ac shutdown</td>
<td>envmon fan syslog</td>
<td>pim neighbor loss syslog</td>
</tr>
<tr>
<td>bridgeilan bridge-domain clear</td>
<td>envmon powersupply syslog</td>
<td>port down due to admin</td>
</tr>
<tr>
<td>bridgeilan bridge-domain shutdown</td>
<td>envmon temperature syslog</td>
<td>port down due to card out</td>
</tr>
<tr>
<td>bridgeilan pseudowire shutdown</td>
<td>fabric hardware syslog</td>
<td>port down due to card down</td>
</tr>
<tr>
<td>bridgeilan pseudowire clear</td>
<td>flash card removed syslog</td>
<td>port down due to oper</td>
</tr>
<tr>
<td>card down</td>
<td>GRE tunnel down</td>
<td>port down due to upper layer down</td>
</tr>
<tr>
<td>card down syslog</td>
<td>high priority member down</td>
<td>port flapping</td>
</tr>
<tr>
<td>card out</td>
<td>ima admin down</td>
<td>rx dormant</td>
</tr>
<tr>
<td>cpu overutilized</td>
<td>ima oper down</td>
<td>rx overutilized</td>
</tr>
<tr>
<td>device unsupported</td>
<td>interface status down GRE tunnel</td>
<td>sonetpath link down</td>
</tr>
<tr>
<td>dropped packets</td>
<td>interface status down connection</td>
<td>sonetpath link down due to admin down</td>
</tr>
<tr>
<td>dropped packets</td>
<td>interface status down non connection</td>
<td>sonetpath link down due to card</td>
</tr>
<tr>
<td>ds0 bundle admin down</td>
<td>keepalive not set</td>
<td>sonetpath link down due to oper down</td>
</tr>
<tr>
<td>ds0 bundle oper down</td>
<td>12tp peer not established</td>
<td>sonetpath link down on unreachable</td>
</tr>
<tr>
<td>ds1 path link down</td>
<td>12tp sessions count exceeds max threshold</td>
<td>sonetpath port down due to admin</td>
</tr>
<tr>
<td>ds1 path link down due to admin</td>
<td>lag admin down</td>
<td>sonetpath port down due to admin</td>
</tr>
<tr>
<td>ds1 path link down due to card</td>
<td>lag oper down</td>
<td>sonetpath port down due to oper</td>
</tr>
<tr>
<td>ds1 path link down due to oper down</td>
<td>lag link admin down</td>
<td>sonetpath port flapping</td>
</tr>
<tr>
<td>ds1 path link down on unreachable</td>
<td>lag link down on unreachable</td>
<td>stop flapping non-cleared</td>
</tr>
<tr>
<td>ds1 path port down due to admin</td>
<td>lag link oper down</td>
<td>sub card down</td>
</tr>
<tr>
<td>ds1 path port down due to card</td>
<td>layer 2 aggregation admin down</td>
<td>sub card out</td>
</tr>
<tr>
<td>ds1 path port down due to oper</td>
<td>layer 2 aggregation oper down</td>
<td>sub-interface admin down</td>
</tr>
<tr>
<td>ds1 path port down due to upper layer downb</td>
<td>layer 2 tunnel down</td>
<td>sub-interface oper down</td>
</tr>
<tr>
<td>ds1 path port flapping</td>
<td>LDP neighbor down</td>
<td>tx dormant</td>
</tr>
<tr>
<td>ds3 path link down</td>
<td>link down</td>
<td>tx overutilized</td>
</tr>
<tr>
<td>ds3 path link down due to admin down</td>
<td>link down due to admin down</td>
<td>vsi admin down</td>
</tr>
<tr>
<td>ds3 path link down due to card</td>
<td>link down due to card</td>
<td>vsi oper down</td>
</tr>
<tr>
<td>ds3 path link down due to oper down</td>
<td>keepalive not set</td>
<td></td>
</tr>
<tr>
<td>ds3 path link down on unreachable</td>
<td>link down due to oper down</td>
<td></td>
</tr>
</tbody>
</table>
Instrumentation Persistency

The instrumentation layer persists the information that was collected from the device to the file system. When the VNE restarts, it uses this information to emulate the device’s response, and thus the VNE can be modeled according to its last persistent state. The next polling instance is performed against the real device.

The registry entries that control instrumentation persistency are provided in Table 26-4.

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

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistencydir</td>
<td>Specifies the directory in which persistency information is saved on the local file system. This is a relative path. Allowed values are a string that represents the relative directory in the file system.</td>
<td>instrumentor-persistency</td>
</tr>
<tr>
<td>persistencylevel</td>
<td>Controls the level of persistency to be used. The allowed values are Full (persisted) or Off (not persisted). These values can be used for certain commands to make sure some are persisted and some are not. If a compound command contains both Full and Off persistency levels, Prime Network will use the full level for all commands.</td>
<td>Full</td>
</tr>
<tr>
<td>persistencystoreenabled</td>
<td>Controls whether the whole storage mechanism is enabled.</td>
<td>true</td>
</tr>
<tr>
<td>persistencestorageinterval</td>
<td>Interval (in milliseconds) for which the data to be persisted is accumulated and then written to the persistent storage in bulk. Files are only updated if they have changed. The default value (20 minutes) is a compromise between small intervals (which cause more I/O operations in the local file system) and long intervals (which result in stored information not being up-to-date).</td>
<td>1200000 (20 minutes)</td>
</tr>
<tr>
<td>persistencytimeout</td>
<td>Timeout period (in milliseconds) at which initial data is marked as obsolete; all subsequent commands will run directly on the device. If the persistency mechanism is enabled when the instrumentation layer starts, it loads all the data from the files. This data can be used for the commands only the first time they are executed. Some commands can be used for the first time, long after other commands have finished multiple cycles; for example, commands which run only when the status on the device has changed. The default value (1 minute) is a compromise between a small value (which can cause the instrumentation layer to ignore the persistent data) and a large value (which causes the data to be retrieved long after the VNE has finished loading). We recommend that this value be at least 600000 (1 minute).</td>
<td>600000 (1 minute)</td>
</tr>
</tbody>
</table>
Topology Persistency

Prime Network supports persistency for Layer 1 topological connections. Layer 1 topology supports one connection per Device Component (DC), so the physical topology reflects a single port connected by a single link.

The following topologies are persisted:
- Layer 1 counter-based topologies.
- Static topologies.

Static topology, which identifies physical links configured by the user, is persisted once a user configures the static link between the two entities. This link is then stored in the registry, in the AVM key that contains the specific VNE registrations.

For other topologies, every time a link is created, the persistency mechanism writes the link to this file. When a link is disconnected, the file representing the link is removed.

**Note**
Topology persistency assumes that the XID (the unique device component ID) is persistable. For example, the port XID should remain the same after the device reboots or after the VNE reboots. This is not dependent on whether the ifIndex is changed from time to time.

Topology persistency is controlled by the setting listed in Table 26-5.

**Table 26-5 Registry Setting for Topology Persistency**

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistency</td>
<td>Enable physical topology persistency.</td>
<td>true</td>
</tr>
<tr>
<td>Note</td>
<td>We recommend that this entry remain enabled.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
All changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.
PART 6

Appendixes
Device Configuration Tasks for VNE Creation

These topics describe the configuration tasks you must perform so that Prime Network can properly model and manage devices.


- Why Device Configuration Tasks Are Important, page A-1
- Validating Devices Before Adding VNEs (Cisco IOS XR), page A-2
- Cisco IOS, Cisco IOS XE, and CatOS Devices—Required Settings, page A-2
- Cisco IOS XR Devices—Required and Recommended Settings, page A-3
- Cisco StarOS Devices—Required Settings, page A-5
- Cisco Nexus OS—Required Settings, page A-7
- All Cisco Devices Added Using SSH—Required, Recommended, and Rollback Device Settings, page A-8
- SNMP Traps and Informs—Required Device Settings, page A-8
- Syslogs—Required Device Settings, page A-13
- IP Address Configuration for Traps, Syslogs, and VNEs, page A-14
- Cisco Carrier Packet Transport Devices, page A-15

Why Device Configuration Tasks Are Important

Note: Do not change the device's default packet size (which 1500 bytes). SNMP requests are sent in bulk by default. A small packet size could result in truncated responses.

Prime Network VNEs communicate with network devices using a variety of protocols such as SNMP, Telnet, and ICMP. When a VNE is created, Prime Network connects to the device and runs a variety of registration commands to build a model of the device, based on the scheme that is chosen for the VNE. After modeling, ongoing notifications and protocol communication allows Prime Network to perform ongoing service and technology monitoring, fault processing, topological and model updates, and so forth. If the required device settings are not configured properly, Prime Network cannot retrieve the necessary information from the network element.
Validating Devices Before Adding VNEs (Cisco IOS XR)

Prime Network validates the configuration of Cisco IOS XR devices before creating VNEs for those devices. The validations are contained in a registration named mis-con, which validates the following:

- The MGBL package is installed on the device.
- The user belongs to root-system.
- XML is enabled on the device.

If any of these validations fail, Prime Network generates a system event. To disable this validation for all Cisco IOS XR devices, use the following command from the gateway server:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/cisco-router-iox-ipcore-scheme-evne/com.sheer.metrocentral.coretech.common.dc.ManagedElement/mis-con/enable" false
success
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/cisco-router-iox-ipcore-scheme/com.sheer.metrocentral.coretech.common.dc.ManagedElement/mis-con/enable" false
success
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/cisco-router-iox-product-scheme/com.sheer.metrocentral.coretech.common.dc.ManagedElement/mis-con/enable" false
success
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/cisco-router-iox-product-scheme-evne/com.sheer.metrocentral.coretech.common.dc.ManagedElement/mis-con/enable" false
success
```

Cisco IOS, Cisco IOS XE, and CatOS Devices—Required Settings

The following settings are required for Cisco IOS, Cisco IOS XE, and CatOS network elements:

```
snmp-server community public-cmty RO
snmp-server community private-cmty RW
```

This setting is required for Cisco IOS and Cisco OS XE devices (it is already set by default for CatOS devices):

```
snmp-server ifindex persist
```

For Cisco IOS devices using reduced polling, the following settings are required.

