Cisco Prime Network 3.8.1 Release Notes

This document contains the following sections:

Release Note Revisions

Table 1 describes information that has been added or changed since the initial release of the Prime Network 3.8.1 Release Notes.

Table 1 Added/Changed Information in This Document

Date	Revision	Location
June 5, 2012	Added the following open caveats: • CSCua00824—ClassCastException in AVM log for VNE referencing ifHighSpeed OID. • CSCua19004—Unable to connect with GUI after upgrading from 3.7.1 to 3.8.1.	• AVM/Unit/VNE Bugs, page 21 • Installation/Upgrade Bugs, page 16
	Updates in the procedure for enabling the Network Discovery feature.	Enabling the Network Discovery Feature for 3.8.1, page 7.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table 1 Added/Changed Information in This Document (continued)

Date	Revision	Location
May 23, 2012	Updated the rollback procedure.	Rolling Back from Prime Network 3.8.1, page 5
April 26, 2012	Added information on installing Cisco Prime Network 3.8.1.	Installing Prime Network 3.8.1, page 3
	Added information on supported RHEL version for RHCS/ADG HA solutions.	Supported Operating System for RHCS/ADG Gateway HA Solutions, page 4
	Added disclaimer for network activation content.	E-Line Activation on 7600 WS Line Cards (with Limitations), page 15
	Added the following open caveat: CSCtw82586—Recommended Solaris patch update.	Installation/Upgrade Bugs, page 16
April 23, 2012	Added the following open caveat: CSCtz36312—Incorrect command to enable VNE Staggering mechanism.	Open Bugs in Prime Network 3.8.1, page 15
April 03, 2012	Added the following open caveats: • CSCty88281—Configuring the VPLS E-LAN activation on Cisco 7600 device fails if VFI is not existing. • CSCty88309—Network Activation script failed to create E-LAN VPLS neighbor on Cisco ASR9000 device. • CSCty87987—Network Activation will not work without removing the timestamp on Cisco ASR9000 device.	Technology-Related Bugs, page 18
May 08, 2012	Added information about support for embedded database on VMware.	Support for Embedded Database on VMware, page 4

Introduction

Cisco Prime Network 3.8.1 provides service providers and other network operators with a comprehensive assurance and device management solution for IP next-generation networks (NGNs). It is offered as a standalone application and as a fully integrated component of the Cisco Prime IP NGN suite for customers needing end-to-end network management lifecycle capabilities.

Cisco Prime Network (Prime Network) users can easily discover network elements (NEs), administer them, diagnose problems, and restore changed configurations. These monitoring, validating, troubleshooting, and administration tasks can be accomplished using the Prime Network GUI client applications.

This document provides information on the new and enhanced features introduced in Cisco Prime Network 3.8.1. It also lists the open and resolved bugs in this release of Prime Network.

Note All the information relevant to this release is consolidated in these release notes. The full documentation set will be updated for the next major release of Prime Network.

The following new features and enhancements have been introduced in Prime Network 3.8.1:

- **Network Discovery**—Allows 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. See Network Discovery, page 8 for more information.
- **Find Mode vs. Automatic Data Retrieval in Prime Network Events**—Allows users to set Prime Network Events to operate in Find mode. In this mode, there is no automatic retrieval of events from the database and users can search for the specific events they want to see. See Find Mode vs. Automatic Data Retrieval in Prime Network Events, page 12 for more information.
- **Support for E-Line Service Activation on 7600 WS Line Cards**—Prime Network 3.8.1 now supports E-line point-to-point service activations on 7600 device ES line cards and the following WS line cards: WS-X6708-10GE, WS-X6748-GE-TX, WS-X6704-10GE, WS-X6724-SFP, 7600-ES20-10G3C. See Change and Configuration Management Additional Device Support, page 13 for more information.
- **Change and Configuration Management (CCM) additional device support**—CCM now provides support for the Cisco ASR 5000 series, Cisco ASR 901, and Cisco ASR 903 routers. See Change and Configuration Management Additional Device Support, page 13 for more information.

Installation and Upgrade Notes Specific to Prime Network 3.8.1

This section includes installation and upgrade information specifically relevant to the Cisco Prime Network 3.8.1 release. The information in this section should be read as a supplement to the *Cisco Prime Network 3.8 Installation Guide*.

Installing Prime Network 3.8.1

To perform a standard installation of Prime Network 3.8.1, follow the instructions for installing Prime Network 3.8 that are documented in the *Cisco Prime Network 3.8 Installation Guide*.

To upgrade to 3.8.1, follow the Upgrading from Cisco ANA 3.7.x to Cisco Prime Network 3.8 section in the *Cisco Prime Network 3.8 Installation Guide*. The procedure is the same, with these differences:

- You do not have to delete the $ANAHOME/main/drivers content from all of the units before you perform the upgrade. (This is stated in a Before You Begin note at the beginning of the upgrade procedure, but you can ignore it.)

- When doing an upgrade from 3.8 to 3.8.1, you must install the 3.8.1 version of the ivne-drivers.tar file for Cisco Prime Network to be fully functional.

