



Cisco Prime Infrastructure 1.3

Deployment Guide

August 2013

Contents

Scope	5
Introduction	5
Installation	6
Prerequisites	6
Server Requirements	7
Client Requirements	7
Server Sizing Matrix	7
Installing the Cisco Prime Infrastructure Virtual Appliance	8
Installing Cisco Prime Infrastructure on a Physical Appliance	8
Starting/Stopping Cisco Prime Infrastructure Services	8
Logging into Cisco Prime Infrastructure for the First Time	8
Verifying IOPS for Prime Infrastructure Virtual Machine	9
Licensing	9
Configuring Backup	9
Advanced System Settings	10
Data Retention	10
Accessing Cisco Prime Infrastructure Through the CLI	10
How to Enable the CLI Root User in the Cisco Prime Infrastructure Server	10
High Availability	10
HA Setup	11
Licensing	11
Cisco Prime Infrastructure High Availability Setup	11
HA Modes	11
Failover	11
Failback	11
Manual/Automatic Options	12
Automatic Failover	12
Primary Failure Example - Manual Failover	12
Upgrade and Data Migration from Previous Applications	13
Upgrading to Prime Infrastructure 1.3	13
Migrating from WCS 7.x to NCS 1.1.1.24	13
Migrating from NCS 1.1.1.24 to Prime Infrastructure 1.3	13
From LMS	13
LMS 2.x	13
LMS 3.x	14
LMS 4.x	14
Exporting from LMS 4.2.2	14
Importing into Cisco Prime Infrastructure 1.3	14
Application Setup	14
Lifecycle Management	15
Design	15
Deploy	15
Operate	15
Report	15
Administer	15
Creating Groupings and Sites	15
Create Sites	15
Import/Edit Maps from WCS/NCS to Cisco Prime Infrastructure	16
Associate Endpoints to Sites	16
Create Port Groups	17
Users and User Group Management	17
Adding New Users	17
Creating User Groups	18
Image Management Settings	19
Configuration Archive Settings	20

Configuring NTP and DNS for NAMs	20
Connection to Cisco.com	21
Proxy Settings	21
Cisco.com Settings	21
Planning/Preparing the Network.....	21
Wireless Planning Tool	21
Ports Used	22
Protocol Check	23
Configuring SNMP	23
Enabling SNMP on Wireless Controllers	23
Enabling SNMP on Routers/Switches	24
Enabling Telnet/SSH on Routers/Switches	24
Enabling Telnet/SSH on Wireless Controllers	24
HTTP/HTTPS	24
Preparing the Wireless Network	24
Import Maps from WCS	24
Discovering Your Network.....	25
Discover Devices	25
Create A New Discovery Profile	25
Configuring Cisco Discovery Protocol/LLDP	26
Filtering	27
Credentials	27
Discover the Network	27
Scheduling Ongoing Discovery	28
Validate Discovery	28
Device Work Center	28
Fixing Credential Errors	28
Importing Devices Manually	29
Automating Branch Device Deployment	29
Deploying Wireless and Advanced Instrumentation.....	29
Deploy a WLAN Using a Configuration Template	29
NetFlow	30
Using Configuration Templates to Enable NetFlow	31
Check Whether NetFlow Data Are Coming or Not	32
Medianet	33
Enabling Medianet	33
Check Whether Medianet Is Enabled	33
Monitoring/Troubleshooting.....	34
Basic Monitoring	34
Basic Device Health	34
Interface Statistics	35
Design Custom Monitoring Templates	35
Deploy Custom Monitoring Templates	36
Data Collection from NAM	36
Turning on Advanced Monitoring	37
NetFlow	38
WAN Optimization - aka Cisco Wide Area Application Services	39
Monitor/Troubleshoot a Wireless Network	39
RRM/Clean air	39
Build RF Profile	40
Apply RF Profiles to AP Groups	42
Monitor/Troubleshoot Clients and Users	45
Client Visibility	45
Wireless Clients	45
Test Analysis Tool (CCXv5 Clients)	47
Wired Clients	47
Alarms and Events	48
Quick Filter	49

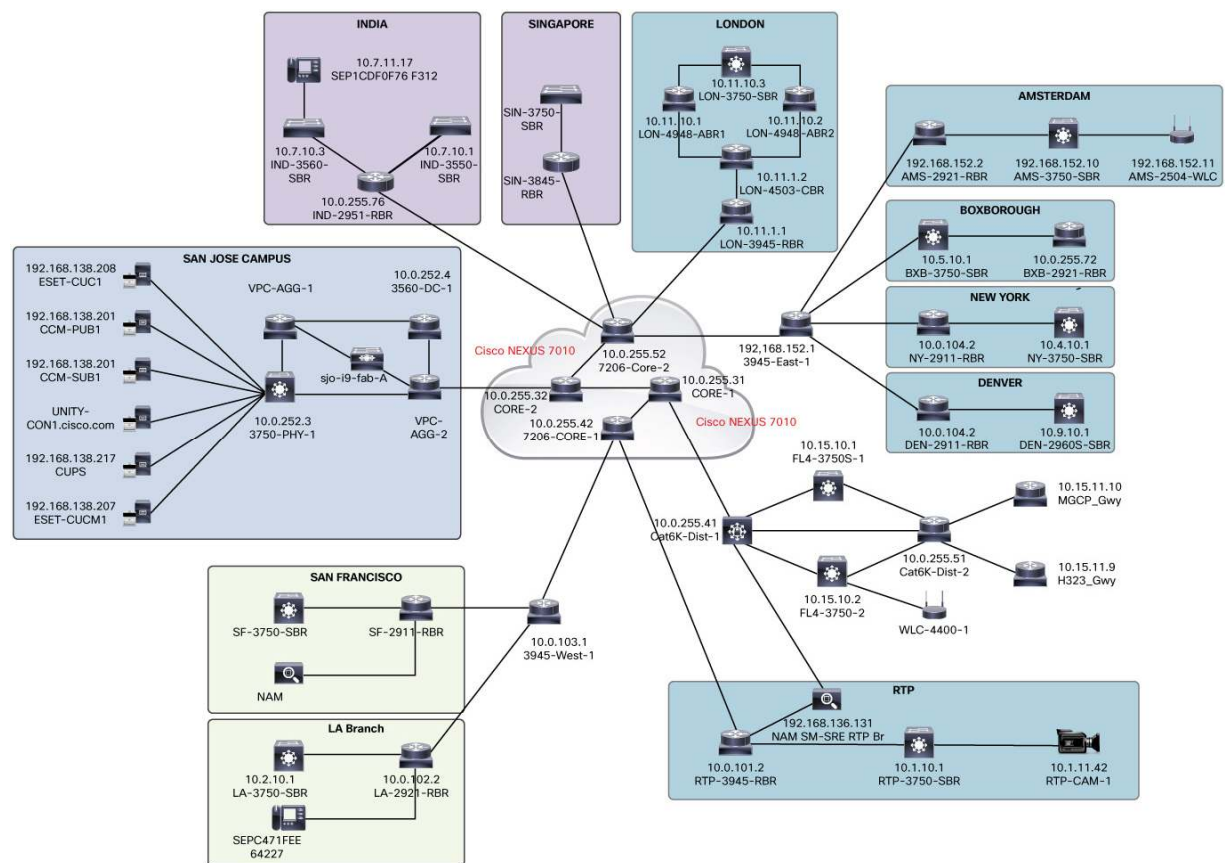
Advanced Filter	49
Trigger Packet Capture from Cisco Prime Infrastructure	49
Manual Packet Capture from Cisco Prime Infrastructure	49
Automating Packet Capture Using Cisco Prime Infrastructure	50
Decoding Packet Capture Using Cisco Prime Infrastructure	50
Miscellaneous Multi-NAM Capabilities Within Cisco Prime Infrastructure	51
Remediate Issues	51
Remediate Wireless Issues	51
Remediate Wired Issues	52
Optimize	53
Use Cisco Prime Infrastructure to Optimize the Operation of Your Converged Network	53
Dashboard Customization	53
Customizing the Dashlet Content	55
Advance Configuration Topics	56
Identity Services Engine Integration	56
Automated Deployment	56
Creating the Bootstrap and Device Configuration Template	58
Create Automated Deployment Templates	60
Deploying the Automated Deployment Template	60
Deploying Devices Using Automated Deployment Templates	62
References	62
Prime Infrastructure 1.3 Links	62
Cisco Product Pages	63
Ordering and Licensing	63
Related Deployment Guides	63