```
configure terminal
archive
log config
logging enable
```
Cisco IOS XR Devices—Required and Recommended Settings

When you create a VNE for a Cisco IOS XR device, Prime Network automatically performs a set of validation checks to ensure that the device is properly configured so it can be fully modeled. If a device fails any of the checks, a System event is generated.

Those automatic validation checks for Cisco IOS XR devices include the following:

- The MGBL package is installed.
- The user belongs to root-system.
- XML is enabled on the device. See Enabling XML on a Device, page A-3.

The following settings (not included in the validation check) are required for Cisco IOS XR network elements:

- If applicable, be sure to commit snmp-server community before snmp-server host.

```bash
domain ipv4 host gateway_name gateway_IP
telnet ipv4 server max-servers no-limit
snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server ifindex persist
vty-pool default 0 99
xml agent tty
```

To include the location of an event for an IOS XR device, execute the following command:

```
# logging events display-location
```

Enabling XML on a Device

There are three different methods for XML communication between devices and Prime Network. The device configuration required depends on the method you are using.

- TTY XML Agent—To enable a TTY XML agent on a device, use the following commands. (In this case you do not need to enter any information in the VNE’s XML tab in the Administration GUI client).

  ```
  configure terminal
  xml agent tty
  commit
  ```

- Dedicated XML agent—With a dedicated XML agent on the router, incoming XML sessions are handled over the dedicated TCP port 38751. In the Administration GUI client, enable XML on the VNE using the Telnet protocol. Enter the following commands on the device:

  ```
  configure
  xml agent
  aaa authorization exec default local
  commit
  exit
  ```

- SSL XML agent—With a dedicated SSL agent on the router, incoming XML sessions are handled over the dedicated TCP port 38752. In the Administration GUI client, enable XML on the VNE using the SSL protocol. Enter the following commands on the device:

  ```
  configure
  xml agent ssl
  ```
aaa authorization exec default local
commit
exit

Other Guidelines for Cisco IOS XR Devices

For Cisco IOS XR devices using reduced polling, the archive must be enabled (it is enabled by default). In addition to the required settings, you must follow these guidelines:

- Install the Cisco IOS XR Manageability Package (MGBL) on top of the Cisco IOS XR version. You can get information on this package from the release notes for your Cisco IOS XR version. (Prime Network automatically performs a validation check to ensure the MGBL package is installed.)
- Prime Network should use the device login user that is a member of group root-system and cisco-support. (Prime Network automatically performs a validation check to ensure this is properly configured.)
- To correctly model logical routers, the Prime Network user should use the admin user unique Telnet login user@admin (and also be a member of groups root-system and cisco-support).
- The devices must have one of the following SNMP community privileges: SDROwner, SystemOwner, or the default (which means no specific level was specified). You may configure this as needed, using the following guidelines.

```
snmp-server community [clear | encrypted] community-string [view view-name] [RO | RW] [SDROwner | SystemOwner] [access-list-name]
```

The `snmp-server` command takes the following arguments.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear</code></td>
<td>Specifies the <code>community-string</code> command format and how it should be displayed in the <code>show running</code> command output.</td>
</tr>
<tr>
<td><code>encrypted</code></td>
<td>- <code>clear</code>—<code>community-string</code> is clear text and should be encrypted when displayed by <code>show running</code>.</td>
</tr>
<tr>
<td><code>encrypted</code></td>
<td>- <code>encrypted</code>—<code>community-string</code> is encrypted text and should be encrypted when displayed by <code>show running</code>.</td>
</tr>
<tr>
<td><code>view view-name</code></td>
<td>Specifies the previously-defined view <code>view-name</code>, which defines the objects available to the community.</td>
</tr>
</tbody>
</table>
Cisco StarOS Devices—Required Settings

This section includes required settings for ASR 5000 series devices, which include settings for:

- SNMP Community, page A-5
- SNMP Trap, page A-5
- Reduced Polling, page A-6

### SNMP Community

SNMP community need to be configured in the device to manage ASR 5000 series device in Prime Network.

#### Configuring SNMP Community

```bash
[local] asr5000# configure
[local] asr5000(config)# snmp community name {community string} read-only
[local] asr5000(config)# end
```

#### Verifying the Above Configuration

```bash
[local] asr5000# show snmp communities
 Community Name             Access Level
--------------------------- ------------
 private                    read-write
 public                     read-only

[local] asr5000#
```

### SNMP Trap

The required settings to enable and send SNMP traps to Prime Network are listed below.
Cisco StarOS Devices—Required Settings

Configuring SNMP Traps

```
[local]asr5000# configure
[local]asr5000(config)# snmp target {target name} {target IP} security-name {community string} version 2c traps
[local]asr5000(config)# snmp trap enable all target {target name}
```

Verifying the Above Configuration

```
[local]asr5000
# show snmp transports
Target Name:    target1
IP Address:     10.56.22.25
Port:           162
Default:        Default
Security Name:  public
Version:        2c
Security:       
Authentication: 
Privacy:        
View:           
Notify Type:    traps

[local]asr5000#
```

Reduced Polling

Configuration-monitor need to be enabled in the device for reduced polling. The required settings are listed below. This setting should be done along with the SNMP trap setting described in the above section.

Configuring for Reduced Polling

```
[local]asr5000# configure
[local]asr5000(config)# cli configuration-monitor
[local]asr5000(config)# end
```

Verifying the Above Configuration

```
[local]asr5000# show cli configuration-monitor
config monitor enabled? : yes
monitoring config changes? : yes
monitoring enabled/disabled : Wed May 23 01:41:37 2012 cli config monitor instance : 0
cli config monitor status : running - idle
# config change traps sent : 0
seconds until next monitor : 713
longest checksum time (sec) : 0
time of last object change : (not set) last config object changed : (no changes)
[local]asr5000#
```
Cisco Nexus OS—Required Settings

Devices running Nexus OS must meet the following prerequisites for modeling to be complete in Prime Network:

- The complete hostname, such as hostname#, must be added when entering the credentials.
- The Virtual Context Device (VDC) must be configured completely for Nexus devices:
  
a. In the default VDC for the Nexus device, the vdc combined-hostname command must be configured.
  
b. Perform the tasks described in Configuring VDCs, page A-7.
  
c. Associate the management IP address of all VDCs with the default VDC’s management-VRF (that is, the is the VRF which is associated with the management IP address of the Nexus switch).
  
d. Ensure the system administrator account on the device is set up.
  
e. Verify that the VDC is set up correctly. See Verifying VDC Configuration, page A-7.

Configuring VDCs

To configure VDC, enter the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# config t</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>switch(config)#vdc vdcname [opt-param]</td>
<td>Creates a VDC and enters VDC configuration mode.</td>
</tr>
<tr>
<td>switch(config-vdc)# show vdc membership</td>
<td>(Optional) Displays the interface membership for the VDC.</td>
</tr>
<tr>
<td>switch(config-vdc)# allocate interface ethernet 2/1</td>
<td>(Optional) Allocates one interface to the VDC.</td>
</tr>
<tr>
<td>switch(config-vdc)# exit</td>
<td>Exits VDC configuration mode.</td>
</tr>
<tr>
<td>switch(config)# show</td>
<td>(Optional) Displays VDC status information.</td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td>Updates the startup configuration file.</td>
</tr>
</tbody>
</table>

Verifying VDC Configuration

Verify that the VDC configuration is complete and confirm that you can switch between VDCs by entering the switchto vdc command as follows:

switch# switchto vdc vdcname
Do you want to enforce secure password standard (yes/no) [y]: no
Enter the password for "admin":
Confirm the password for "admin":

---- Basic System Configuration Dialog VDC: 4 ----

Would you like to enter the basic configuration dialog (yes/no): no
switch-cisco3# switchback
switch# switchto vdc vdcname2
switch-cisco3#

where:

- vdcname is the name of the VDC you created.
• `vdcname2` is the name of a different VDC.

All Cisco Devices Added Using SSH—Required, Recommended, and Rollback Device Settings

This SSH information applies to all device types and operating systems. (For information on how to set up a device to run SSH, see your device documentation.) The following is an example of how to enable SSH on Cisco devices when they need to be added to Prime Network using SSH:

```
(config) ip domain-name DOMAIN
(config) crypto key generate rsa
```

**Note**

When you are requested to enter the modulus length, leave the default value. Although a longer modulus length may be more secure, it takes longer to be generated and used.

Configure vty to accept local password checking:

```
line vty 0 4
login local
```

The following are *recommended* SSH configuration settings:

```
ip ssh time-out 120
ip ssh authentication-retries 2
ip ssh version 1(2)
```

To roll back to the original device configuration, use the following settings:

```
no ip ssh {timeout | authentication-retries}
crypto key zeroize rsa
```

SNMP Traps and Informs—Required Device Settings

The required settings for SNMP traps and informs are listed below. Note the additional information for Cisco IOS XR devices.

- **Required SNMP Settings by Device Operating System, page A-9**
- **Recommended and Optional SNMP Settings for Cisco IOS XR Devices, page A-11**
## Required SNMP Settings by Device Operating System

The following table lists the settings you must configure in order to properly receive SNMP traps and informs. Syslogs must be enabled to use reduced polling.

<table>
<thead>
<tr>
<th>SNMP Type</th>
<th>Required Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td><code>snmp-server enable traps</code> <code>snmp authentication linkdown linkup coldstart warmstart</code> <code>snmp-server enable traps chassis</code> <code>snmp-server enable traps module</code> <code>snmp-server enable traps bgp</code> <code>snmp-server enable traps ospf state-change</code> <code>snmp-server enable traps ospf errors</code> <code>snmp-server enable traps ospf retransmit</code> <code>snmp-server enable traps ospf lsa</code> <code>snmp-server enable traps ospf cisco-specific state-change</code> <code>snmp-server enable traps ospf cisco-specific errors</code> <code>snmp-server enable traps ospf cisco-specific retransmit</code> <code>snmp-server enable traps ospf cisco-specific lsa</code> <code>snmp-server enable traps ipmulticast</code> <code>snmp-server enable traps entity</code> <code>snmp-server enable traps rtr</code> <code>snmp-server enable traps flash insertion removal</code> <code>snmp-server enable traps envmon fan shutdown supply temperature status</code> <code>snmp-server enable traps rtr</code> <code>snmp-server enable traps mpls ldp</code> <code>snmp-server enable traps ipsec tunnel start</code> <code>snmp-server enable traps ipsec tunnel stop</code> <code>snmp-server trap-source interface_name</code></td>
</tr>
</tbody>
</table>

**Note**  
`interface_name` is the active management IP address. This setting is required if the device has a management IP address.

Required for Nexus devices:  
`snmp-server enable traps`  
`snmp-server host event_collector_IP use-vrf management-VRF`

Required for ASR 1000 IPSec traps:  
`snmp-server enable traps ipsec tunnel start`  
`snmp-server enable traps ipsec tunnel stop`

**Note**  
`management-VRF` is the VRF which is associated with the management IP address of the Nexus switch.

Optional for all devices:  
`snmp-server enable traps config`  
`snmp-server enable traps syslog`

**SNMPv1**  
`snmp-server host event_collector_IP version 1 community`

**SNMPv2**  
`snmp-server host event_collector_IP (traps | informs) version 2c community`
### SNMP Type

<table>
<thead>
<tr>
<th>SNMP Type</th>
<th>Required Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMPv3 With Authentication</strong></td>
<td><strong>Note</strong>  <em>MyUsr, MyGrp, MyPs wd, and MyView</em> must match the information you enter when you create the VNEs in Prime Network.</td>
</tr>
<tr>
<td></td>
<td>• For all devices:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server group MyGrp v3 priv write MyView</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server view MyView internet included</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server view MyView 1.2.840.10006.300 included</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server group MyGrp v3 auth [notify MyView]</code></td>
</tr>
<tr>
<td></td>
<td>• For Cisco IOS, Cisco IOS XE, and CatOS devices:</td>
</tr>
<tr>
<td></td>
<td>`snmp-server user MyUsr MyGrp v3 auth (md5</td>
</tr>
<tr>
<td></td>
<td>• For Cisco IOS XR devices:</td>
</tr>
<tr>
<td></td>
<td>`snmp-server user MyUsr MyGrp v3 auth (md5</td>
</tr>
<tr>
<td></td>
<td>• For all devices, after configuring SNMPv3 on the device, configure the following setting:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server host event_collector_IP traps version 3 auth MyUsr</code></td>
</tr>
<tr>
<td><strong>SNMPv3 With Privacy and Authentication</strong></td>
<td><strong>Note</strong>  <em>MyUsr, MyGrp, MyAuthPs wd, MyPrivPs wd, and MyView</em> must match the information you enter when you create the VNEs in Prime Network.</td>
</tr>
<tr>
<td></td>
<td>• For all devices:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server group MyGrp v3 priv write MyView</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server view MyView internet included</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server view MyView 1.2.840.10006.300 included</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server group MyGrp v3 priv [notify MyView]</code></td>
</tr>
<tr>
<td></td>
<td>• For Cisco IOS, Cisco IOS XE, and CatOS devices:</td>
</tr>
<tr>
<td></td>
<td>`snmp-server user MyUsr MyGrp v3 auth (md5</td>
</tr>
<tr>
<td></td>
<td>• For Cisco IOS XR devices:</td>
</tr>
<tr>
<td></td>
<td>`snmp-server user MyUsr MyGrp v3 auth (md5</td>
</tr>
<tr>
<td></td>
<td>• For all devices, after configuring SNMPv3 on the device, configure the following setting:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server host event_collector_IP traps version 3 priv MyUsr</code></td>
</tr>
<tr>
<td><strong>SNMPv3 No Authentication</strong></td>
<td><strong>Note</strong>  <em>MyNoAuthUsr</em> and <em>MyNoAuthGrp</em> must match the information you enter when you create the VNEs in Prime Network.</td>
</tr>
<tr>
<td></td>
<td>• For Cisco IOS, Cisco IOS XE, and CatOS devices:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server group MyNoAuthGrp v3 noauth</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server user MyNoAuthUsr MyNoAuthGrp v3</code></td>
</tr>
<tr>
<td></td>
<td>• For Cisco IOS XR devices:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server user MyNoAuthUsr MyNoAuthGrp v3 SystemOwner</code></td>
</tr>
<tr>
<td></td>
<td>• For all devices, after configuring SNMPv3 on the device, configure the following setting:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server host event_collector_IP traps version 3 noauth MyNoAuthUsr</code></td>
</tr>
</tbody>
</table>
### SNMP Informs

SNMP Informs can be configured for all SNMPv3 modes. The following is an example for configuring SNMPv3 Informs for the mode SNMPv3 With Privacy and Authentication. The configuration is similar for the other modes (refer to the required settings for each mode for guidelines).

**Note** For Informs, *MyUsr* corresponds to Prime Network’s local user (not the device-configured user that is used for polling and receiving traps).

- For Cisco IOS, Cisco IOS XE, and CatOS devices:
  ```
  snmp-server user MyUsr MyGrp remote event_collector_IP v3 auth {md5|sha} MyAuthPswd priv {des|aes 128|aes 192|aes 256} MyPrivPswd
  ```

- For Cisco IOS XR devices:
  ```
  snmp-server user MyUsr MyGrp remote event_collector_IP v3 auth {md5|sha} {WORD,CLEAR,encrypted} MyAuthPswd priv {des|aes 128|aes 192|aes 256} {WORD,CLEAR,encrypted} MyPrivPswd SystemOwner
  ```

- For all devices, after configuring SNMPv3 on the device, configure the following setting:
  ```
  snmp-server host event_collector_IP informs version 3 priv MyUser
  ```

### Recommended and Optional SNMP Settings for Cisco IOS XR Devices

In large-scale environments that contain more than 100 EFPs or PWs associated with the same interface/subinterface, an interface outage may generate a large number syslogs and traps. In such scenarios we recommended that you increase the default snmp server queue length buffer size using the following command. This applies to Cisco IOS XR 4.0 and later. The value of *new-buffer-size* should at least equal the number of EFP or PW objects. (This increase is also advisable if traps are being used as a transport mechanism for syslogs by way of the CISCO-SYSLOG-MIB.)

```
snmp-server queue-length new-buffer-size
```

If a Cisco IOS XR device has a configured virtual IP address and the VNE was added using that address, the device can receive the traps and syslogs through the virtual IP address. You do not need to configure the source for the SNMP traps and syslogs in the Prime Network Administration GUI client, as described in VNE Events Settings, page 19-42. The following are examples of commands for configuring a virtual IP address:

```
ipv4 virtual address 10.49.224.120 255.255.255.128
ipv4 virtual address use-as-src-addr
```

To enable all traps to be sent from a Cisco IOS XR device:

```
snmp-server traps <CR>
```

Alternatively, choose from the following list to enable forwarding of specific traps from Cisco IOS XR devices:

- `snmp-server trap link ietf`
- `snmp-server traps rf`
- `snmp-server traps bfd`
- `snmp-server traps ethernet cfm`
- `snmp-server traps ds1`
- `snmp-server traps ds3`
- `snmp-server traps ntp`
- `snmp-server traps ethernet oam events`
- `snmp-server traps otn`
- `snmp-server traps copy-complete`
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
snmp-server traps snmp coldstart
snmp-server traps snmp warmstart
snmp-server traps snmp authentication
snmp-server traps flash removal
snmp-server traps flash insertion
snmp-server traps sonet
snmp-server traps config
snmp-server traps entity
snmp-server traps syslog
snmp-server traps system
snmp-server traps ospf lsa lsa-maxage
snmp-server traps ospf lsa lsa-originate
snmp-server traps ospf errors bad-packet
snmp-server traps ospf errors authentication-failure
snmp-server traps ospf errors config-error
snmp-server traps ospf errors virt-bad-packet
snmp-server traps ospf errors virt-authentication-failure
snmp-server traps ospf errors virt-config-error
snmp-server traps ospf retransmit packets
snmp-server traps ospf state-change if-state-change
snmp-server traps ospf state-change neighbor-state-change
snmp-server traps ospf state-change virtif-state-change
snmp-server traps ospf state-change virtneighbor-state-change
snmp-server traps bridgemib
snmp-server traps isis all
snmp-server traps bgp
snmp-server traps frame-relay pvc interval 30
snmp-server traps atm pvc interval 30
snmp-server traps ima
snmp-server traps hsrp
snmp-server traps vrrp events
snmp-server traps vpls all
snmp-server traps vpls status
snmp-server traps vpls full-clear
snmp-server traps vpls full-raise
snmp-server traps 12vpn all
snmp-server traps 12vpn vc-up
snmp-server traps 12vpn vc-down
snmp-server traps mpls traffic-eng up
snmp-server traps mpls traffic-eng down
snmp-server traps mpls traffic-eng reroute
snmp-server traps mpls traffic-eng reoptimize
snmp-server enable traps mpls frr all
snmp-server enable traps mpls frr protected
snmp-server enable traps mpls frr unprotected
snmp-server traps mpls idp up
snmp-server traps mpls idp down
snmp-server traps mpls idp threshold
snmp-server traps mpls traffic-eng p2mp up
snmp-server traps mpls traffic-eng p2mp down
snmp-server traps rsvp all
snmp-server traps rsvp new-flow
snmp-server traps rsvp lost-flow
snmp-server enable traps mpls l3vpn all
snmp-server enable traps mpls l3vpn vrf-up
snmp-server enable traps mpls l3vpn vrf-down
snmp-server enable traps mpls l3vpn max-threshold-cleared
snmp-server enable traps mpls l3vpn max-threshold-exceeded
snmp-server enable traps mpls l3vpn mid-threshold-exceeded
snmp-server enable traps mpls l3vpn max-threshold-reissue-notif-time 1
snmp-server traps fabric plane
Syslogs—Required Device Settings

The following table lists the settings you must configure for syslogs.

<table>
<thead>
<tr>
<th>Required Settings</th>
<th>All</th>
<th>Cisco CatOS, Cisco IOS, and Cisco IOS XE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>logging source-interface interface_name1</td>
<td>logging on</td>
</tr>
<tr>
<td></td>
<td>logging gateway_IP</td>
<td>logging buffered 64000 informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logging trap informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logging event link-status default</td>
</tr>
</tbody>
</table>

Required for ASR 1000 IPSec Syslogs:

| crypto logging session |

Note If a device supports MPLS TP, enable the following configurations to make sure Prime Network is properly notified of MPLS TP-related changes:

- mpls tp
- [no] logging events
- [no] logging config-change

If you are using reduced polling, be sure the follow the requirements in this section. These settings increase the depth of syslogs that will be logged, and ensures that all syslogs are handled. If the device is using Cisco IOS XR, verify the syntax of the settings against the Cisco IOS XR documentation in case there have been changes across OS releases.

snmp-server traps fabric bundle link
snmp-server traps fabric bundle state
snmp-server traps sensor
snmp-server traps fru-ctrl
### IP Address Configuration for Traps, Syslogs, and VNEs

Traps and syslogs maybe dropped if any of the VNEs managed by Prime Network are configured in such a way that the following addresses are different:

- The traps and syslogs source IP address
- The VNE IP address (entered when the VNE was created and displayed in the VNE properties)

To avoid missing any traps or syslogs, do one of the following:

- Change the device configuration so that traps and syslogs are sent using the VNE’s IP address. In addition, make sure that the source IP address matches the startup-config.
- Configure the VNE to receive traps and syslogs using a different IP address by changing the VNE Events Settings, page 19-42.

#### Required Settings

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XR</td>
<td><code>logging events level informational</code></td>
</tr>
<tr>
<td></td>
<td><code>logging buffered &lt;307200-125000000&gt;</code></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The range indicates the minimum of 307200 and maximum of 125000000 log messages that can be stored on the device.</td>
</tr>
<tr>
<td></td>
<td><code>logging trap informational</code></td>
</tr>
<tr>
<td></td>
<td><code>logging events link-status software-interfaces</code></td>
</tr>
<tr>
<td></td>
<td>If you will be using Path Tracer or event correlation to mimic flows that involve bridge tables, configure the following:</td>
</tr>
<tr>
<td></td>
<td><code>l2vpn resynchronize forwarding mac-address-table location node-id</code></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If devices are running an older version of Cisco IOS XR, enable the following commands to make sure Prime Network is properly notified of link status changes:</td>
</tr>
<tr>
<td></td>
<td><code>logging events link-status logical</code></td>
</tr>
<tr>
<td></td>
<td><code>logging events link-status physical</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nexus Devices</th>
<th>Either of these commands can be used</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>logging server gateway-IP use-vrf management-VRF</code></td>
</tr>
<tr>
<td></td>
<td><code>logging server gateway-IP facility use-vrf management-VRF</code></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td><code>management-VRF</code> is the VRF which is associated with the management IP address of the Nexus switch.</td>
</tr>
</tbody>
</table>

1. Required if the device has a management IP address. `interface_name` is the active management IP address.
Cisco Carrier Packet Transport Devices

The following settings are required for Prime Network to properly model Cisco Carrier Packet Transport devices.

These settings should be configured using the Packet Transport System View GUI.

- The SNMP host settings must set in the Provisioning tab (in the SNMP area).
- The Syslogs destinations must be set in the Maintenance tab (in the Syslog area).

For information on how to configure CPT devices using the Packet Transport System View, see the Cisco Carrier Packet Transport documentation.

These settings should also be configured:

- For Cisco IOS devices, set the following command so that Prime Network can determine the mode used by the CPT device:

  service internal

- Configure the following snmp community setting on the NGXP card:

  `snmp-server community cellbus RO`

If a device is running in CTC mode, the following is not supported:

- Reduced (event-based) polling
- Syslogs and trap event notifications that are disabled by default
Prime Network Log Files

The following topics describe the logs maintained by Prime Network, and the overall logging mechanism and customizable points:

- How Prime Network Saves Log Files, page B-1
- Changing Log File Behavior, page B-2
- Log Files, page B-2

How Prime Network Saves Log Files

Each Prime Network module writes a log file to its own folder within the NETWORKHOME/Main/logs folder. Log sizes are limited to 4 MB by default. When a log file reaches its maximum size, Prime Network does the following:

- Zips the log file and appends a number to the backup file.
- Starts a new log file.

In the following example, the oldest file is process.log.2.gz, and process.log is the current log file.

<table>
<thead>
<tr>
<th>Time</th>
<th>Size</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:42 PM</td>
<td>4,481,607</td>
<td>process.out</td>
</tr>
<tr>
<td>07:22 AM</td>
<td>5,120,447</td>
<td>process.out.1.gz</td>
</tr>
<tr>
<td>03:17 AM</td>
<td>5,120,105</td>
<td>process.out.2.gz</td>
</tr>
</tbody>
</table>

When process.log exceeds the maximum size, the following happens:

- The contents of process.out.2.gz are moved to process.log.3.gz.
- The contents of process.out.1.gz are moved to process.log.2.gz.
- The contents of process.out are moved to process.log.1.gz.
- A new log files is started (process.log).

Prime Network saves a maximum of 10 log files for each process. When the number of backups exceeds 10, the oldest file is deleted.

You can change the maximum log file size and the maximum number of backup log files by following the procedure in Changing Log File Behavior, page B-2.

For a complete list of log files, see Log Files, page B-2.
Log Files and Server Restarts

Whenever the Prime Network server is restarted, all log files are moved to NETWORKHOME/Main/logs/old.

Prime Network saves a maximum of 3 “older” sets of log files in these directories:
NETWORKHOME/Main/logs/old
NETWORKHOME/Main/logs/older
NETWORKHOME/Main/logs/oldest

For example, if a newly-installed Prime Network gateway server has been restarted once, the following happens:

- The contents in NETWORKHOME/Main/logs are moved to NETWORKHOME/Main/logs/old.
- The latest log files are stored in NETWORKHOME/Main/logs.

If the gateway server is restarted a second time, the following happens:

- The contents in NETWORKHOME/Main/logs/older are moved to NETWORKHOME/Main/logs/oldest.
- The contents in NETWORKHOME/Main/logs/old are moved to NETWORKHOME/Main/logs/older.
- The latest log files are stored in NETWORKHOME/Main/logs.

For a complete list of log files, see Log Files, page B-2.

Changing Log File Behavior

Log file behavior is managed by the settings in NETWORKHOME/Main/scripts/log.pl. To change the number of log files that are saved, or to change the maximum log size, change the following settings in log.pl:

```
$LASTLOGINDEX = 10;               # max file index to backup.
$MAXSIZE = 1024*1024*4;          # max file size – hitting that size will cause rollover
```

You must restart the gateway server for your changes to take effect.

For a complete list of log files, see Log Files, page B-2.

Log Files

Table B-1 lists the log files that are stored on the gateway server. You can view these files using any text editor.

<table>
<thead>
<tr>
<th>Gateway Server Log File</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Files Located in NETWORKHOME/Main/logs</td>
<td></td>
</tr>
<tr>
<td>0.out</td>
<td>Switch Virtual Machine (handles communication with unit servers)</td>
</tr>
<tr>
<td>11.out</td>
<td>Gateway server</td>
</tr>
<tr>
<td>25.out</td>
<td>Event persistence</td>
</tr>
</tbody>
</table>
### Table B-1  Gateway Server Log Files (continued)

<table>
<thead>
<tr>
<th>Gateway Server Log File</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>35.out</td>
<td>Gateway server (CE service discovery)</td>
</tr>
<tr>
<td>66.out</td>
<td>Workflow Engine</td>
</tr>
<tr>
<td>76.out</td>
<td>Jobs scheduler</td>
</tr>
<tr>
<td>77.out</td>
<td>Change and Configuration Management</td>
</tr>
<tr>
<td>78.out</td>
<td>VNE topology</td>
</tr>
<tr>
<td>83.out</td>
<td>TFTP server (Change and Configuration Management)</td>
</tr>
<tr>
<td>84.out</td>
<td>Report manager</td>
</tr>
<tr>
<td>99.out</td>
<td>Management Virtual Machine (unit server management)</td>
</tr>
<tr>
<td>100.out</td>
<td>Event Collector</td>
</tr>
<tr>
<td>nnn.out</td>
<td>User-created AVM nnn management</td>
</tr>
<tr>
<td>nnn.log.restartx</td>
<td>AVM restart information for AVM nnn (x can be 1-5)</td>
</tr>
<tr>
<td>drivers/ivne-install-log-\texttt{mmddyy-hhmNSS}</td>
<td>Device Package installation log (web repository or local folder)</td>
</tr>
<tr>
<td>drivers_rollback_{\texttt{mmddyy-hhmNSS}}.log</td>
<td>Device Package rollback log</td>
</tr>
<tr>
<td>drivers_backup_{\texttt{mmddyy-hhmNSS}}.log</td>
<td>Device Package backup log</td>
</tr>
<tr>
<td>emdb.log</td>
<td>Logs related to embedded Oracle database</td>
</tr>
<tr>
<td>haevents.log</td>
<td>Unit server high availability events</td>
</tr>
<tr>
<td>license_server.log</td>
<td>License server</td>
</tr>
<tr>
<td>mvm.log</td>
<td>System restart log</td>
</tr>
<tr>
<td>mvmcsh.log</td>
<td>System restart log (units) (for units, indicates if files were properly copied from gateway on unit restart)</td>
</tr>
<tr>
<td>old (directory)</td>
<td>Logs from last session</td>
</tr>
<tr>
<td>older (directory)</td>
<td>Logs from 2 sessions earlier</td>
</tr>
<tr>
<td>oldest (directory)</td>
<td>Logs from 3 sessions earlier</td>
</tr>
<tr>
<td>vneCreation-\texttt{mmddyy-hhmNSS}.txt</td>
<td>vne_creation_script.pl log file (short format)</td>
</tr>
<tr>
<td>vneCreation-\texttt{mmddyy-hhmNSS}.verbose</td>
<td>vne_creation_script.pl log file (verbose format)</td>
</tr>
</tbody>
</table>

#### Log Files Located in /var/adm/cisco/prime-network/logs

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install-log-\texttt{xxxxxxxxxxxxX}</td>
<td>Prime Network installation log</td>
</tr>
<tr>
<td>uninstall-log-\texttt{xxxxxxxxxxxxX}</td>
<td>Prime Network uninstallation log</td>
</tr>
<tr>
<td>verbose-\texttt{xxxxxxxxxxxxX}</td>
<td>Prime Network installation log (verbose format)</td>
</tr>
<tr>
<td>verbose-uninstall-\texttt{xxxxxxxxxxxxX}</td>
<td>Prime Network uninstallation log (verbose format)</td>
</tr>
</tbody>
</table>

#### Other Log Files

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\texttt{ORACLE_BASE}/ana_logs</td>
<td>Prime Network embedded database log</td>
</tr>
<tr>
<td>$\texttt{FLEXNET_HOME}/logs</td>
<td>Prime Network license log (Flexnet and liccontrol)</td>
</tr>
</tbody>
</table>
Log files for Prime Network Change and Configuration Management are described in the *Cisco Prime Network 3.9 Change and Configuration Management User Guide*.

**Table B-1  Gateway Server Log Files (continued)**

<table>
<thead>
<tr>
<th>Gateway Server Log File</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>directory/scriptlogxxx.txt</td>
<td>Log file for vne_creation_script.pl (for bulk VNE import). directory is the directory from which the script was run and xxx is the suffix that was specified when the command was issued.</td>
</tr>
<tr>
<td>NETWORKHOME/.replication</td>
<td>Used for ADG gateway geographical redundancy to record local and remote timestamps used by GWSync.</td>
</tr>
<tr>
<td>NETWORKHOME/.replication_remote</td>
<td>Used for ADG gateway geographical redundancy to log when local and remote timestamps are more than 10 minutes apart (and a System event is generated).</td>
</tr>
<tr>
<td>NETWORKHOME/.replication_log</td>
<td>Used for ADG gateway geographical redundancy to log when local and remote timestamps are more than 10 minutes apart (and a System event is generated).</td>
</tr>
<tr>
<td>NETWORKHOME/oracle_monitoring.log</td>
<td>Used for ADG gateway geographical redundancy to provide information on the Redo-apply log from the standby server.</td>
</tr>
<tr>
<td>NETWORKHOME/Main/network-conf-xxxxxx.log</td>
<td>Output of network-conf portion of installation session</td>
</tr>
<tr>
<td>NETWORKHOME/Main/ha/logs</td>
<td>Gateway server high availability</td>
</tr>
<tr>
<td>NETWORKHOME/Main/mvmcsh.log</td>
<td>Used for debugging purposes</td>
</tr>
<tr>
<td>NETWORKHOME/restarts.log</td>
<td>Used for debugging purposes</td>
</tr>
<tr>
<td>/var/log/messages</td>
<td>Used for RHCS local gateway redundancy</td>
</tr>
<tr>
<td>/varVRTSvcs/log</td>
<td>Veritas log files (gateway server high availability)</td>
</tr>
</tbody>
</table>

1. xxxxxxxxxx is a random unique identifier.
APPENDIX C

Working with the Registry

The following topics provide an introduction to the Prime Network registry and common settings you may want to customize:

- Overview of the Prime Network Registry, page C-1
- Changing Registry Settings Using runRegTool.sh, page C-2

Overview of the Prime Network Registry

The Prime Network registry is a collection of xml files (called hives) that comprise and control the Prime Network system configuration. The registry contains almost all definitions and configurations used by Prime Network. A copy of the registry is located on the gateway server and every unit in the following location:

NETWORKHOME/Main/registry/

Registry files are made up of key names and entry names. The following file fragment shows some key and entry names in the pollinggroups.xml registry file:

```
<key name="pollinggroups">
  <key name="default">
    <key name="buffering">
      <entry name="interval">190000</entry>
    </key>
    <key name="configuration">
      <entry name="interval">900000</entry>
    </key>
  </key>
</key>
```

In this example, the registry key path for the buffering interval would be:

pollinggroups/default/buffering/interval

where pollinggroups is the name of the hive, default is a subkey of the root key, buffering is a subkey of buffering, and so forth.

The registry files on the gateway server and units are replicas of the Golden Source registry. The Golden Source registry is the master registry that is responsible for maintaining, distributing, and updating registry configuration files to all units and the gateway server. The Golden Source registry is centrally located on the gateway server. Whenever a unit or gateway restarts, it accesses the Golden Source registry to retrieve any updates to the configuration. If a unit cannot connect to the gateway, it uses its local copy of the registry files.

The master copy of the Golden Source files is centrally located on the gateway server at:

NETWORKHOME/Main/registry/ConfigurationFiles
The contents are:

<table>
<thead>
<tr>
<th>Subdirectory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/0.0.0.0</td>
<td>Template directory, which is used by the system. This directory on the</td>
</tr>
<tr>
<td></td>
<td>gateway server is the Golden Source registry.</td>
</tr>
<tr>
<td>/127.0.0.1</td>
<td>Gateway directory</td>
</tr>
<tr>
<td>/unit-IP-address</td>
<td>Unit directory (one for each unit)</td>
</tr>
</tbody>
</table>

The subfolders are created during the installation procedure. Each subfolder contains the relevant registry .xml files. These files can be edited as described in Changing Registry Settings Using runRegTool.sh, page C-2.

All Golden Source subdirectories contain a file called site.xml. This file contains registry settings that have been customized. When the system restarts, these settings are copied to (and override) all other Golden Source directories. For this reason, it is important to make customizations to this file, so that in case of restart, your customizations are not overwritten by the system defaults. Every key and entry in the Golden Source can be overridden by an entry in site.xml; the only

The Golden Source mechanism enables consistent management of the entire system. Each unit and gateway has its own set of registry configuration files and parameters. The registry files are replicated automatically during the installation of the unit and gateway.

Each time a unit and gateway process starts, it accesses the Golden Source and retrieves the updated configuration. All additions and changes to the Golden Source are automatically sent to the relevant units servers. Each unit keeps a local copy of its relevant registry files. When a unit cannot connect to the gateway, the unit’s local copy of the registry is used.

**Changing Registry Settings Using runRegTool.sh**

**Note**

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

You can change registry settings using the `runRegTool.sh` script, which is located in \NETWORKHOME\Main, using the following command format:

```
runRegTool.sh -gs hostname-IP command unit-IP key [value]
```
The `runRegTool.sh` script takes the following options.

<table>
<thead>
<tr>
<th>Argument/Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>gs</code></td>
<td>Performs a registry command using the Golden Source.</td>
</tr>
<tr>
<td><code>hostname-IP</code></td>
<td>IP address of the gateway server or unit server where the golden source is located. In most cases the golden source is on the gateway server; you can use the gateway IP address or the address <code>127.0.0.1</code>.</td>
</tr>
<tr>
<td><code>command</code></td>
<td>The <code>runRegTool.sh</code> script registry command:</td>
</tr>
<tr>
<td></td>
<td>- <code>set</code>—Sets a registry key named <code>key</code> to a new value of <code>value</code></td>
</tr>
<tr>
<td></td>
<td>- <code>setEncrypted</code>—Sets and encrypts the registry key named <code>key</code> to <code>value</code></td>
</tr>
<tr>
<td></td>
<td>- <code>unset</code>—Returns a registry key named <code>key</code> to its default value</td>
</tr>
<tr>
<td></td>
<td>- <code>add</code>—Adds a new registry key named <code>key</code> with a value of <code>value</code></td>
</tr>
<tr>
<td></td>
<td>- <code>remove</code>—Deletes a registry key named <code>key</code></td>
</tr>
<tr>
<td></td>
<td>- <code>list</code>—Lists all registry keys under a given <code>key</code></td>
</tr>
<tr>
<td></td>
<td>- <code>get</code>—Retrieves the value of a registry key named <code>key</code></td>
</tr>
<tr>
<td><code>unit-IP</code></td>
<td>IP address of the destination to which the changes should be written, according to these guidelines:</td>
</tr>
<tr>
<td></td>
<td>- Gateway server changes (<code>hostname-ip</code> is the gateway server):</td>
</tr>
<tr>
<td></td>
<td>- Use <code>unit-IP 127.0.0.1</code> for <code>get</code> commands.</td>
</tr>
<tr>
<td></td>
<td>- Use <code>unit-IP 127.0.0.1</code> for all commands on AVMs (reserved AVMs or user-created AVMs).</td>
</tr>
<tr>
<td></td>
<td>- Use <code>unit-IP 0.0.0.0</code> for all other command instances.</td>
</tr>
<tr>
<td><code>key</code></td>
<td>Registry entry name consisting of the XML file name, the key name(s), and entry.</td>
</tr>
<tr>
<td></td>
<td>- For all user-created AVMs, use this format, where <code>avm.xxx</code> is the AVM on which the VNE resides, and <code>vne-key</code> is the VNE name used by Prime Network. The <code>site/</code> prefix is not required for reserved AVMs. <code>avm.xxx/agents/da/vne-key/...</code></td>
</tr>
<tr>
<td></td>
<td>- For all other registry keys, precede the key string with <code>site/</code> so that changes are made to (or values are checked against) the local site.xml file: <code>site/key</code></td>
</tr>
<tr>
<td><code>value</code></td>
<td>The new value for the registry entry.</td>
</tr>
</tbody>
</table>

**Note** Registry changes should be made to the site.xml file, except for changes being made to AVM XML files. Therefore, your command syntax should always include `site` as the first part of the key name (this is not required for `get` or `list` commands):
The following are some examples of how to use the `runRegTool.sh` script:

- This `get` command returns the current settings for all polling groups on the unit with the IP address `unit-IP`. It uses the `site/` prefix in case any customizations have been performed:
  
  ```bash
  # ./runRegTool.sh -gs hostname-IP get unit-IP site/pollinggroups
  ```

- This `set` command configures the LDP Neighbor Down event to `not` persist its alarm information. Note that `site` precedes the key so that customizations are made locally:
  
  ```bash
  # ./runRegTool.sh -gs gateway-IP set unit-IP
  "site/event-persistency-application/events/LDP neighbor loss/sub-types/LDP neighbor
down/alarm-persistency" unpersist
  ```

- This `get` command returns the current adaptive polling settings for a VNE with the ID CRS1-local, that runs on AVM 521. Because the change is made to a user-created VNE, the key is not preceded with `site`.