Web Browser Support

1. Prime Network 3.8.1 web browser based GUI is supported on the following browsers:
   - Mozilla Firefox 7.0
   - Google Chrome 12, 13, and 14
   - Apple Safari 5.1
   - Internet Explorer 8 (on Microsoft Windows 7)
   - Internet Explorer 9 supported in IE 8 Capability Mode
2. The minimum browser dimensions that Prime Network supports to successfully view the network discovery tool, is 900 x 600.

Supported Operating System for RHCS/ADG Gateway HA Solutions

Prime Network 3.8.1 is supported on Red Hat Enterprise for Linux, 5.5, 5.6, 5.7 with the Red Hat Clustering Suite. This applies to both local and geographical redundancy.

Support for Embedded Database on VMware

Oracle can now be installed on VMware. Prime Network 3.8.1 supports embedded database on VMware, with fault management performance of five events per second.

Post-Upgrade—Restarting Crontab Jobs for Unit Behind NAT/FW

Upgrading to Cisco Prime Network 3.8.1 removes crontab jobs from units. To manually restart these jobs for units behind NAT/firewall, do the following:

Step 1 Log in to the unit as the *network user.*

Step 2 Copy the **upgrade_restart_crons.pl** script from the gateway, as follows:

```
remote_copy.cmd "[your_gateway's_ip]:~/Main/scripts/upgrade_restart_crons.pl" Main/scripts
```

Step 3 Execute the above script on the unit. The following output is displayed:

```
./Main/scripts/upgrade_restart_crons.pl
+ Updating the unit's cronjobs
- Writing log to ~/Main/logs/upgrade_crons.log
- Copying the files from the gateway (gateway's_ip)
- Restarting the cronjobs
```

Step 4 Verify the crontab list is not empty by executing the following command:

```
crontab -l
```

Step 5 Verify the unit is starting up by executing the following command :

```
ps  -ef | grep network user
```

Rolling Back from Prime Network 3.8.1

Rollback is available if you encounter problems during the upgrade, or if you need to roll back to an earlier version after the upgrade completes.

Note If you are rolling back a gateway and one or more units are connected to the gateway, roll back the units first, then the gateway. The rollback will remove redundant units from the registry and the GoldenSource.

Complete the following procedure to roll back to Prime Network 3.8 or ANA 3.7.x:

Step 1 Verify that the Prime Network application is not running.

Step 2 Verify that the gateway and units are powered up and connected. That is, you can open an SSH session between the gateway and all units.

Step 3 If your environment contains standby/NAT units, use Prime Network Administration to remove the standby units from the gateway.

Step 4 Restore the backed-up database and start the database services and the listener. The database backup was done during the upgrade process as the database table structure changes during the upgrade. In order for the system to function correctly after a rollback, the old table structure must be recovered through a database backup. To restore an external database, contact your database administrator. Do the following to restore an embedded database:

a. Log into the gateway as *network user*.

b. Change to the directory NETWORKHOME/Main/scripts/embedded_db:

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

c. Execute the restoration script:

```
# emdbctl --restore
```

Note After you restore the database, Prime Network tries to reboot. The reboot does not succeed and an error appears in the gateway log that AVMs with a heap size of 6 GB cannot be configured. You can ignore this message and continue with the next step.

Step 5 If rolling back to 3.8, save the ~/Main/.ana and ~/Main/.version files for all units outside of the Prime Network home directory. If rolling back to 3.7.x, continue to Step 7.

Step 6 Uninstall and install 3.8 or 3.7.x unit (depending on the version you are rolling back to), but do not configue the unit at this point.

Note Make sure the unit's user name and directory is same as the gateway.

Step 7 As the *network user*, go to the directory where the upgrade directory was copied during the upgrade procedure and enter the following command to change to the upgrade directory:

`cd Prime_Network_upgrade` (for 3.8)

`or`

`cd ANA_upgrade` (for 3.7.x)

Note Make sure that the upgrade directory is not a subdirectory of the prime network home directory.

Step 8 As the *network user*, enter the following command on the Prime Network gateway only:

`perl rollback.pl`

Caution Do not deploy the **`rollback.pl`** script in the Prime Network home directory. If you do this, an error message appears that the script should not run from this location.

Step 9 Enter the required information at the prompts. The following table lists the prompts that appears at various stages of the rollback their required settings

Table 1-2 Rollback Prompts and Required Input

Prompt for...	Enter...	Notes
Have you rolled back the database?	Y	Enter **Yes** if you have rolled back the database, as described in Step 4. If you have not rolled back the database, do not continue. Complete the database rollback first, and then start this procedure again.
Have you reinstalled the units?	Y	Enter **Yes** if you have reinstalled any units connected to the gateway. If not, do not continue. Reinstall the units, and then begin the procedure again.
Are you sure you want to roll back the current Prime Network installation?	Y	Enter **Yes**.
Enter the full path to the backup archive file	Example: /export/home/PrimeNetworkBackUp _[10 digits number].tar.gz	Enter the location of the backup archive directory. The **rollback.pl** script does not delete the backup archive.

The script reverts the gateway back to its earlier version.