Scope

This document is meant to be used for successfully deploying Cisco Prime™ Infrastructure. The assumption is that the basic wired and wireless network is already deployed. Cisco Prime Infrastructure will be used to manage the existing network and modify or enhance it. This guide has been updated for Prime Infrastructure 1.3.

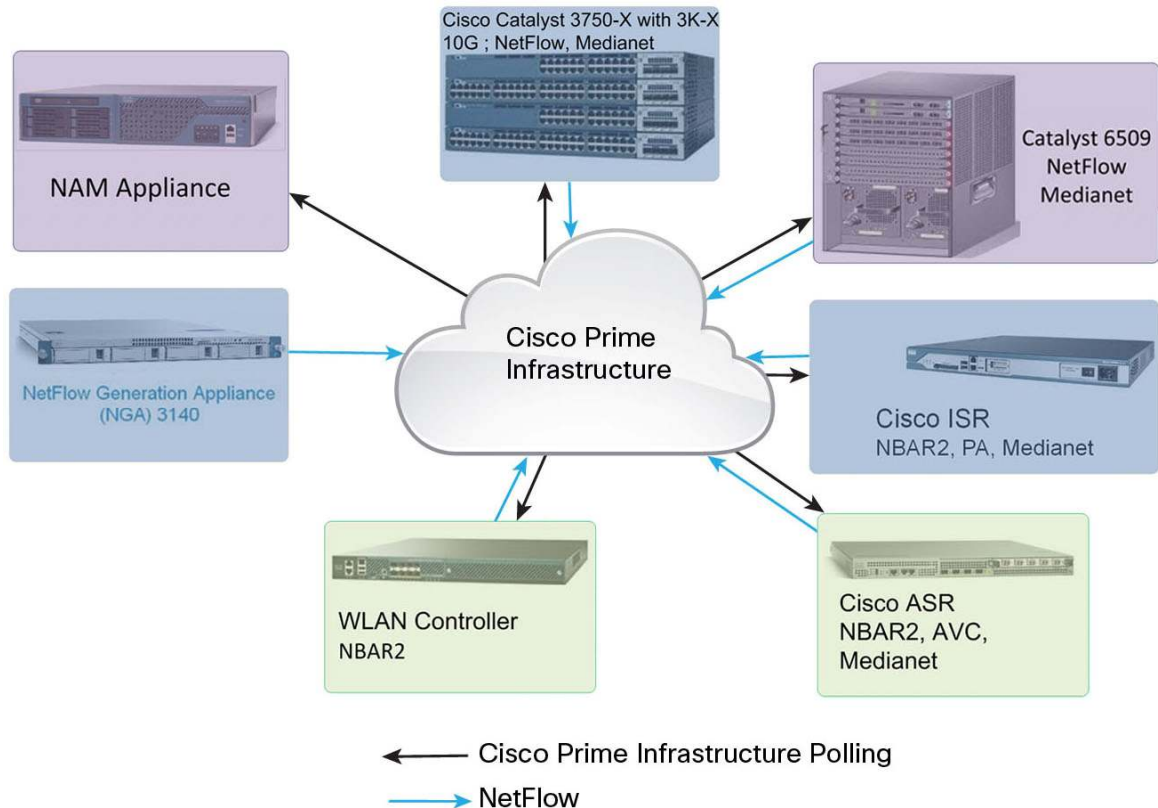
Introduction

Combining the wireless functionality of Cisco Prime Network Control System (NCS) with Cisco Prime LAN Management Solution (LMS), Cisco Prime Infrastructure simplifies and automates many of the day-to-day tasks associated with maintaining and managing the end-to-end network infrastructure from a single pane of glass. The new converged solution delivers many of the existing wireless capabilities for RF management, user access, reporting, and troubleshooting along with wired lifecycle functions such as discovery, inventory, configuration and image management, compliance reporting, integrated best practices, and reporting.



The image above shows a typical network diagram of a global enterprise that has many sites with varying sizes. You may see traffic coming from one site to another, as well as to and from sites to headquarters. How can we measure which site is consuming most of the WAN bandwidth? Which site has the worst user experience from an application point of view? Which site has more wired clients compared to wireless clients? This is just a partial list of questions that a network engineer could have and that can be easily answered with Cisco Prime Infrastructure.

If you have an Assurance add-on license, you should be able to get an aggregated view from all the data sources in your network as shown in the following figure below:



As we can see, some of the devices are being polled by Cisco Prime Infrastructure using SNMP, while Prime Infrastructure can also collect NetFlow from other data sources directly. In case of Cisco Prime Network Analysis Module (NAM), Cisco Prime Infrastructure collects all the information from the NAM natively. On the other hand, the NetFlow Generation Appliance (NGA) sends NetFlow to Cisco Prime Infrastructure. Routers and switches capable of NetFlow and medianet can be enabled and configured by Cisco Prime Infrastructure to get application visibility for the ones that flow through them.

Installation

The Cisco Prime Infrastructure software runs on either a dedicated Cisco Prime Appliance (PRIME-NCS-APL-K9) or on a VMware server. The Cisco Prime Infrastructure software image does not support the installation of any other packages or applications on this dedicated platform. The Cisco Prime Infrastructure application comes preinstalled on a physical appliance with various performance characteristics.

Prerequisites

Cisco Prime Infrastructure runs on a 64-bit, Red Hat Linux Enterprise Server 5.4 operating system. You cannot install Cisco Prime Infrastructure on a standalone operating system such as Red Hat Linux, as Cisco Prime Infrastructure is shipped as a physical or virtual appliance that comes preinstalled with a secure and hardened version of Red Hat Linux as its operating system.

Server Requirements

The recommended deployments for a virtual appliance are ESX and ESXi. The following table shows the resources needed for different sizes of the virtual appliance.