  ```bash
  # ./runRegTool.sh -gs hostname-IP get unit-IP
  "avm521/agents/da/CRS1-local/dcs/type/com.sheer.metrocentral.coretech.common.dc.Manage
dElement/adaptivePolling"
  ```
**Numerics**

6PE, 6VPE 19-6
6RD 19-6

**A**

Access List 19-6

adaptive polling
  Cisco IOS XR devices and 22-21
  configuring 19-42
  customizing 22-17, 22-18
  overview 22-15
  turning off 19-42

add_db_storage_for_tablespace (embedded database) 11-6
add_emdb_storage (embedded database) 11-5
ADG (Oracle Active Data Guard). See high availability, gateway (RHCS/ADG)
Administrator (user access role) 7-3
admin status, AVM 4-5
Agent Not Loaded (VNE communication state) 19-3, 20-5
Agent Unreachable (VNE communication state) 19-3, 20-5
ALARM database table 10-2
alarms
  database purging 10-1, 11-1
  persistency 26-2
  saving in database 10-1, 11-1
  scopes and 7-3
  system shutdown and 26-2
  user roles and 7-2
anact1_ha (Veritas gateway high availability) 17-9
ANAHOME (default) 2-1
AOP (Automatic Overload Prevention) 9-17

archiving vs. purging 10-6, 10-9
ARP 19-7, 19-30
ATM 19-6
ATM PW 19-6
AUDITEVENT database table 10-2
authentication, user 7-20
  choosing 7-20
  external
    changing 7-2, 7-14
    configuring 7-7
    emergency user 7-2
    GUI client 1-27
    overview 7-2, 7-7
    problems 7-14
LDAP configuration 7-10
  overview 7-1
Prime Network 7-2, 7-7
Authentication Method (GUI client) 1-27
auto-add
  AVMs 4-4
  VNEs 19-11, 19-14, 19-17
Automatic AVM Management (GUI client) 1-18
AVM 0 4-3, 4-8, 16-4
AVM 100 3-5, 4-3, 6-7, 9-2, 10-2, 13-4, 14-1, 14-6, 16-4, 16-6
  overview 14-3
  unit server high availability and 16-3
  See also Event Collector
AVM 11 4-3, 10-3, 10-10, 16-4
AVM 19 4-3
AVM 25 4-3, 14-1, 14-5, 14-6, 14-15, 16-4
  impact of failure 16-5
  overview 14-5
  proxy AVM 25 14-15
Index

AVM 35 4-3, 16-5
AVM 66 4-3, 12-1, 16-4, 16-5
AVM 76 4-3, 16-5
AVM 77 4-3, 16-4, 16-5
AVM 78 4-3, 16-5
AVM 83 4-3, 16-5
AVM 84 4-3, 16-6
AVM 99 4-3, 4-8, 16-4, 16-6
AVM protection 4-7, 4-8
  configuring, AVMs 16-10
  impact of failure 16-4
  impact of timeouts and restarts 16-6
  overview 16-1
  watchdog protocol 16-1
AVMs
  adding 4-8, 4-9
  auto-add 4-3
  automanagement 1-18
  configuring AVM protection 16-10
  description of 4-2
  diagnostics 4-11
  failover 16-1
  failure, impact 16-4
  gateway AVMs 4-3
  GUI client and 1-14
  load balancing 4-4, 4-11
  log files B-2, B-3
  memory allocation 4-2
  moving 4-13
  properties 4-6
  protection. See AVM protection
  starting and stopping 4-12
  status (admin and oper) 4-5
  status (networkctl) 2-3
  timeouts and restarts 16-6
  unit AVMs 4-3
  user-created 16-4

B
backup
  database, embedded 11-10
  default backup location 11-11
  enabling 11-11
  manual 11-12
  number of backups saved 11-10
  overview 11-10
  database, external 8-1
Prime Network data 8-1
  backed-up content 8-1
  changing schedule 8-3
  data that is backed up 8-1
  default backup location 8-2
  manual 8-4
  number of backups saved 8-2
  overview 8-1
  schedule 8-2
Backup Pseudowire 19-6
backup time
  database, embedded
  change 11-12, 11-13
banners
  creating 2-5
  Message of the Day (GUI client) 1-22
  removing 2-5
BFD 19-6
BGP 19-6
bosenable, bosconfig, bosusermanager passwords 15-4
BQL
  port 13-3
  security 13-3

C
CatOS. See Cisco CatOS VNEs
CDP 19-7
CEM Group 19-7
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFM 19-7</td>
</tr>
<tr>
<td>CGN 19-7</td>
</tr>
<tr>
<td>Change and Configuration Management</td>
</tr>
<tr>
<td>AVM 77 and 4-3</td>
</tr>
<tr>
<td>AVM 83 and 4-3</td>
</tr>
<tr>
<td>changing gateway IP 9-21</td>
</tr>
<tr>
<td>database scheme 10-3</td>
</tr>
<tr>
<td>database tables 10-1</td>
</tr>
<tr>
<td>log file B-3</td>
</tr>
<tr>
<td>Cisco Carrier Packet Transport VNEs A-15</td>
</tr>
<tr>
<td>Cisco CatOS VNEs A-2, A-10, A-11, A-13</td>
</tr>
<tr>
<td>Cisco documentation, obtaining xvii</td>
</tr>
<tr>
<td>Cisco Nexus VNEs A-9, A-14</td>
</tr>
<tr>
<td>prerequisites for adding VNEs 19-13</td>
</tr>
<tr>
<td>VDC configuration A-7</td>
</tr>
<tr>
<td>Clocking Enhancements 19-7</td>
</tr>
<tr>
<td>clone VNEs 19-14</td>
</tr>
<tr>
<td>Cloud VNEs</td>
</tr>
<tr>
<td>adding 15-5, 19-21</td>
</tr>
<tr>
<td>communication states and 19-3, 19-4</td>
</tr>
<tr>
<td>configuring duplicate IP addresses 23-3</td>
</tr>
<tr>
<td>creating 19-29</td>
</tr>
<tr>
<td>editing properties 19-43</td>
</tr>
<tr>
<td>Ethernet 23-2</td>
</tr>
<tr>
<td>investigation states and 19-4</td>
</tr>
<tr>
<td>overview 23-1</td>
</tr>
<tr>
<td>populating 23-3</td>
</tr>
<tr>
<td>static links and 23-8</td>
</tr>
<tr>
<td>clustat (RHCS/ADG gateway high availability) 18-6</td>
</tr>
<tr>
<td>clusvcadm (RHCS/ADG gateway high availability) 18-6</td>
</tr>
<tr>
<td>collectors, VNE</td>
</tr>
<tr>
<td>activation scripts and 25-3</td>
</tr>
<tr>
<td>command priorities 25-2, 25-4</td>
</tr>
<tr>
<td>expedited commands and 25-3</td>
</tr>
<tr>
<td>fast collectors 25-2, 25-5</td>
</tr>
<tr>
<td>overview 25-1</td>
</tr>
<tr>
<td>communication states, VNEs 19-1, 19-3, 20-3, 24-1, 24-2</td>
</tr>
<tr>
<td>Configuration polling, VNEs 19-40, 22-1</td>
</tr>
<tr>
<td>Configurator (user access role) 7-3</td>
</tr>
<tr>
<td>Connecting (VNE communication state) 19-4, 20-5</td>
</tr>
<tr>
<td>conventions, in this guide xvii</td>
</tr>
<tr>
<td>CPT. See Cisco Carrier Packet Transport devices</td>
</tr>
<tr>
<td>CPU utilization problems. See polling</td>
</tr>
<tr>
<td>CSC (Carrier Supporting Carrier) 19-7</td>
</tr>
<tr>
<td>CSV method for adding VNEs 19-7</td>
</tr>
<tr>
<td>Currently Unsynchronized (VNE investigation state) 19-5, 20-18, 20-22, 22-2, 22-15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>database 10-1</td>
</tr>
<tr>
<td>administrative 10-3</td>
</tr>
<tr>
<td>archiving 10-9</td>
</tr>
<tr>
<td>backup. See backup</td>
</tr>
<tr>
<td>Change and Configuration Management 10-3</td>
</tr>
<tr>
<td>embedded. See embedded database</td>
</tr>
<tr>
<td>Event Archive 10-2</td>
</tr>
<tr>
<td>log file B-3</td>
</tr>
<tr>
<td>password, changing 15-1</td>
</tr>
<tr>
<td>purging 10-1, 10-4, 10-6, 11-1</td>
</tr>
<tr>
<td>integrity tests 10-6</td>
</tr>
<tr>
<td>schedule 10-5</td>
</tr>
<tr>
<td>schemas 10-1</td>
</tr>
<tr>
<td>security 13-1, 13-3</td>
</tr>
<tr>
<td>tables 10-1, 10-3</td>
</tr>
<tr>
<td>time zones 10-1</td>
</tr>
<tr>
<td>workflows 10-2</td>
</tr>
<tr>
<td>default (polling group) 22-22</td>
</tr>
<tr>
<td>default installation directory 2-1</td>
</tr>
<tr>
<td>Defined Not Started (VNE investigation state) 19-5, 20-18</td>
</tr>
<tr>
<td>deployment plan (system) 1-1</td>
</tr>
<tr>
<td>Device Packages</td>
</tr>
<tr>
<td>applying to VNE 21-4, 21-7</td>
</tr>
<tr>
<td>checking for new DPs 21-2</td>
</tr>
<tr>
<td>downloading 21-6</td>
</tr>
</tbody>
</table>
Device Packages (continued)
  installed, indentifying 21-3
  installing 21-6
  overview 21-1
  troubleshooting installation 21-8
  uninstalling 21-7
  used by VNE, indentifying 21-4
Device Partially Reachable (VNE communication state) 19-4, 20-5
device reachability 24-5
  communication states (VNE) and 19-1
  HTTP 19-39, 24-7
  ICMP 24-6
  overview 20-1, 24-1
  policies, controlling 24-1, 24-2
  SNMP 24-3
  Telnet 24-5
  XML 19-38
Device Reachable (VNE communication state) 19-4, 20-5
disabling user accounts 7-22
Disconnected
  AVM stats 4-5
  VNE status 4-15
Discovering (VNE investigation state) 19-5, 20-18
discovery
  commands 25-1
  communication states (VNE) and 19-3, 20-3
  investigation states (VNE) and 19-1, 19-4, 20-14
  triggers 19-4, 20-16, 22-2
  See also collectors, VNE
document
  contents xiv
  conventions xvii
  organization xiv
documentation, obtaining xviii
Down
  AVM status 4-5
  VNE status 4-15
DSx 19-7
dynamic links. See links

E

EFP 19-7
embedded database
  add_db_storage_for_tablespace utility 11-6
  add_emdb_storage utility 11-5
  backup. See backup
disk usage 11-7
  emdbctl (control utility) 11-3
  error messages 11-2
  logs 11-1
  purging data 11-7
  restarting (RHCS/ADG gateway high availability) 18-3
  restore. See restore
tablespace usage 11-7
  emdbctl (embedded database) 11-3
emergency user, LDAP 7-2
ensure-management (VNE communication policy) 24-1
Ethernet (technology) 19-7
Ethernet Channel 19-7
Ethernet LMI 19-7
Ethernet OAM 19-7
Event Archive