Step 10 Run the following command on all units:

`network-conf`

Note If a unit fails after executing **network-conf**, do the following:

a. For roll back to 3.8, copy the ~/Main/.ana and ~/Main/.version file from the location specified in Step 5, back to ~/Main.

b. Copy $ANAHOME/Main/registry/ConfigurationFiles/UNIT_IP/avm99.xml file from the gateway to the corresponding unit (UNIT_IP) to $ANAHOME/Main/registry. The UNIT_IP should be of the form 0.0.0.1.

c. Start the unit (**anactl start** (ANA 3.7.x) or **networkctl start** (3.8 onwards)) without running **network-conf** again.

Step 11 If you have rolled back to 3.8, run **networkctl start** command to start the units or run **anactl start** command if you have rolled back to ANA 3.7.x.

Step 12 Use Prime Network Administration(for 3.8) or ANA Manage (for 3.7.x) to reconnect standby units.

Note For units behind NAT, remove the newly created unit from the gateway.

Enabling the Network Discovery Feature for 3.8.1

You must perform the following steps after Cisco Prime Network installation or after an upgrade for the Network Discovery feature to work in Prime Network 3.8.1. For more details on the network discovery tool, see Network Discovery, page 8.

Step 1 Log in to the Prime Network gateway machine OS shell as the Prime Network user.

Step 2 Change the user to be the super user.

```
su root
```

Step 3 Enter the super user password.

```
enter root password: XXXX
```

Step 4 Navigate to the scripts folder located under the home directory of the Prime Network user.

```
cd /export/home/network381/local/scripts
```

Step 5 Change to tcsh shell.

```
tcsh
```

Step 6 Execute the setFpingPermissions script.

```
./setFpingPermissions.tcsh
```

The setFpingPermissions script is executed to ensure successful functioning of the network discovery tool and sets some permissions to the Fping utility. You will get a Fping permissions set successfully message if the utility is successfully executed. If you do not receive this message, please contact your Cisco account representative for assistance.

New Features and Enhancements in Prime Network 3.8.1

The following topics describe the new features and enhancements in Prime Network 3.8.1:

Network Discovery

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.

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 8 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 11 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 disovery 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 3 lists the parameters to be defined before initiating the discovery process.

Table 3 Discovery Profile Settings

Field	Description
Name	A unique name for the discovery profile.
Discovery Technique	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: • 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. • 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. **Note** You can specify multiple techniques in order to locate and discover the largest number of devices.
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.

Table 3 Discovery Profile Settings

Field	Description
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/geograpic 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.

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 4.

Note To see the latest status, please click the Refresh button to refresh the display.

Table 4 Network Discovery Results Table

Field	Description
Name	Name provided by the system for the discovery job, derived from the discovery profile name plus a unique ID.
Status	Status of the executed discovery. The status can be one of the following: • Completed • Running • Stopped • Aborted **Note** Icons next to the Name field provide an at-a-glance view of the discovery job status. See Table 5.
Start Time	Start time of the network discovery job.
End Time	End time of of the network discovery job.
Discovery Profile	Name of the discovery profile in which the discovery settings were defined.
Reachable	The number of discovered devices that are reachable and manageable using the specified credentials.
Filtered	The number of devices that were filtered from the discovery results.
Credential Error	The number of devices that were identified in the network but cannot be managed using the specified credentials.

The status of the network discovery is reflected in the icons displayed next to the job name, as described in Table 5.

Table 5 Discovery Job Status Icon Reference

Status	Icon	Description
Running		The job is running and there are no credential errors.
		The job is running and there are credential errors.
Completed		The job is completed and there are no credential errors.
		The job is completed and there are credential errors.
Stopped		The job is stopped.
Aborted		The job is aborted.

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.

Find Mode vs. Automatic Data Retrieval in Prime Network Events

When Prime Network Events is opened, or when you switch between tabs in the application, the database is automatically queried to retrieve and display events. Depending on the volume of events, this can take some time. If you want to find specific events and you are not interested in browsing all the available

events, you can set Prime Network Events to operate in Find mode. In this mode, no events will be retrieved from the database when you open the application or switch between tabs, and you can click the Find button in the toolbar to search for the events you need.

To enable and use Find mode:

Step 1 In Prime Network Events, select **Tools > Options**.

Step 2 Check the Find mode check box and click **OK**.

The window will be cleared of events. The following text will appear under the events table: “Find mode (No automatic data retrieval).”

Step 3 Click the Find button in the toolbar and define a query to display specific events.

Change and Configuration Management Additional Device Support

Change and Configuration Management provides support for the Cisco ASR 5000 series, Cisco ASR 901, and Cisco ASR 903 routers in Prime Network 3.8.1. The following topics describe the support information in detail:

- Cisco ASR 5000 Series Device Support, page 13
- Cisco ASR 903 Device Support, page 14

In addition, please note the following:

- Change and Configuration Management does not support special characters for any of the editable fields in the GUI, including filters. In the Configuration and Image Management Settings pages, Change and Configuration Management does not support the following special characters:
  - For Password fields—>, <, ', and "
  - For all other fields—‘, ~, @, #, $, %, ^, &, *, (,), +, =, |, {, }, [,], ', ?, >, <, and "
- For ACE cards on Cisco 7600 devices, Configuration Management supports only TFTP protocol for image baseline, backup, and restore operations.