Virtual Appliance Size	VMware ESX/ESXi	Processor	DRAM	Hard Disk	Minimum IOPS MBytes/sec **
Small Virtual Appliance	Version 4.1 or 5.0	4 vCPUs	8 GB	200 GB	200 MBps
Medium Virtual Appliance	Version 4.1 or 5.0	4 vCPUs	12 GB	300 GB	200 MBps
Large Virtual Appliance	Version 5.0	16 vCPUs	16 GB	400 GB	200 MBps
Extra Large Virtual Appliance	Version 5.0	16 vCPUs	24 GB	1200 GB	200 MBps

** Refer to "Logging In to Cisco Prime Infrastructure for the First Time" for more details on calculating IOPS.


Cisco Prime Appliance comes with the specifications shown in the following table:

Physical Appliance	Processor	DRAM	Hard Disk
Cisco Prime Appliance	16 CPUs	16 GB	900 GB (After RAID5)

Client Requirements

The following table shows all the supported browsers that can be used to access Cisco Prime Infrastructure.

Supported Browser	Browser Version	Additional Note
Internet Explorer	8.0 or 9.0	Chrome Plug-in is strongly recommended.
Firefox	13 or later	Latest Firefox v may be used, but it's not tested
Firefox ESR	ESR 10.x	ESR is the more stable version with less frequent updates.
Google Chrome	19.0 or later	Latest Chrome may be used, but it's not tested

 **TIP:** It is strongly recommended to use client with at least 4GB or more. Adding more memory will definitely enhance the end-user experience.

Server Sizing Matrix

The following table should help users to pick the right OVA size image for Prime Infrastructure Virtual Appliance:

Prime Infrastructure 1.3 Sizing	Small	Medium	Large	X-Large
Network Devices				
• Max Wired Devices	100	300	6,000	13,000
• Max Controllers	2	5	500	1,000
• Max Autonomous APs	100	300	3,000	3,000
• Max Unified APs	100	300	5,000	15,000
• Max NAMs	0	0	500	1,000
Total Max Devices	250	500	10,000	18,000
Max Wired Clients	1000	6,000	50,000	50,000
Max Wireless Clients	1000	4,000	75,000	200,000
Max Roaming Clients	250	1,000	25,000	40,000
Max Events (events/sec)	100/sec	100/sec	300/Sec	1000/sec
Max Netflows Rate (flows/sec)	0	0	16,000	80,000

Sizing Notes:

- Netflow is supported only on Large and X-Large OVA in Prime Infrastructure 1.x
- Sizing Numbers are based on internal testing

Installing the Cisco Prime Infrastructure Virtual Appliance

Cisco Prime Infrastructure is delivered as a Virtual Appliance a.k.a Open Virtualization Archive ([OVA](#)) file. OVA files allow you to easily deploy a prepackaged virtual machine (VM) - an application along with an operating system. Please follow the link below for detailed instruction on installing Prime Infrastructure Virtual Application.

- [Installing Cisco Prime Infrastructure](#)
- [Before You Begin](#)
- [Deploying the OVA](#)
- [Installing the Server](#)

Installing Cisco Prime Infrastructure on a Physical Appliance

Cisco Prime Infrastructure 1.3 comes preinstalled on the PRIME-NCS-APL-K9 physical appliance. The Cisco Prime Infrastructure 1.3 software image does not support the installation of any other packages or applications on this dedicated platform. If for some reason the appliance comes without any software, the application may be installed from the DVD that comes with it. Once the server boots up, the procedure will be similar to the procedure described for a virtual appliance.

Starting/Stopping Cisco Prime Infrastructure Services

In normal circumstances, you will not have to stop or start **ncs** services. The services will start automatically once installation is complete, and no manual startup of services is required. If there is a need to restart the services for some reason, the following commands may be executed by the admin user from the CLI:

pi1.cisco.com/admin# **ncs stop** - Stops the Cisco Prime Infrastructure server

pi1.cisco.com/admin# **ncs status** - Shows the Cisco Prime Infrastructure server status

pi1.cisco.com/admin# **ncs start** - Starts the Cisco Prime Infrastructure server

```
Type Licensed
VUDI PRIME-NCS-VAPL;pi1:af4ee9e0-ec0d-11e1-82f1-005056857f2f
Product Id PRIME-NCS-VAPL
Serial Number pi1:af4ee9e0-ec0d-11e1-82f1-005056857f2f
```

Logging into Cisco Prime Infrastructure for the First Time

Once the Cisco Prime Infrastructure server has been installed and configured, it is now ready to be accessed from the web. The server URL would be https://server_hostname or <https://ip.ad.dr.ess>. In Cisco Prime Infrastructure 1.3, login using the following credential for the very first time:

Username: **root**

Password: <the root password is the one that was entered during the install script>

After the server has been configured, it is advisable to log in with a non-root user to keep the root user for system level configurations as and when needed. More updated information can be found at Prime Infrastructure 1.3 Quick Start Guide at [Logging into the Prime Infrastructure User Interface](#)

Verifying IOPS for Prime Infrastructure Virtual Machine

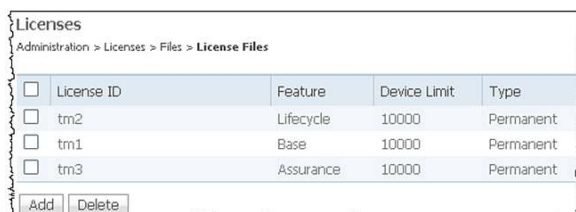
Until Prime Infrastructure 1.3, there was no easy way to verify datastore IOPS for the virtual infrastructure. With the addition of the following new command, users can now verify the raw performance before proceeding any further. Here is how to use the command (from root shell):

```
pi13-test5/admin# ncs run test iops
Testing disk write speed ...
8388608+0 records in
8388608+0 records out
8589934592 bytes (8.6 GB) copied, 128.195 seconds, 67.0 MB/s
```

Note that the recommended value for the IOPS (Input/Output Operations Per Second) is 200 MB/s as mentioned in the server requirement section.

Licensing

After you have installed Cisco Prime Infrastructure for the first time you may access the lifecycle and assurance features using the built-in evaluation license that is available by default. The default evaluation license is valid for 60 days for 100 devices and 150 interfaces. You will need to purchase the base license and the corresponding feature license before the evaluation license expires. Cisco Prime Infrastructure 1.3 can be ordered using the standard Cisco® ordering tools at <http://www.cisco.com/go/ordering>. More information about getting the license files can be found in the [Cisco Prime Infrastructure 1.x Ordering and Licensing Guide](#). Note that you order Cisco Prime Infrastructure 1.3 using the Cisco Prime Infrastructure 1.2 part numbers. The 1.2 part numbers have been updated to deliver 1.3 software, rather than 1.2.”



<input type="checkbox"/>	License ID	Feature	Device Limit	Type
<input type="checkbox"/>	tm2	Lifecycle	10000	Permanent
<input type="checkbox"/>	tm1	Base	10000	Permanent
<input type="checkbox"/>	tm3	Assurance	10000	Permanent

Add Delete

Cisco Prime Infrastructure licenses are locked to a specific Cisco Prime Infrastructure instance based on a unique device identifier (UDI) for a physical appliance or a virtual unique device identifier (VUDI) for a virtual appliance (figure above). The identifier can be found within the Cisco Prime Infrastructure user interface under Administration > Licenses. Once you have obtained the license file (.lic), you are now ready to apply it. License files can be added to Cisco Prime Infrastructure by going to Administration > Licenses > Files > License Files. The license files should look like the figure on the right. For more information on Cisco Prime Infrastructure licensing you can also refer to the [Cisco Prime Infrastructure 1.3 Quick Start Guide](#).