  AVM 25 and 4-3
database scheme 10-2
database tables 10-1, 10-2
disabling and enabling 14-16
Event Collector and 14-1
purging data 10-6
Event Collector
  AVM 100 and 4-3
  AVM 25 and 14-5, 14-15
default 14-3
default examples 14-6
Fault Agent 14-5
log file B-3
multiple 14-10, 14-12
new VNEs and 14-15
on gateway 14-11
on unit 14-11
overview 14-1
single 14-6, 14-11
VNEs and 14-4
event listener. See Event Collector
Event Management Settings (GUI client) 1-19
event notification service
  configuring 6-3
deleting existing 6-2
editing existing 6-2
GUI client 1-16
overview 6-1
viewing existing services 6-2
events
  filtering 9-17, 14-3
  high availability, unit 16-11
  licensing 5-6
polling and 22-2
purging from database 10-1, 10-6, 11-1
time zones 10-1
external authentication. See authentication, user

F
fail-safe mechanism (reduced polling) 22-14
Fault Agent 4-3
Fault Database
database tables 10-2
Event Collector and 14-1
purging data 10-6
firewalls 9-2
device proxy, configuring 9-2
devices and 13-4
gateway and 13-4
managed devices behind 9-2
servers and units behind 9-2
units and 13-4
Frame Relay 19-7

G
gateway
  AVM 4-3
  AVMs installed on 4-3
changing IP address 9-21
firewalls and 9-2, 13-4
GUI client and 1-9, 1-11
log file B-2, B-3
overview 2-1
security 13-1, 13-2, 13-3
starting and stopping 2-3
viewing properties 2-2
gateway high availability. See high availability, gateway
General tab (VNE properties) 19-29
global event filter 9-17
Global Settings, GUI overview 1-17
GMT 2-1
Golden Source registry C-1
graphs. See diagnostics
GRE 19-7

H
HA/DR (High Availability/Disaster Recovery). See high availability, gateway
HDLC 19-7
high availability, gateway (RHCS/ADG) 18-1
  geographical redundancy
    ADG replication process 18-9
    architecture 18-8
    configuring 18-8
    failover scenarios 18-12
    GW Sync process 18-11
    LDAP and 18-12
    logs 18-14
    overview 18-8
    primeha command 18-15, 18-18, 18-20, 18-21
licensing and 5-2
local redundancy
  architecture 18-1
  configuring 18-2
  failover 18-4
  fencing devices 18-3
  IP addresses 18-3
  logs 18-5
  monitoring 18-5
  multicast addresses 18-4
  overview 18-1
  RHCS interfaces 18-5, 18-6
  switchover 18-4
Oracle, restarting 18-6
Prime Network, restarting 18-6
RHCS services 18-3

high availability, gateway (Veritas) 17-1
  geographical redundancy
    architecture 17-3
    configuring 17-13
    failover scenarios 17-19
    failover scenarios 17-19
    manual failover 17-17
    overview 17-13
  impact of failures 17-22
  licensing and 5-2
  local redundancy
    architecture 17-1
    configuring 17-6
    failover triggers 17-11
    overview 17-6
high availability, unit
  creating new 16-8
  estimating failure down time 16-4
  Event Collector and 14-8
  events 16-11
  impact of failure 16-4
  log file B-2, B-3
  overview 16-1, 16-2
  protection groups. See protection groups
    switching to standby unit
      automatically 16-9
      manually 16-9
  timeout machine failure 16-8
  timeout process failure 16-6
  watchdog protocol. See watchdog protocol
high CPU problems. See polling
HP_SYSLOG database table 10-2
HP_TRAP database table 10-2
HTTP
  determining protocol reachability 24-7
  VNE properties 19-39
HVPLS 19-7
ICMP
  changing communication policies 24-1, 24-2
  customizing testing 24-7
  determining protocol reachability 24-3, 24-6
  settings, VNEs 19-39
IMA 19-7
Independent VNE drivers. See VNEs, updating
installation directory, default 2-1
installation log files B-3
integrity tests (data purging) 10-6
investigation states, VNEs 19-1, 19-4, 20-14
IOS. See Cisco IOS VNEs
IOS XE. See Cisco IOS XE VNEs
IOX. See Cisco IOS XR VNEs
IP (technology) 19-7
IPoDWDM 19-7
IP Routing (technology) 19-7
IPSLA Responder 19-7
IPv6 19-7
ISIS 19-7
ISIS IGPv6 19-7

LDAP. See authentication, user
License Report (GUI client) 1-21, 5-5
licensing
  FlexNet server, managing 5-5
  license files
    installing 5-4
    obtaining 5-3
    verifying status 5-5
License Report (GUI client) 1-21
license server, controlling 5-6
log file B-3
overview 5-1
Prime Network upgrades and status, checking 5-5
System events 5-6
troubleshooting 5-5
links
  device scopes and 7-17
dynamic and static 23-1
See also Cloud VNEs
static
  creating 23-8
deleting 23-8
  validating 23-8
troubleshooting display 7-17
links, Topology GUI and 1-31
LLDP 19-7
load balancing (AVMs) 4-4, 4-11
Local Settings (VNE adaptive polling) 19-42
Local Switching 19-7
log files B-2
  and server restarts B-2
customizing B-2
default size B-1
  list of B-2
  overview B-1
logging in and out (Prime Network Administration) 1-4

L3 VPN and VRF 19-7
LAG 19-7, 23-9
Layer 1 polling, VNEs 19-40, 22-24
Layer 2
  polling, VNEs 19-40, 22-24
  VPN 19-8
Layer 3
  VPN 19-7
  VRF 19-7
M

Maintenance (VNE investigation state) 19-5, 20-19
maintenance mode, changing status 19-44
maps and user access 7-23
Martini (technology) 19-8
memory allocation (AVMs) 4-2
Message of the Day
  GUI overview 1-22
  managing 2-5
MLACP 19-6
MLPPP 19-7
MLPS P2MP TE 19-8
MONITOR database table 10-2
MP-BGP 19-7
MPLS 19-7
MPLS TE-Tunnel 19-8
MPLS TP 19-8
MST-AG 19-8
MSTP 19-8

N

navigation pane (Prime Network Administration window) 1-7
network38 2-1
network-conf 4-11, 9-7, 15-1, 18-3
networkctl
  running command on all units 15-5
  starting Prime Network gradually 9-5
  using 2-3, 3-4, 4-3
NEWTRAPEVENT database table 10-2
NETWORKHOME 2-1
network interface cards, dual 9-21
network-user
  database schemas and 10-1
database scheme 10-2
user account 2-1
NEWTRAPVALUE database table 10-2
Nexus. See Cisco Nexus VNEs
NICs, dual 9-21
notstrict (VNE communication policy) 24-1

O

Operational (VNE investigation state) 19-5, 20-18
operational status, AVM 4-5
Operator (user access role) 7-3
OperatorPlus (user access role) 7-3
Oracle. See database
organization, of this guide xiv
OSPF 19-8

P

Partially Discovered (VNE investigation state) 19-5, 20-19, 20-22
passwords
  bosenable, bosconfig, bosusermanager 15-4
database 15-1
diagnostics tool 9-7, 15-5
Prime Network Administration 1-4
root 7-24, 15-4
rules (global) 7-14
users 1-28, 7-7, 7-20, 7-21, 7-22, 7-24
Password Settings GUI overview 1-28
permissions
  maps 7-23
  user access roles 7-2
  user defaults 7-19
persistency, VNE
  alarms 26-2
  instrumentation persistency 26-6
log file B-2
overview 26-1
topology persistency 26-7
polling
  adaptive. See adaptive polling
  expedited 22-2, 25-3
high CPU
  adaptive polling 22-15
  thresholds 22-17
  troubleshooting 22-2
overview
polling groups. See polling groups
reduced. See reduced polling
smart polling 22-1, 22-27
smooth polling 22-1, 22-26
polling groups
  applying to VNE 19-40
Configuration 22-24
  creating 22-24
default (group) 22-23
defaults 22-1
deployment example 22-24
GUI overview 1-23
Layer 1 22-24
Layer 2 22-24
overview 22-1, 22-23
slow (group) 22-23
Status 22-24
System 22-24
VNEs and 19-40
Polling Groups (GUI client) 1-23
ports
  BQL 13-3
Cloud VNEs and 23-1
diagnostics tool 9-7
Event Notification Service and 6-3
LDAP and 7-9, 7-11
standby units and 14-3
static links and 23-8
status (Status polling) 22-24
port watchdog 10-5
POS 19-8
PPP 19-8
Prime Central 1-4
disabled features in Prime Network 1-4
user accounts and 1-5
VNEs and 1-5
primeha command (ADG gateway geographical redundancy) 18-15, 18-18, 18-20, 18-21
Prime Network
  AVMs. See AVMs
database. See database
database tables 10-1
deployment 1-1
Event Collector. See Event Collector
gateway. See gateway
installation directory, default 2-1
licensing 5-1
log files B-2
Prime Central and 1-4
restarting (RHCS/ADG gateway high availability) 18-3
setup 1-1
units. See units
upgrades and licensing 5-2
VNEs. See VNEs
Prime Network Administration window
  All Servers branch 1-9, 1-14
content area 1-8
Event Notification branch 1-16
Global Settings branch 1-17
  Authentication Method 1-27
  Automatic AVM Management 1-18
  Event Management Settings 1-19
  License Report 1-21
  Message of the Day 1-22
  Password Settings 1-28
  Polling Groups 1-23
  Protection Groups 1-24
  Report Settings 1-20, 1-25
  User Account Settings 1-29
Prime Network Administration window (continued)

navigation pane 1-7
parts of 1-6
password 1-4
role required to use (GUI client) 1-1, 7-3
Scopes branch 1-29
tables 1-8, 1-36
Topology branch 1-31
Users branch 1-32