Cisco ASR 5000 Series Device Support

For Cisco ASR 5000 series devices, you can follow the same workflow as that of the Cisco IOS devices. The following enhancements or changes have been made in Change and Configuration Management for Cisco ASR 5000 series devices in Prime Network 3.8.1:

- The two types of configuration files for Cisco ASR 5000 series devices are: the running (current operating) configuration and the boot configuration. For a boot configuration file, the version of the archived configuration is always displayed as ‘1’ in the Archived Configurations page.
- The following processes are not applicable for the boot configuration files of Cisco ASR 5000 series devices:
  - Restoring a configuration from the archive to the device
  - Synchronization of out-of-sync devices
- The Device Properties window displays a priority list for the Cisco ASR 5000 series devices. The priority list displays various combinations of a configuration file and an image file in priority order for the device. This information is retrieved from the device configuration.

- Whenever a boot configuration file is backed up to the archive, Prime Network always overwrites the existing boot configuration in the archive.
- Prime Network allows restoring of running configuration only in 'merge' mode, by which if the running configuration version you selected is different from the existing running configuration on the device, then the existing running configuration will be merged with the configuration present in the version you selected from the archive.
- You can view the latest changes to the device configuration using the Configuration Change Logs page. However, Prime Network does not display the following information for Cisco ASR 5000 series devices:
  - Changed—Date and time when a change was made to the device.
  - User—Name of the user who made the change.
- In the Image Repository page, Prime Network displays only the Family and Size fields for Cisco ASR 5000 series devices. All other fields are displayed as UNKNOWN or N/A.
- For Cisco ASR 5000 series devices, you can activate a boot configuration file on the device in addition to an image. However, if a device is activated with a new configuration, which does not have the correct user credentials, a timeout error occurs during activation.
- In the activation workflow (by Images or Devices) and in the distribution and activation workflow (by Images or Devices), after selecting the device and required image(s), you must enter the boot configuration file in the **Enter Boot Config** page. The boot configuration value should always be passed as **flash:/asr.cfg**.
- For Cisco ASR 5000 series devices, Change and Configuration Management supports FTP mode for all configuration and image transfers. FTP username and password configuration in the device should be same as the device management username and password.
- The following features or functions are NOT supported for Cisco ASR 5000 series devices:
  - Clear Flash—Allows clearing the disk space on the storage location for distributing the image or package if there is insufficient memory.
  - Warm Upgrade—Provides the capability for a Cisco IOS image to read and decompress another Cisco IOS image and then transfer control to this new image.
  - Importing images from Cisco.com—Allows you to download images from Cisco.com and add them to the Prime Network image repository.

Cisco ASR 903 Device Support

The following enhancements or changes have been made in Change and Configuration Management for the Cisco ASR 903 device in Prime Network 3.8.1:

- Prime Network allows restoring of running configuration only in 'merge' mode, by which if the running configuration version you selected is different from the existing running configuration on the device, then the existing running configuration will be merged with the configuration present in the version you selected from the archive.
- In the Image Repository page, Prime Network displays only the Family and Size fields for a Cisco ASR 903 device. All other fields are displayed as UNKNOWN or N/A.
- The Warm Upgrade feature, which provides the capability for a Cisco IOS image to read and decompress another Cisco IOS image and then transfer control to this new image, is not supported for a Cisco ASR 903 device.

E-Line Activation on 7600 WS Line Cards (with Limitations)

Although the E-line point-to-point activations provided with Prime Network 3.8.1 are intended as reference configuration examples only, and not as production-ready activations, you might choose to use them in your network, at your own risk. If you do so, please be aware that these activations can be used on 7600 device ES line cards and the following WS line cards: WS-X6708-10GE, WS-X6748-GE-TX, WS-X6704-10GE,WS-X6724-SFP. Sub-interface configuration for the WS line cards uses the EFP ID with the following limitations:

- The Outer VLAN ID will be the dot1q encapsulation configured on the sub interface.
- Inner VLAN ID is not supported.
- VLAN preservation value must be "None" as VLAN manipulation is not supported on sub-interfaces, and VLAN mapping will not be supported.
- VLAN hub and multiple EFPs are not supported on WS cards (only on ES cards).
- Only ES cards are executed as part of E-LAN VPLS HUB and Multipoint EFPs for the 7600 device.

Note All of the activations (templates, scripts, and workflows) provided with Cisco Prime Network Activation are reference configuration examples to aid in customer implementation activities and to demonstrate the capability of Prime Network Activation. They are not intended to be production-ready activations of any Carrier Ethernet, IP RAN, or MPLS VPN configurations. The activations are expected to require customer-specific implementation extensions. Implementation extensions and modifications to the software product are not supported via Cisco Support Agreements. If you require assistance in extending these activations, please contact Cisco Advanced Services.

New Device Support Information

Prime Network 3.8.1 incorporates all the device support additions that were provided in Prime Network 3.8.x Device Packages (DPs) 1 and 2. To get the latest VNE support, please download and install the latest Prime Network 3.8.x DP(s) from the Prime Network download site on Cisco.com.

For detailed information about new device support in Prime Network 3.8.1, please see Addendum: Additional VNE Driver Support for Cisco Prime Network 3.8.