Configuring Backup

At this point, you do not have any data, but soon you will start accumulating lots of data. It is strongly advisable to configure the backup plan in a more proactive manner. Backup can be configured by navigating to Administration > Background Tasks > Other Background Tasks (Section) > Prime Infrastructure Server Backup. You can either use the default repository, defaultRepo, or create an external backup repository by clicking the Submit button as shown in the figure (below). Enter FTP credentials and other relevant information to create this new remote backup repository.



Advanced System Settings

There are some settings in Cisco Prime Infrastructure that need to be looked at closely before you start to manage the network. Optimal settings are already configured, but you may need to tweak the settings based on the network you are managing. You can access the settings by navigating to Administration > System Settings.

Data Retention

This menu item (Administration > System Settings) allows you to specify how much data is to be stored in Cisco Prime Infrastructure. By default you can store up to 7 days of raw data and 1 year worth of aggregated data. You can increase these numbers based on the hard drive space that is provided to Cisco Prime Infrastructure.

Accessing Cisco Prime Infrastructure Through the CLI

In normal circumstances, you may not need to access the CLI, but if there is a need for access to some service requirements, the Cisco Prime Infrastructure server may be accessed through Secure Shell Protocol Version 2 (SSH2) by the admin user. The admin user is provided with a Cisco IOS® Software-like shell, which is the preferred shell for carrying out most operational tasks. The password for this admin user is configured during the initial installation and configuration, as mentioned in the “Installing the Cisco Prime Infrastructure OVA” section. Please note that the root password that is prompted in the install script is **only** for web access and not access to the CLI.

How to Enable the CLI Root User in the Cisco Prime Infrastructure Server

The root user is **not** enabled by default, but you can enable the root user for the first time using the **root_enable** command at the admin console. Once the root user is enabled, log out of the admin shell and login using the **root** user and the previously defined password for root.

High Availability

The Cisco Prime Infrastructure High Availability (HA) implementation allows one primary Cisco Prime Infrastructure server to failover to one secondary (backup) Cisco Prime Infrastructure server. A second server is required that has sufficient resources (CPU, hard drive, network connection) in order to take over Cisco Prime Infrastructure operation in the event that the primary Cisco Prime Infrastructure system fails. In Cisco Prime Infrastructure, the only HA configuration is supported is 1:1 - 1 primary system, 1 secondary system.

The size of the secondary server must be larger than or equal to that of the primary server; for example, if the primary Cisco Prime Infrastructure server is the medium OVA, then the secondary Cisco Prime Infrastructure server must be the medium or large OVA.

HA Setup

The primary and secondary server can be a mix of a physical and a virtual appliance. For example, if the primary Cisco Prime Infrastructure server is a physical appliance, the secondary server can be either a physical appliance or a large OVA virtual appliance; for example, the server configuration and sizing of large OVA is the same as the physical appliance. Customers must be running the same version of Cisco Prime Infrastructure on both the primary and secondary Cisco Prime Infrastructure servers. The Cisco Prime Infrastructure HA feature is transparent to the wireless controller, that is, there is no software version requirement for the Cisco Wireless LAN Controller (WLC), access points (APs), and the Cisco Mobility Services Engine (MSE).

Licensing

Only one Cisco Prime Infrastructure server license needs to be purchased. There is no need to purchase a license for the secondary Cisco Prime Infrastructure server. The secondary server will use the license from the primary when a failover occurs. The secondary node will simulate the UDI information of the primary; thus the secondary server will be able to use the synchronized license from the primary server when the secondary server is active. The same Cisco Prime Infrastructure license file resides on both the primary and secondary Cisco Prime Infrastructure servers. Since the Cisco Prime Infrastructure JVM is only running on the primary or secondary (not both), the license file is only active on one system at a given point in time.

Cisco Prime Infrastructure High Availability Setup

Cisco Prime Infrastructure HA can also be deployed with geographic separation of the primary and secondary servers. This type of deployment is also known as Disaster Recovery (DR), or Geographic Redundancy.

HA Modes

There are two HA modes: failover and failback. Let's take a look at each of them in detail.

Failover

After initial deployment of Cisco Prime Infrastructure, the entire configuration of the primary Cisco Prime Infrastructure server is replicated to the host of the secondary Cisco Prime Infrastructure server. During normal operation (that is, when the primary Cisco Prime Infrastructure server is operational), the database from the primary server is replicated to the secondary Cisco Prime Infrastructure server. In addition to the database replication, application data files are also replicated to the secondary Cisco Prime Infrastructure server. Replication frequency is 11 seconds (for real - time files) and 500 seconds (for batch files).

Failback

When the issues on the server that host the primary Cisco Prime Infrastructure server have been resolved, failback can be manually initiated. Once this is done, the screen is displayed on the secondary Prime Infrastructure server. When you initiate failback, the Cisco Prime Infrastructure database on the secondary Cisco Prime Infrastructure server and any other files that have changed since the secondary Cisco Prime Infrastructure server took over Cisco Prime Infrastructure operation are synchronized between the secondary and the primary Cisco Prime Infrastructure servers. Once database synchronization has been completed, the primary Cisco Prime Infrastructure JVM is started by the primary HM. When the primary Cisco Prime Infrastructure JVM is running, the following screen is displayed on the secondary HM.

Health Monitor Details

Settings

Status	Remote NCS IP Address	State	Failover Type	Action
✖	171.69.217.142	Primary Alone	automatic	None

Logging

Message Level

Information ▼

Set Logging

Logs

Download Health Monitor Log Files

Download

Events

Manual/Automatic Options

Automatic Failover

Automatic failover is a much simpler process. The configuration steps are the same except that automatic failover is selected. Once automatic failover is configured, the network administrator does not need to interact with the secondary HM in order for the failover operation to take place. Only during failback is human intervention required.

Primary Failure Example - Manual Failover

In this example, the secondary Cisco Prime Infrastructure server was configured with manual failover. For example, the network administrator is notified through email that the primary Cisco Prime Infrastructure server has experienced a down condition. The Health Monitor on the secondary Cisco Prime Infrastructure server detects the failure condition of the primary Cisco Prime Infrastructure server. Because manual failover has been configured, the network administrator needs to manually trigger the secondary Cisco Prime Infrastructure server to take over Cisco Prime Infrastructure functionality from the primary Cisco Prime Infrastructure server. This is done if you log in to the secondary HM. Even though the secondary Cisco Prime Infrastructure server is not running, the secondary HM can be connected to through this syntax:

`https://<Secondary_PI_IP_Address>:8082/`

The secondary HM displays messages in regard to events that are seen. Because manual failover has been configured, the secondary HM waits for the system administrator to invoke the failover process. Once manual failover has been chosen, the message is displayed as the secondary Cisco Prime Infrastructure server starts. Once the failover process has been completed, which means that the Cisco Prime Infrastructure database replication process is completed and the secondary Cisco Prime Infrastructure JVM process has started, then the secondary Cisco Prime Infrastructure server is the active Cisco Prime Infrastructure server.

Health Monitor on the secondary Cisco Prime Infrastructure server provides status information on both the primary and secondary Cisco Prime Infrastructure servers. Failback can be initiated through the secondary HM once the primary Cisco Prime Infrastructure server has recovered from the failure condition. **The failback process is always initiated manually** so as to avoid a flapping condition that can sometimes occur when there is a network connectivity problem.