Workflow Engine branch 1-33
Prime Network settings (VNE adaptive polling) 19-42
Prime Performance Manager 1-5, 14-4
private key, SSH 19-37
properties, VNEs (detailed) 19-28
protection groups
  adding units to 16-9
  recommendations 16-4
  unit high availability and 16-2
Protection Groups branch (GUI client) 1-24
protocols
  changing communication 24-1, 24-2
  customizing testing 24-7
  determining reachability 24-3
HTTP 19-39, 24-7
ICMP 24-6
SNMP 24-3
Telnet 24-5
XML 19-38, 24-5, A-3
PROVISIONINGEVENT database table 10-2
PTP 1588 19-8
public key, SSH 19-37
purging vs. archiving 10-6, 10-9
PVST 19-8
PWE3 19-8
PW VCCV 19-8

R

raw event filter 14-3
reduced polling
  applying to VNE 19-40
  checking VNE setting 19-40
  customizing 22-4, 22-8
  fail-safe mechanism 22-14
  overview 22-2
  throttling mechanism 22-12
registry
  backing up 8-1
  changing settings C-2
  Golden Source C-1
  location C-1
  overview C-1
  runRegTool command usage C-2
  security 13-4, 13-6
  site.xml file C-2
  subdirectories C-1
related documentation i-xvii
REP 19-8
REP-AG 19-8
reports
  AVM 84 and 4-3
  log file B-3
  purging 10-5, 10-8, 10-9
  sharing 10-8, 10-9
Report Settings GUI 1-20, 1-25
restore
  embedded database 11-13
  Prime Network data 8-4, 11-13
RHCS (Red Hat Cluster Suite). See high availability,
gateway (RHCS/ADG)
roles. See user access roles
root password 7-24, 15-4
runRegTool command C-2

Q

Q-in-Q 19-8
S

safe mode. See AOP

SBC 19-8
schemes, database 10-1
schemes (VNE) 19-5, 19-29
scopes
  activities included in scope 7-3
  alarms and 7-3
  assigning to users 7-19
  controlling user access 7-22
  creating 7-16
  deleting 7-18
  editing 7-18
  GUI overview 1-29
  links and 7-17
  overview 7-3
  security 7-3
  Special (security level) 7-3
  user access roles and 7-5
  viewing 7-18
Scopes branch (GUI client) 1-29
SDH 19-8
security
  communication, to/from devices 13-4
  communication, within Prime Network 13-1
  database 13-3
  default permissions 7-2, 13-6
  gateway and client communication 13-3
  gateway and unit communication 13-2
  registry 13-4
  scopes 7-3, 13-6
  system, overview 13-1
  user access roles 7-2, 13-6
SECURITYEVENT database table 10-2
security level (scope), Special 7-3
service request, submitting xviii

Shutting Down
  AVM status 4-5
  VNE status 4-15
Shutting Down (VNE investigation state) 19-5, 20-19
site.xml C-2
slow (polling group) 22-23
SL-XLAT 19-8
smart polling 22-1, 22-27
smooth polling 22-1, 22-26
SNMP
  changing communication policies 24-1, 24-2
  customizing testing 24-7
  determining protocol reachability 24-3
  traps A-8, A-13
  VNE setup 19-31
SNMPv3 security 13-4
SONET 19-8
Special (scope security level) 7-3
SSH 13-1
  device configuration prerequisites A-8
  encryption algorithms 13-5
  file format
    private key 19-37
    public key 19-37
  login sequence 19-33, 19-38
  managing VNE connection rates 19-45
  prerequisites to adding VNEs A-8
  security 13-4
  VNE settings 19-32
    SSHv1 19-33
    SSHv2 19-34
SSL 13-1
staggering VNEs (controlling connections) 19-45
standby units
  switching
    automatically 16-9
    manually 16-9
  switchover 16-2, 16-6
Starting Up
   AVM status 4-5
   VNE status 4-15
states, VNEs. See VNEs
static links. See links
status
   AVMs 4-5, 4-12
   VNEs 4-14, 4-15
Status polling, VNEs 19-40, 22-24
Stopped (VNE investigation state) 19-5, 20-19
STP 19-8
strict (VNE communication policy) 24-1
SVI 19-8
SynCE 19-8
syslogs 14-3
   configuring notification service for 6-3
dropped 19-42, A-14
   Event Collector and 14-1, 14-3
   Event Notification Service and 6-1
   polling and 22-2
   VNE settings A-13
SYSTEMEVENT database table 10-2
System polling, VNEs 19-40, 22-24

throttling mechanism (reduced polling) 22-12
TICKET database table 10-2
tickets, removing. See database
time zones
events 10-1
gateway 2-1
topology AVM, VNEs (AVM 78) 4-3
Topology branch (GUI client) 1-31
topology discovery, disabling 22-2
Tracking Disabled (VNE communication state) 19-4, 20-6
traps
   configuring notification service for 6-3
dropped 19-42, A-14
   Event Collector and 14-1
   Event Notification Service and 6-1
   polling and 22-2
   VNEs A-8, A-13
troubleshooting VNEs 20-1
bugs, opening 20-24
discovery problems (investigation states) 19-1, 20-14
reachability problems (communication states) 19-1, 20-3

U
unit hot standby. See unit server high availability
units
   adding 3-2
   AVM 99 and 4-3
   AVMs installed on 4-3
   connecting and disconnecting 3-4
deleting 3-5
   firewalls and 9-2, 13-4
   GUI client and 1-11
   high availability. See high availability, unit
   log file B-3
   overview 3-1
   protection groups GUI 1-24
   restarting 3-4
units (continued)
  running command on all 15-5
  security 13-1, 13-2
  viewing properties 3-2
Unreachable (AVM status) 4-5
Unreachable (VNE status) 4-15
Unsupported (VNE investigation state) 19-5, 20-18, 20-21
Up
  AVM status 4-5
  VNE status 4-15
updates, VNEs. See VNEs, updating
upgrades (Prime Network) and licensing 5-2
user access roles
  alarms and 7-2
  assigning default permissions 7-19
  overview 7-1, 7-2, 13-7
  required for Prime Network Administration 7-3
  scopes and 7-5
types 7-3
User Account Settings (GUI client) 1-29
users
  access roles. See user access roles
  authentication. See authentication, users
  controlling map access 7-23
  creating 7-19
default permissions 7-19
deleting 7-24
disabling accounts 7-15, 7-22
emergency (LDAP) 7-2
GUI client settings 7-21, 7-22
GUI overview 1-32
maximum connections 7-21, 7-22
passwords 1-28, 7-7, 7-14, 7-20, 7-21, 7-22, 7-24
Prime Central and 1-5
scopes and 1-29, 7-6
workflows and 12-1
Users branch (GUI client) 1-32

V
VC Switching 19-8
Viewer (user access role) 7-3
VLAN 19-7
VLAN Bridging 19-8
vne_creation_script 15-5
VNE drivers. See Device Packages
VNE persistency
  instrumentation persistency 26-6
topology persistency 26-7
VNEs
  adaptive polling. See adaptive polling
  adding
    auto-add 19-11
cloning 19-14
    CSV file 19-17
    manually 19-21
    overview 19-11
  vne_creation_script 15-5
  auto-add 4-3
  bugs, opening 20-24
Carrier Packet Transport (CPT) devices A-15
Cisco Nexus devices A-7, A-9, A-14
Cloud 23-1
  communication policies 24-1, 24-2
communication states 19-1, 19-3, 20-3
deleting 4-16
device reachability. See device reachability
discovery. See discovery
editing 19-28, 19-43
Event Collector and 14-4
Fault Agent 14-5
HTTP and 19-39
investigation states 19-1, 19-4, 20-14
VNEs (continued)

- IP address 19-29
- maintenance mode 19-44
- moving 4-16
- polling. See polling
- prerequisites to creating 19-12, A-1

Prime Central and properties
- Events 19-42
- General 19-29
- HTTP 19-39
- ICMP 19-39
- Polling 19-40
- SNMP 19-31
- Telnet/SSH settings 19-32
- XML 19-38

Reduced polling. See reduced polling
Restarting. See VNEs, stopping and starting schemes 19-5, 19-29

SSH settings 19-33, 19-34
Staggering (controlling connections) 19-45
Starting and stopping 19-44
Status
- changing 19-44
- overview 4-14

Syslog settings 19-42, A-13, A-14
Traps 19-42, A-8, A-13, A-14
Troubleshooting. See troubleshooting VNEs
type 19-29
Updating 21-1
Viewing properties 19-28
XML and 19-38

See also device reachability

VNEs, updating
- Device Packages
  - applying to VNE 21-4, 21-7
  - checking for new DPs 21-2
  - downloading 21-6
  - installed, identifying 21-3

Installing 21-6
Overview 21-1
Troubleshooting 21-8
Used by VNE, identifying 21-4

Independent VNE drivers 21-1
Uninstalling DPs 21-7

VNE topology log file B-3

VNE Unreachable (VNE communication state) 19-3, 20-5

VPLS 19-8

VPN
- Layer 2 19-8
- Layer 3 19-7

VRF, Layer 3 19-7

VRRP 19-8

VTP 19-8

W

Watchdog protocol 16-1
- Configuring 16-10
- Editing 16-11
- Events 16-11
- Managing for high availability 16-10
- Overview 16-6
- Viewing properties 16-11

Workflow Engine branch (GUI client) 1-33

Workflows
- Aborting 12-6
- AVM 66 and 4-3
- Database scheme 10-2
- Database tables 10-1
- GUI overview 1-33
- History 12-1
- Log file B-3
- Managing workflows 12-4
- Password, changing 15-1
- Purging 10-5, 12-1
- Searching for 12-4, 12-6
- Templates 12-3
workflows (continued)
  templates, deleting  12-3
  users and  12-1
  Workflow Editor  12-1

X

XML  24-5
  determining protocol reachability  24-5
  enabling on device  A-3
  VNE properties  19-38