In addition, please note the following:

- Prime Network Change and Configuration supports the following network elements in this release:
  - Cisco ASR 901 network elements.
  - Cisco ASR 903 network elements.
  - Cisco ASR 5000 network elements.

Open Bugs in Prime Network 3.8.1

The following sections identify bugs that are open in Prime Network 3.8.1, according to the following criteria:

- All catastrophic and severe bugs (if any).
- Moderate, minor and enhancement bugs that are considered likely to affect the customer's experience with Prime Network.

- Bugs that were fixed in previous releases of Prime Network but are still open in the current release because they were identified too late in the Prime Network 3.8.1 development cycle.

The open bugs have been grouped in the following categories:

Installation/Upgrade Bugs

Table 6 Installation/Upgrade Bugs

Identifier	Title
CSCua19004	Unable to connect with GUI after upgrading from 3.7.1 to 3.8.1
CSCtw82586	Recommended Solaris patch update
CSCtq83852	User ana_xmp is removed and installation fails after second network-conf
CSCtr11676	After upgrade, AVM 11 starts with errors
CSCtt41552	Unit is not redefined after upgrade to Prime Network 3.8
CSCtx45445	RHCS: Wrong version validation of rpm
CSCtx54365	After upgrading, running Prime Network scripts failed due to Class not found
CSCty36682	Unit becomes unreachable after installation

Device-Related Bugs

Table 7 Device-Related Bugs

Identifier	Title
CSCty28617	Warning message about incompatible drivers when installing Cisco-Others
CSCto31096	High CPU utilization on ASR 9000 device
CSCtr95939	CSC PathTrace fails
CSCtr98822	ASR5K-InterfaceTable-Input access list,Output access list+desc are blank
CSCts17077	Duplicate ports displayed on module
CSCts48120	MPLS LDP session up trap is not correlated to Link up ticket

Table 7 Device-Related Bugs

Identifier	Title
CSCts55761	VLAN IP interface down not correlated to card down
CSCtu70278	Poll now does not update Clock, PTP on reduced polling VNE
CSCtu95760	Syslog "L2-SONET_LOCAL-4-ALARM: SONET0/1/2/0: LAIS" not supported
CSCtw51495	Exception upon executing preview for "AddHostName Script" on ASR901
CSCtw61690	LSP end points role oper state of neighbor device not changed to 'DOWN'
CSCtw64033	MPLS-TP Tunnel Endpoints Oper status of neighbor device not showing 'Up'
CSCtw79231	EFP updates are not reflected immediately on ASR903 using Poll Now
CSCtw95044	Bridges on Cisco ASR5000 device are not modeled
CSCtx19245	Some activation scripts are not working for Nexus 7000 device
CSCtx02470	Some activation scripts are not working for Nexus 5010 device
CSCtx29511	Configuration changes are not updated on XR VNE with reduced polling
CSCtx48077	VDC level Interface Scripts are failing in Nexus 7K
CSCtx67427	Configuration change not updated for channelized controllers
CSCtx86760	Wrong pluggable transceiver out tickets on GSR 12k IOX
CSCtx87344	7600: Channelization is not modeled on CHOC12 or 48 card
CSCtx90642	MWR2900: VNE fails associate transceiver cefc FRU trap wt port connector
CSCtx93011	EFPs are not modeled correctly
CSCtx94475	Not all of the configured timeslots on ds0 are displayed
CSCty10686	Container status is Unknown on Fan & PWR modules
CSCty17058	Reduced polling VNE - "no switchport" is not supported
CSCty18359	ASR 5K Image distribution fails when password has special characters
CSCty19685	Shutting down a VRRP interface moves the CRS VNE to unreachable state
CSCty16496	7600: STS3 or STS12 paths not modeled on OC12 or OC48 interfaces
CSCtx67165	Some entries are missing in IPInterface table for Ethernet port
CSCtw96596	Cold Start Trap appears twice in the ENS selection window
CSCtx76206	Bridges are not modeled in ASR903
CSCtg54230	ATM IMA cards do not populate Loopback, Framing, or Scrambling values
CSCth01054	Cisco 3750g fiber optic ports are modeled as RJ45 ports
CSCtj19233	Cisco RSP 720 removal redundancy state ticket is issued only after reinsertion.
CSCtj92252	VNE restarts due to software version change
CSCtr47998	After reloading a Cisco 7600 device, all related IP interface down events are not cleared
CSCtl12886	Cisco ASR 9000 series power supply redundancy state and configured value are None
CSCts79008	Memory usage information is missing in Nexus5K
CSCtq36525	Wrong PID shown for transceiver/SFP modules for Nexus 7000 device

Table 7 Device-Related Bugs

Identifier	Title
CSCty88281	Configuring the VPLS E-LAN activation on Cisco 7600 device fails if VFI is not existing.
CSCty88309	Network Activation script failed to create E-LAN VPLS neighbor on Cisco ASR9000 device.
CSCty87987	Network Activation will not work without removing the timestamp on Cisco ASR9000 device.