Upgrade and Data Migration from Previous Applications

Upgrading to Prime Infrastructure 1.3

Users can upgrade to Prime Infrastructure 1.3 only from one of the following supported versions:

- Prime Infrastructure 1.1.0.58
- Prime Infrastructure 1.1.1.24
- Prime Infrastructure 1.2.1.12

Patch Requirements: If you are using NCS 1.1.1.24, you **MUST** apply the patch before beginning the upgrade process. You can find the more patch details at:

http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.3/quickstart/guide/cpi_qsg_1_3.html#wp69624

Note: Recommended best practice is to use “database restore” instead of an “in-line upgrade”.

Migrating from WCS 7.x to NCS 1.1.1.24

Direct migration from WCS 7.x to PI 1.3 is **NOT** possible. **We strongly recommend upgrading your WCS to 7.0.230.0 or higher before attempting to migrate to NCS.** Users will first need to do an intermediary migration to NCS 1.1.1.24, and then do an inline upgrade (or migration) to Prime Infrastructure 1.3.

- [Migrating WCS to NCS 1.1](#)
 - [Exporting WCS Data](#)
 - [Migrating WCS Data to NCS](#)
 - [Non-upgradable Data](#)
 - [Migrating WCS User Data to NCS 1.1 \(for Multiple WCS Servers\)](#)
 - [Upgrading Prime Infrastructure in a High Availability Environment](#)

Migrating from NCS 1.1.1.24 to Prime Infrastructure 1.3

To migrate to a new Prime Infrastructure 1.3 system, follow the process as described in the following two links below:

- [Back Up the Data from the Existing System](#)
- [Install a New Prime Infrastructure System and Migrate the Data from the Backup](#)
- [Restoring Prime Infrastructure Database in a High Availability Environment](#)

From LMS

Cisco Prime LMS features were reevaluated for usefulness, usability, and value. Some features are redesigned and have transitioned, some are on the road map, others are to be determined by customers, and a few are being deprecated.

LMS 2.x

LMS 2.x has reached its end of life, and that is why upgrading from LMS 2.x to Cisco Prime Infrastructure 1.3 is not supported. Customers could export their device inventory into a comma-separated value (CSV) file for their own records. Alternatively customers can also start using Cisco Prime Infrastructure 1.3 for basic network management type features.

LMS 3.x

LMS 3.x has also reached end of engineering. If you are currently using basic management features such as monitoring, configuration management, inventory management, software image management, and fault management, you should consider upgrading to Cisco Prime Infrastructure 1.3. Although data migration is not possible, you should still be able to manage your network in no time starting with discovery from within Cisco Prime Infrastructure 1.3.

LMS 3.x customers using features like CiscoView, Layer 2 topology, IP service-level agreements (IP SLAs), and VLAN management are recommended to run Cisco Prime Infrastructure 1.3 as a separate server side by side or to wait until all the features have been migrated into Cisco Prime Infrastructure 2.x.

LMS 4.x

LMS 4.x customers using basic management features like monitoring, syslogs, configuration management, inventory management, software image management, and fault management should consider migrating to Cisco Prime Infrastructure 1.3.

LMS 4.x customers using features like CiscoView, Layer 2 topology, IP SLAs, work centers, and VLAN management are recommended to run Cisco Prime Infrastructure 1.3 as a separate server side by side or to wait until all the features have been migrated into Cisco Prime Infrastructure 2.x.

Exporting from LMS 4.2.2

With LMS 4.2.2, there is a way right from the web interface to export the device list with credentials that can be consumed by Cisco Prime Infrastructure. The device list can be exported from Administration > Export Data to Cisco Prime Infrastructure (under System). Then select Export Device List and Credentials from the export options as shown in the below figure.



Importing into Cisco Prime Infrastructure 1.3

Once you have the exported device list with credentials from LMS 4.2.2, it can be imported into Cisco Prime Infrastructure 1.3 by navigating to Operation > Device Work Center > Bulk Import as shown in following figure:



Application Setup

Cisco Prime Infrastructure 1.3 introduces a new lifecycle approach to managing your wired and wireless infrastructure. There are five phases in this lifecycle: design, deploy, operate, report, and administer. The details for each of these phases are briefly described below:

Lifecycle Management

Design

In this phase, you can assess, plan, and create configurations required to roll out new network services and technologies. Create templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the-box implementation, automating the work required to use Cisco validated designs and best practices.

Deploy

In this phase, you can schedule the rollout and implementation of network changes. Changes may include published templates created in the design phase, software image updates, and support for user-initiated ad hoc changes and compliance updates. This accelerates service rollout, minimizes chances for errors, and is highly scalable.

Operate

In this phase, you can utilize preconfigured dashboards to provide up-to-date status monitoring on the overall health of the network. Simple one-click workflows and 360-degree views enhance troubleshooting and reduce the time to resolve network issues. Unified alarm displays with detailed forensics provide actionable information and the ability to automatically open service requests with the Cisco Technical Assistance Center (TAC).

Report

In this phase, you can provide a wide variety of preconfigured reports for up-to-date information on the network, including detailed inventory, configuration, compliance, audit, capacity, end of sale, security vulnerabilities, and many more. Reports can be scheduled or run immediately, emailed, or saved as PDFs for future viewing purposes.

Administer

In this phase, you can provide an easy-to-use set of workflows that help to maintain the health of the application and keep devices, users, and the software up to date, allowing the IT staff to focus on other important activities.

Creating Groupings and Sites

Cisco Prime Infrastructure provides a very easy way to map each of the devices into its own site. There is also an ability to create groups based on predefined rules or criteria. Let's take a look at how to create sites and groups in Cisco Prime Infrastructure to help visualize applications in an intuitive manner.

Create Sites

There are two way of creating sites. If your access points follow a very consistent naming convention, you can automatically create a site tree map based on the hostname. The image at left below shows how a device hostname separated by hyphens can be used as a delimiter to create a site map tree automatically.

To create an automatic site hierarchy go to **Design > Automatic Hierarchy Creation**. Enter the AP Hostname and a suitable regular expression (or generate one as mentioned in the tip below). Click **Test** to see how the site is created from the hostname. Change the pull-down to map to the appropriate campus, building, floor, device, and so on.

Sample AP name: LON-Oxford-1-3500

Delimiter: - Create basic regex based on delimiter

Regular expression: (.*)-(.*)-(.*)-(.*)

See Examples Test

Match the groups of your regular expression with Campus, Building, and Floor:

Group #	Group type	Resulting map name
Group 1	Campus	LON
Group 2	Building	Oxford
Group 3	Floor/Outdoor Area	1
Group 4	Device	3500

Your device will appear in the map LON > Oxford > 1

TIP: After entering a sample hostname for an AP, you can click **Create basic regex based on delimiter** to automatically generate the regular expression.

Import/Edit Maps from WCS/NCS to Cisco Prime Infrastructure

If you have already created sites for the wireless network in a previous version of WCS or NCS, you can export from those applications and import the information into Cisco Prime Infrastructure as well. You can go to **Design > Site Map Design > Import Maps > Choose File** (as shown in figure below).

Import Map

Monitor > Maps > Import Map

Step 2 of 4: Select a file previously exported from WCS or NCS to Import

Import Map data with XML Format (File exported from WCS or NCS)

Choose File No file chosen

Next Cancel

Once the file has been uploaded, all the sites will be automatically created by Cisco Prime Infrastructure.

Associate Endpoints to Sites

Now that you have created all the sites where your network equipment is staged, it is time to map those sites to their respective subnets, data sources, and VLANs. This allows Cisco Prime Infrastructure to see the traffic flow, especially when it comes to application performance. In order to create an endpoint, you can go to **Design > Endpoint-Site Association**. The image below shows how various sites are mapped to their subnets. In addition to the subnet mask, you can also specify the default data source desired for that site in addition to the VLANs for those sites.

Site	SubNet	Data Source	VLAN
Amsterdam Branch	192.168.152.0/26		
Boxborough Branch	10.5.0.0/16		
Denver Branch	10.9.0.0 / 16		
India Branch	10.7.0.0/16		
London Branch	10.11.0.0/16		
Los Angeles Branch	10.2.0.0/16		
Management Apps	192.168.0.0/16		
Management Apps	171.0.0.0/8		

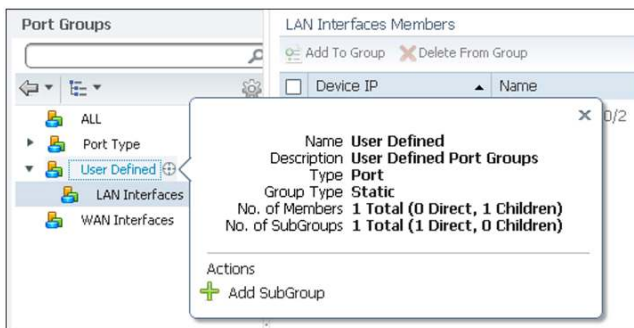
Endpoint-Site Association

SubNet: 10.9.0.0 / 16

Data Source: 10.0.109.2-32582, 10.0.107.2-32630

Create Port Groups

The next step in getting started with Cisco Prime Infrastructure is to create groups in addition to the default port groups that come preconfigured. Port groups creation can be accessed from **Design > Port Grouping**. If a custom port group needs to be created, you can hover over **User Defined** and click the plus sign icon to access a pop-up menu for adding a new group as shown in image below.



The WAN Interfaces port group is a special preconfigured port group. The interfaces in this group are your WAN interfaces that need to be actively monitored. In order to add WAN interfaces to this group, select all groups and filter the WAN interfaces based on your interfaces type, IP address, interface description, or any other attributes that are used to denote a WAN interface group. It is highly recommended to populate this group with the WAN interface to get the most out of this application.



Users and User Group Management

Adding New Users

As noted earlier, it is not advisable to use the root user to log in for normal use. New users and groups can be created by choosing

Administration > Users, Roles & AAA as shown in preceeding figures. It would help to chalk out what are the various levels at which you want to distribute the users, and to create those roles first. It doesn't really matter whether you create users or groups first. New users can be easily added by going to **Administration > Users, Roles & AAA > Users > Add Users** (from the drop-down on the right). Once you get into the add user workflow, fill in the username, password, and local authorization for this user as shown in the figure below.

User Groups
Administration > Users, Roles & AAA > User Groups

Group Name	Members	Audit Trail	Export
Admin	test1, bkapoor		Task List
Config Managers	bkapoor		Task List
Lobby Ambassador			Task List
Monitor Lite			Task List
North Bound API			Task List
Root	root		Task List
Super Users	test1, bkapoor		Task List
System Monitoring	bkapoor		Task List
User Assistant			Task List
User Defined 1	prime		Task List
User Defined 2	test		Task List

A virtual domain can also be assigned to the users when you define their roles by selecting the virtual domain on the left side and moving it to the right side as shown in image below.

Add User
Administration > Users, Roles & AAA > Users > Add User

General Virtual Domains

Available Virtual Domains	Selected Virtual Domains
	ROOT-DOMAIN

Available Virtual Domains

ADD > < Remove

Creating User Groups

User groups are synonymous with roles. All the roles except User Defined # are preconfigured. User-defined groups can be modified by going to **Administration > Users, Roles & AAA > User Groups > User Defined #**. Other groups and roles cannot be modified, but you can add users to them, see the audit trail, and even export the TACACS+/RADIUS command sets by clicking the task list. User-defined roles can be modified by clicking the User Defined # link in the figure above (left). Once clicked, all the knobs on the user access controls are exposed as shown in the figure above (below). You can select the whole category, for example, Network Configuration, or a few of the options within that category to customize the role. Once the group/role is created, multiple users can then be assigned to that group.

Tasks Permissions Members

☒ Mobility Service Management ☒ View CAS Notifications Only

☒ Monitor Menu String Task

☒ Monitor Menu Access

☒ Network Configuration

<input checked="" type="checkbox"/> Configure Autonomous Access Point Templates	<input checked="" type="checkbox"/> Config Archive Read-Write Task
<input checked="" type="checkbox"/> Design Configuration Template Access	<input checked="" type="checkbox"/> WIPS Service
<input checked="" type="checkbox"/> Add Device Access	<input checked="" type="checkbox"/> Device View configuration Access
<input checked="" type="checkbox"/> Configure Ethernet Switches	<input checked="" type="checkbox"/> Configure Lightweight Access Point Templates
<input checked="" type="checkbox"/> Device Bulk Import Access	<input checked="" type="checkbox"/> Configure Templates
<input checked="" type="checkbox"/> Configure WIPS Profiles	<input checked="" type="checkbox"/> Migration Templates
<input checked="" type="checkbox"/> Configure Ethernet Switch Ports	<input checked="" type="checkbox"/> Configure ACS View Servers
<input checked="" type="checkbox"/> Configure WFI TDOA Receivers	<input checked="" type="checkbox"/> Deploy Configuring Access
<input checked="" type="checkbox"/> Auto Provisioning	<input checked="" type="checkbox"/> Configure Controllers
<input checked="" type="checkbox"/> Configure Spectrum Experts	<input checked="" type="checkbox"/> Delete Device Access
<input checked="" type="checkbox"/> Configure Choke Points	<input checked="" type="checkbox"/> Global SSID Groups
<input checked="" type="checkbox"/> Scheduled Configuration Tasks	<input checked="" type="checkbox"/> Configure ISE Servers
<input checked="" type="checkbox"/> Device WorkCenter	<input checked="" type="checkbox"/> Config Archive Read Task
<input checked="" type="checkbox"/> Configure Third Party Controllers and Access Point	<input checked="" type="checkbox"/> Configure Access Points
<input checked="" type="checkbox"/> Configure Switch Location Configuration Templates	<input checked="" type="checkbox"/> Configure Config Groups

Image Management
Administration > System Settings > Image Management

Cisco.com user name

Cisco.com password

SSH user name

SSH password

Staging directory

☒ Continue distribution on failure

☐ Collect images along with inventory collection

☐ Reboot immediately

☐ Distribute parallelly

☐ TFTP fallback

☐ Backup current image

☐ Insert boot command

☐ Recommend latest maintenance version of each major release

☐ Recommend Same Image Feature

☐ Recommend versions higher than current version

☐ Recommend general deployment images only

☒ Include CCO for recommendation

☐ Use SCP for image upgrade and import

Image transfer protocol order

TFTP
SCP

Image Management Settings

There aren't any mandatory settings required for software image management, but a number of knobs can be accessed from **Administration > System Settings > Image Management** as shown in figure above. These include team shared cisco.com username/password, job failure handling options, image and configuration protocol options, and so on. Users are strongly recommended to glance through this page and set it up initially so that preferred preferences are applied when distributing images on managed devices. Images can easily be added to the local repository by choosing **Operate > Software Image Management > Import**. Follow the wizard to import images from cisco.com directly. Images can be deployed to devices by going to **Operate > Software Image Management**. Select the image from the list (once it has been added to the repository) and click **Distribute Images**. Once the devices are selected to be upgraded/downgraded, a prerun status is shown, which avoids the job failure in the first place. You can also run Upgrade Analysis from the same place to get a report on this.