Network Discovery Bugs

Table 8 Network Discovery Bugs

Identifier	Title
CSCty32744	User cannot add snmpv2 row to any job after editing credentials of 1 job
CSCtw96705	Top navigation tool bar disappears
CSCty35489	Unable to create telnet credential without user name

Technology-Related Bugs

Table 9 Technology-Related Bugs

Identifier	Title
CSCts07862	DS0 bundle and BGP vrf tickets not correlated to Sonet interface down
CSCtu12098	Missing VPN links after moving VNE
CSCtu14594	Unit servers at 100% cpu due to XBgpRouterIDAdvertiseMsg message flood
CSCts33148	Fake links between ATM ports although flag 'topology/atm/enabled' false
CSCtt44445	Ethernet counters test disconnects links
CSCtx58626	STP model creates fake physical link between two routers
CSCtn63353	BFD and BGP events are not correlated to Bundle Interface Up/Down tickets
CSCty48255	Subinterfaces under lag and ports sometimes deleted
CSCty48323	BGP link is not discovered
CSCtu15976	Pathtrace that should pass from a VLAN interface to a bridge stops at the VLAN interface
CSCtu15772	Some VPNs are not deleted after deleting relevant VNEs
CSCtu08449	PW and L2 tunnel down traps are not correlated to an EFP down ticket
CSCtt98442	Some edge EFPs are associated to 2 VLANs, one of which is invalid
CSCtt39828	LAG link is not rediscovered after making changes to VNEs
CSCts59855	Ethernet flow points inside a network VLAN are incorrectly calculated as VLAN edges even though they are connected to each other

Table 9 Technology-Related Bugs

Identifier	Title
CSCts45734	In VLAN view, a path trace that ends on a LAG port does not run
CSCts39840	BGP Neighbor Loss syslog is not correlated to Device Unreachable ticket
CSCts15541	Tickets generated for link down and LAG link down alarms on an unreachable device do not correlate
CSCtr83226	Terminating Ethernet flow points under a switching entity that are not connected to another Ethernet flow point in the same NetworkVlan are not recognized as edges
CSCtr81979	OSPF neighbor down event may not correlate to link down or interface status down event
CSCtr77298	Duplicate switching entities are created after deleting and then recreating a VLAN
CSCto13384	AVM 11 stops after continuous Find EVC by Name operations
CSCtn76375	Trunk service link is disconnected after configuring a static VLAN mapping that includes an inner VLAN tag
CSCto75365	BFD links are not removed from the GUI after clearing a BFD connectivity down ticket
CSCts63063	ISIS neighbor data is not created for both IPv4 and IPv6 address families
CSCts40361	Duplicate MPLS-TP network service objects are not automatically removed
CSCto82042	After a P2MP tunnel's status changes from Up to Down, the change is not reflected in Prime Network
CSCts82544	Some OSPF interfaces and neighbors are not modeled for CRS device
CSCts63874	Incorrect BDF links might be discovered for a BDF configuration that has 2 of the same source IP addresses with different destinations
CSCtk65010	Wrong serial connection through CDP in MLPPP technology
CSCts01836	Modification of destination and source port not reflected in Prime Network
CSCtr37523	Links table may display links which have no context but are not marked as external
CSCtj30236	LAG link is not rediscovered after clearing and removing the ticket
CSCtj03925	Physical and Ethernet links disappear after moving and restarting AVM
CSCth30478	Error messages sometimes appear when trying to connect devices that were once connected to the cloud and later removed back to the cloud
CSCtt44288	BGP does not model in Prime Network if the BGP AS number contains a dot
CSCtr69267	Extra EVCs are created for network VLANs whose bridge domain (that contains a terminating Ethernet flow point) is not recognized

Soft Properties Bugs

Table 10 Soft Properties Bugs

Identifier	Title
CSCtx59562	Export/Import of SNMP table SoftProperties doesn't work
CSCts15613	LSE and MPLS soft properties added to a VNE are not visible in Inventory window

Change and Configuration Management (CCM) Bugs

Table 11 CCM Bugs

Identifier	Title
CSCtx79524	CCM operations will fail on IPv4/IPv6 dual stack setup
CSCtr42741	In Admin mode, Prime Network Change and Configuration Management may copy the running configuration instead of the admin configuration
CSCtq61849	Activating Image Command Builder script fails
CSCto02471	Gateway CPU consumption reaches 100% during Config backup of 10,000 VNEs

Fault Management Bugs

Table 12 Fault Management Bugs

Identifier	Title
CSCtx87994	ENS: Incorrect alarms mapped to alarm-type 651
CSCty24297	Detailed Traps report on Event Vision doesn't show the real device ip
CSCtq94497	Multiple “Active IP interfaces found” events returned after shutting down an interface
CSCtl08357	Event handling issues occur 25 minutes after system cold restart
CSCth36256	Cisco Prime Network generates two separate link down events when a port is disconnected and connected a few times
CSCtg96406	Tickets that contain alarm severities of both Cleared and Information have a severity of Cleared instead of Information
CSCsz61942	If you right-click a link in the VPN map view and choose Filter Ticket, no results are displayed
CSCtl47169	Syslog ENVMON-OVERTEMP-2 is not processed by Prime Network
CSCtx28435	Internal process-to-process messages are dropped by Prime Network