Distribute Images

Device Name	IP Address	Distribute Image Name	Distribute Location	Status	Status Message
FL4-3750S-1	10.15.10.1	c3750-ipservicesk9-mz.122-58.SE1.bin	flash1	✗	Warning: Required Spa...
3750-PHY-1	10.0.252.3	c3750-ipservicesk9-mz.122-58.SE1.bin	flash1	✓	Ok
AMS-3750-SBR	192.168.152.10	c3750-ipservicesk9-mz.122-58.SE1.bin	flash1	✗	Warning: Required Spa...
LON-3750-SBR	10.11.10.3	c3750-ipservicesk9-mz.122-58.SE1.bin	flash1	✗	Warning: Required Spa...
LA-3750-SBR	10.2.10.1	c3750-ipservicesk9-mz.122-58.SE1.bin	flash1	✗	Warning: Required Spa...
SIN-3750-SBR	10.6.10.1	c3750-ipservicesk9-mz.122-58.SE1.bin	flash2	✗	Warning: Required Spa...
NY-3750-SBR.cisco.com	10.4.10.1	c3750-ipservicesk9-mz.122-58.SE1.bin	flash1	✗	Warning: Required Spa...
RTP-3750-SBR	10.1.10.1	c3750-ipservicesk9-mz.122-58.SE1.bin	flash1	✗	Warning: Required Spa...
SF-3750-SBR	10.3.10.1	c3750-ipservicesk9-mz.122-58.SE1.bin	flash1	✓	Ok
BXB-3750-SBR	10.5.10.1	c3750-ipservicesk9-mz.122-58.SE1.bin	flash1	✓	Ok

▼ Distribution Options

☐ Insert boot command

☐ Distribute Parallelly

☐ Backup Current Image

☐ TFTP Fall Back

Reboot Device: OFF

☐ Erase Flash Before Distribution

☒ Continue on failure

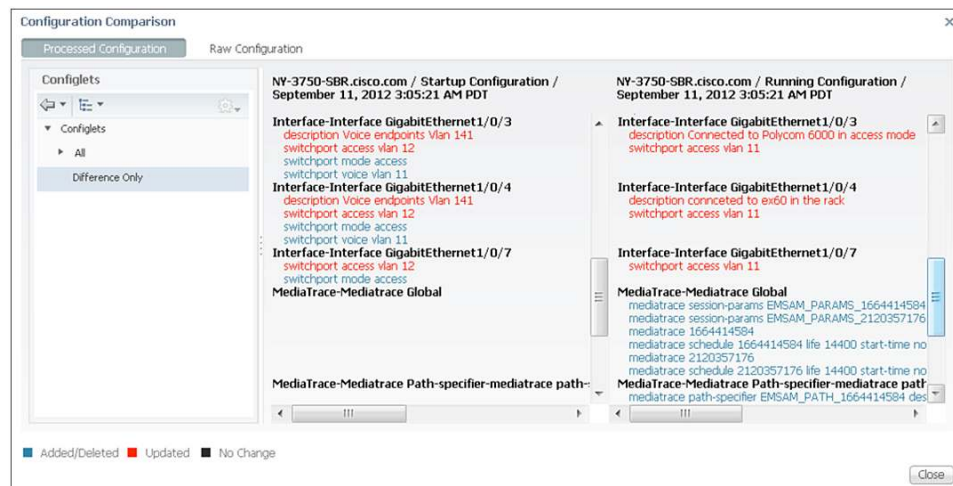
☐ Use SSH

Submit Cancel

Configuration Archive Settings

<input type="checkbox"/>	NY-3750-SBR.cis...	Cisco Catalyst 3750 Se...	10.4.10.1	Switches and Hubs/Cis...	September 11, 2012 3:05:21 A	Yes	Yes
	Date	Created By	Description			Out of band	
▼	<input type="radio"/>	September 11, 2012 3:05:21 AM P...	Inventory	Archived by inventory			Yes
	Configuration Type		Compare With				
	Running Configuration		Previous Startup Other Version Other Device				
	Startup Configuration		Previous Other Version Other Device				
	Vlan Configuration						

The Configuration Archive will be one of the most used portions from a daily operation point of view. It is highly recommended to go to Administration > System Settings > Configuration Archive. The Basic tab allows users to define protocol order, Simple Network Management Protocol (SNMP) timeout, the number of days and the versions to retain, thread pool count, and other such variables. The Advanced Tab allows users to define a command exclude list for each of the device family types. Once this is done, users may view and compare configurations by navigating to **Operations > Configuration Archives** (under the Device Work Center). Browse the device and open up the tree to see all the configuration versions that have been archived for this device as shown in the preceeding figure. When you click Compare there, you quickly see the color-coded configuration differences instantly as shown in same preceeding figure.



Configuring NTP and DNS for NAMs

It is extremely important to configure NTP and DNS for all the NAMs in your network. You can now configure those without going to the CLI or logging in to the individual NAM web GUIs. From the Cisco Prime Infrastructure Device Work Center, navigate to Device Group > Device Type > Cisco Interfaces and Modules. Click the name of the NAM on which you want to configure NTP/DNS, and then click **Configure** in the bottom pane. Now click **Feature** on the left (still in the bottom pane), and you will see a link for "system." Click it to see a form for this NAM that allows you to configure all the system-related information for a given NAM including NTP and DNS. The following image shows where the NTP and DNS can be configured.

Device Group > Device Type > Cisco Interfaces and Modules

Cisco Interfaces and Modules

Selected 1 | To

Edit Delete Sync Groups & Sites Add Device Bulk Import Show All

<input type="checkbox"/>	Device Name	Reachability	IP Address	Device Type	Collection Status	Collection Time	Software Version
<input type="checkbox"/>	ACC-NAM2204.c...	Unreachable	192.168.136.67	Cisco NAM 2204 ...	Managed with Warri...	September 28, 2...	5.1(1)
<input checked="" type="checkbox"/>	Campus-NAM3.es...	Reachable	192.168.136.129	Cisco Catalyst 65...	Managed	October 25, 201...	5.1(2)
<input type="checkbox"/>	DC-NAM2220.cisc...	Reachable	192.168.136.32	Cisco NAM 2220 ...	Managed	October 25, 201...	5.1(2)
<input type="checkbox"/>	NAM	Reachable	192.168.136.123	Cisco SM-SRE Ne...	Managed with Warri...	October 25, 201...	
<input type="checkbox"/>	RTP-NAM-SRE.cis...	Reachable	192.168.136.131	Cisco SM-SRE Ne...	Managed	October 25, 201...	5.1(2-patch5)

Configuration Archive Image

▼ DNS Parameters

Domain Name Name Servers

► SNMP Agent

▼ System Time

Synchronize System Time with NTP ☒

Primary NTP Server Name/IP Address
 Secondary NTP Server Name/IP Address
 Time Zone

Connection to Cisco.com

Cisco.com connection is required for some of the advanced features such as Smart Interactions (TAC service requests, and support forums), importing software images, contract connection, and many others. It is vital for the Cisco Prime Infrastructure server to be able to connect to cisco.com to pull the data for those reasons. There are two parts to making this work: proxy settings and cisco.com user settings.