AVM/Unit/VNE Bugs

Table 13 AVM/VNE Bugs

Identifier	Title
CSCua00824	ClassCastException in AVM log for VNE referencing ifHighSpeed OID
CSCtz36312	Incorrect command to enable VNE Staggering mechanism
CSCtx52584	AVM with VNE is restarted by AVM99 due to an Out Of Memory
CSCty42565	NAT unit seen as regular if other device answers with same private ip
CSCty42129	Fail to copy VNE persistency files from an IPv4 unit to an IPv6 gateway while moving AVMs/VNEs
CSCtl23101	Moving AVMs operation fails; not all AVMs are moved between units
CSCti93564	Cannot start new AVM 100 on unit when unit with old AVM 100 is down
CSCth22846	Proxy for AVM 25 does not work in high availability (HA) scenarios

VCB Bugs

Table 14 VCB Bugs

Identifier	Title
CSCty90696	Cross launch of VCB from Manage in Suite mode does not work

Bugs Resolved in Earlier Releases but Still Open in Prime Network 3.8.1

The bugs listed in Table 15 were identified too late in the Prime Network 3.8.1 development cycle to be fixed for this release. The fixes for these bugs have been provided to customers running older versions of the product as needed and are scheduled for inclusion in the next release.

T

Table 15 Bugs Resolved in Earlier Releases but Still Open in Prime Network 3.8.1

Identifier	Title
CSCtr30287	Port down ticket is not cleared after the port is up
CSCtr35459	Cannot create a command with Command Builder on selection of a row in Sub Interface table (Physical interface inventory)
CSCtq04992	Free memory on the unit decreases over time.
CSCto42504	In OSPF Neighbor for cases like Bundle-Ether Interface name - OSPF Neighbor down alarms do not correlate to Link down on IOX
CSCts07862	DS0 bundle and BGP vrf tickets not correlated to Sonet interface down
CSCts96142	AVM 11 does not process any links for 15 min
CSCtw62838	PP version is missing in Prime Network GUI (Help -> About)

Table 15 Bugs Resolved in Earlier Releases but Still Open in Prime Network 3.8.1

Identifier	Title
CSCtr94015	Need to support a new Product type as "Packet Microwave" for the DragonWave devices
CSCtu18795	Soft property is not shown as a hyperlink

Resolved Bugs

Table 16 identifies bugs that were listed as open bugs in the Prime Network 3.8 release notes and have since been resolved.

Table 16 Resolved Bugs in Cisco Prime Network 3.8.1

Identifier	Title
CSCtl87991	cefc FRU Inserted alarm is not shown in Prime Network Events
CSCtr95905	In gateway server high availability setups, the standby database might stop applying redo and thus not synchronize with the primary database
CSCtt01448	Adding or editing a user-defined VNE by software version without selecting a scheme results in a null-pointer exception
CSCtu41821	VNE enters and stays in Currently Unsynhronized state
CSCtr41020 (duplicate of CSCtt99335)	Command Builder not working for CPT device
CSCtt46945	Interface table not modeled for bridges on Nexus 7000 device
CSCtt43304	Inside and Outside VRF details are not modeled for a NAT 44 instance
CSCtt41323	Importing images to the repository fails for C3750, C7200, C3560, and ME340X series devices
CSCts10451	"Ticket is in use" error occurs after running Remove command on a ticket
CSCtk10574	No IS-IS Neighbor tab for Cisco 7600 devices
CSCtl71330	Independent VNE installer: checks if the driver was already updated
CSCth96692	Cisco ANA 3.7.1 Upgrade: After upgrade, deleting old ANA user results in exception
CSCtt96125	Catalyst 4503 device is not modeled in GUI
CSCth58175	Cisco ASR 9000 devices: OSPF processes do not show serial interfaces in GUI
CSCtj32671	Port 162 appears to be occupied when IP address contains “162”
CSCtt10154	VNEs reach Operational state before physical inventory is populated
CSCtl12761	Fix upgrade.pl warning for uninitialized value
CSCtk95452	Migration: **anactl start** halts after upgrade step fails
CSCtk67684	Pseudowire tunnel container is removed when all tunnels are removed
CSCtk57982	Soft Property command in debug takes too long
CSCtl07781	Yes or no questions during the embedded database installation accept incorrect input
CSCtl03963	Embedded database: Path for destination cannot contain underscore (_) or dash (-)
CSCtk95873	Discovery protocol disappears from NetworkVision physical inventory after a change
CSCtj97320	OSPFv3 Routing Neighbor Down syslog on Cisco IOS XR does not correlate to OSPF interface
CSCtl22749	VNE flapping due to time synchronization issue

Table 16 Resolved Bugs in Cisco Prime Network 3.8.1 (continued)

Identifier	Title
CSCtl76285	In a local installation, embedded database installation files are not validated
CSCtn20251	**ana-conf** asks twice for remote Oracle machine information
CSCtn10145	**emdbctl -restore** script does not accept environmental variables as input
CSCtn05357	**emdbctl -restore** command fails
CSCti05580	BFD with registered protocols of OSPF and BGP link topology not discovered
CSCtn29290	Opening ticket properties with a large number of correlated events times out
CSCtb54145	Redundant Martini tunnel status is not updated
CSCtq26697	Missing VPN links on MPLS setup with IPv6 configuration
CSCtk68092	Layer 2 tunnel down alarm is not generated if a neighbor or cross-connect is removed
CSCte63920	Creating a cross-connect in an ATM cloud takes a long time
CSCtr06712	VNE was detected as being unsupported and continued to run even though the agent was not already loaded
CSCtg57041	Using Filter in EventVision for large table of Syslog
CSCtq06756	Duplicate BGP Link Down Due to Oper generated by Cisco ANA
CSCtn49323	High Availability: Problem with multicast address
CSCtk64981	The TFS **update** command does not have a validateRequest method
CSCtj77809	BGP Neighbor Down VRF syslog not correlated to BGP Link Down VRF due to Admin ticket
CSCtn70728	SCP backup failure caused by authorization
CSCtl08804	Incorrect behavior for backup directory when running restore
CSCtq04481	High Availability: NTP servers are not synchronized
CSCto16849	Duplicate Link Down on Unreachable tickets in card down scenario
CSCts10091	SIP400 card down ticket on Cisco 7606S device creates separate card out ticket for its subslot SPAs
CSCtl74253	NetworkVision issues an Insufficient Memory error and closes in large scale setup
CSCts78869	Unable to establish SSH connection after running Stop/Resume replication command
CSCts90609	Setup replication script does not stop Prime Network on the gateway server high availability node
CSCtr59244	Launching the gateway will take around 15 minutes when the gateway is started for the first time after installing Prime Network
CSCtq34912	Cannot open the Shell from the default GUI menu
CSCtq33136	Migration: Restore database fails to start gateway
CSCtl56075	FRR Unprotected trap not correlated to Link Down alarm
CSCto67825	VSI presentation in inventory is not updated with pseudowires
CSCts60990	Moving a VNE to another AVM and then back causes some BGP and VPN links to disappear

Table 16 Resolved Bugs in Cisco Prime Network 3.8.1 (continued)

Identifier	Title
CSCtj61896	Running images are not recognized
CSCti25818	BGP State Change trap is not processed if source peer is from the VPN IPv6 table
CSCtn04519	Power supply modules for Cisco CRS 8-slot devices running Cisco IOS XR software appear as individual slots on the chassis
CSCto10818	MAC address not modified in GUI for Ether bundle on Cisco IOS XR 12000
CSCto67407	Add TE-Tunnel Rerouted or Reoptimized syslog and trap flow
CSCtl92858	Correct the mapping of RTM group number for non-Cisco devices
CSCtn57568	Monitoring and archiving dangling events and auto-clearing old tickets
CSCtl00393	Some 10GigabitEthernet port location information is marked as Unknown
CSCtu23875	Image distribution fails while data transfers from external location to device
CSCtu11656	SNMP Link Down/Up ticket associated with wrong interface
CSCtu00707	Port Security properties for Cisco ME 3400 device are not populated
CSCtt46925	VC table and cross connect information not modeled for ATM port on Cisco 7600 device
CSCtt46916	OSPFv3 neighbors are not modeled for Nexus 7000 device
CSCts75628	CDP neighbors detail command does not list all IPv4 and IPv6 entries on IOS XR platform

Closed Bugs

Table 17 identifies bugs that were listed as open bugs in the Prime Network 3.8 release notes and have since been closed.

Table 17 Closed Bugs in Cisco Prime Network 3.8.1

Identifier	Title
CSCtr59590	ELAN VPLS HUB script fails to run because of missing command
CSCtq87812	Redundant link down ticket issued
CSCtn77815	NSA: Attach Bandwidth Profile script fails-Cisco ME3800
CSCti79028	CCO credentials are passed in clear text through internet
CSCth17529	Business Element Not Found error when trying to add an EVC to a map
CSCts74887	MPLS LDP does not support IPv6-only interfaces on IOS XR platform
CSCts23284	VLAN interfaces on Catalyst WS-C4948 devices are not modeled properly
CSCtr56846	Investigation State for a device does not match its Communication State
CSCtq61427	Some of the registrations fail in the LCM report and return the "Error Unrecoverable" message

Related Documentation

The following documentation is available for Cisco Prime Network 3.8.1:

- *Open Source Used in Cisco Prime Network, 3.8.1*
- *Cisco Prime Network 3.8.1 Release Notes* (this document)

The content of the following Prime Network 3.8 guides is still applicable to Prime Network 3.8.1:

- *Cisco Prime Network 3.8 Administrator Guide*
- *Cisco Prime Network 3.8 Customization User Guide*
- *Cisco Prime Network 3.8 Device Package Third-Party VNE Reference Guide*
- *Cisco Prime Network 3.8 Documentation Guide*
- *Cisco Prime Network 3.8 Installation Guide*
- *Cisco Prime Network 3.8 Quick Start Guide*
- *Cisco Prime Network 3.8 Reference Guide*
- *Cisco Prime Network 3.8 User Guide*
- *Cisco Prime Network 3.8 Change and Configuration Management User and Administration Guide*

Cisco Prime Network 3.8 Integration Developer Guide is available on the Prime Network Technology Center. This guide describes how to use Prime Network integration interfaces.

The 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 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:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.