Proxy Settings

If Cisco Prime Infrastructure requires a proxy to connect to the Internet, you can enter the proxy information by going to **Administration > System Settings > Proxy Settings**. You can enable proxy settings and enter all the proxy information there. Authenticating proxies is also supported in Cisco Prime Infrastructure.

Cisco.com Settings

Once the proxy settings are configured, you can enter your cisco.com credentials at the following places:

- Administration > System Settings > **Image Management**
- Administration > System Settings > **Support Request Settings**

Planning/Preparing the Network

Wireless Planning Tool

The built-in planning tool provides a way for network administrators to determine what is required in the deployment of a wireless network. As part of the planning process, various criteria are input into the planning tool. Complete these steps:

1. Specify the AP prefix and AP placement method (automatic versus manual).
2. Choose the AP type and specify the antenna for both the 2.4 GHz and 5 GHz bands.

3. Choose the protocol (band) and minimum desired throughput per band that is required for this plan.
4. Enable planning mode for advanced options for data, voice, and location. Data and voice provide safety margins for design help. Safety margins help design for certain RSSI thresholds, which is detailed in online help. The location with monitor mode factors in APs that could be deployed to augment location accuracy. The location typically requires a denser deployment than data, and the location check box helps plan for the advertised location accuracy.
5. Both the Demand and Override options allow for planning for any special cases where there is a high density of client presence such as conference rooms or lecture halls.

Generated proposal contains these:

- Floor plan details
- Disclaimer/scope/assumptions
- Proposed AP placement
- Coverage and data rate heat map
- Coverage analysis

Add APs

Name Prefix

Add APs

AP Type

Enable 11n Support ☐

802.11a/n Antenna

802.11b/g/n Antenna

Protocol

Throughput (MB/s)

802.11a/n

802.11b/g/n

Services: ☐ Advanced Options

☒ Data/Coverage
☐ Voice
☒ Location
☐ Location with Monitor Mode APs

Total Coverage Area 16 (sq feet)

Recommended AP Count:

Data/Coverage 4

Voice 1

Location 4

Location with Monitor Mode APs

Demand

Override Coverage Per AP

Ports Used

The following table shows all the ports that are used by Cisco Prime Infrastructure to communicate with devices and with other Cisco Prime Infrastructure servers.

Protocol	Transport	Port Used	Port Usage Description
ICMP		7	Server to endpoints. Endpoint discovery
SSH	TCP	22	SSH to Cisco Prime Infrastructure/Assurance server
SCP	TCP	22	SCP to Cisco Prime Infrastructure/Assurance server
TFTP	UDP	69	Network devices to Cisco Prime Infrastructure/Assurance server
FTP	TCP	2021	FTP to Cisco Prime Infrastructure/Assurance server
SNMP	UDP	161	Cisco Prime Infrastructure/Assurance server to network devices/NAM
SNMP Trap	UDP	162	Network devices to Cisco Prime Infrastructure/Assurance server
Syslog	UDP	514	Network devices to Cisco Prime Infrastructure/Assurance server
JNDI		1099	AAA server to Cisco Prime Infrastructure/Assurance server
RMI		4444	AAA server to Cisco Prime Infrastructure/Assurance server
HTTPS	TCP	443	Browser to Cisco Prime Infrastructure/Assurance server
NetFlow	UDP	9991	Network devices/NAMs to Cisco Prime Infrastructure/Assurance server
JMS		61617	JMS port open for Automated Deployment Gateway
Health Monitor		8082	Prime Infrastructure Health Monitor Check. System use only

Protocol Check

For successfully managing a device using Cisco Prime Infrastructure, it is crucial that all the essential protocols be defined in the device credential for a given device. The following matrix shows what protocols are needed for various wired and wireless device types.

Device Family	SNMP RW	Telnet/SSH	HTTP
Wireless controllers	✓		
Wireless controllers (IOS XE)	✓	✓	
Access points	✓	✓	
Routers/switches	✓	✓	
Medianet-capable routers and switches	✓	✓	✓
Network Analysis Module	✓	✓	✓
Third-party devices	✓		

These credentials are sufficient to discover wired as well as wireless networks. Let's now focus on how to enable each of these protocols.

Configuring SNMP

SNMP is one of the protocols that Cisco Prime Infrastructure uses when talking to devices for getting basic information. When discovery is initiated, SNMP is used to query what type of device is it. Cisco Prime Infrastructure supports all versions of SNMP: v1, v2c, and v3 (noAuthNoPriv, authNoPriv, authPriv).

Enabling SNMP on Wireless Controllers

From the WLC web GUI, navigate to **Management > Communities** (under SNMP). Click **New** to create a new SNMP v1/v2c community. SNMP v3 community can be configured by going to the SNMP v3 User from the left panel menu.

Enabling SNMP on Routers/Switches

As the routers and switches may have Cisco IOS Software, Cisco IOS XE Software, or NX-OS running, it may be best to refer to

http://www.cisco.com/en/US/customer/tech/tk648/tk362/technologies_tech_note09186a0080094aa4,the.shtml documentation to configure SNMP on the devices. For configuring SNMP on Cisco Nexus® 5000 or similar devices, use

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/sm_snmp.html. For more devices, the following **sample** syntax should work for SNMP v1/v2c:

configure terminal

snmp-server community pu6l1c RO (using “public” is not recommended)

snmp-server community pr1vat3 RW (using “private” is not recommended)

Enabling Telnet/SSH on Routers/Switches

Cisco Prime Infrastructure can work with Telnet or SSHv2. If you are able to Telnet/SSH into the device, Cisco Prime Infrastructure should be able to do the same. If you have to enter another password to enable this, be sure to enter that in the device credentials. More on how to edit credentials is discussed in the section “Fixing Credential Errors.”

Enabling Telnet/SSH on Wireless Controllers

From the WLC web GUI, navigate to **Management > Telnet-SSH** to open the Telnet-SSH Configuration page. Allow either the Telnet or SSH sessions.

HTTP/HTTPS

The HTTP protocol is mainly used for a selected few devices as mentioned in the protocol matrix above. HTTP is used by NAM for Representational State Transfer (REST) API calls, as well as for enabling/disabling Mediatrace on medianet-capable devices. For medianet-capable devices, the HTTP user must have a privilege level of 15.

Preparing the Wireless Network

There are some tasks that are wireless centered, and do not apply to the wired infrastructure. Let's take a look at those in this section. This document assumes that your wireless infrastructure is up and running. If you need to deploy the wireless network, please refer to the NCS 1.1 Deployment Guide at

http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bba943.shtml.

Import Maps from WCS

The map export/import feature is available in WCS 7.0. This feature is detailed in the WCS 7.0 Configuration Guide, which is available at:

<http://www.cisco.com/en/US/docs/wireless/wcs/7.0/configuration/guide/WCS70cg.html>. After you export maps from your WCS server, you can import this set of maps in your NCS server. The next step on how to import your maps is covered in the WCS 7.0 Configuration Guide.



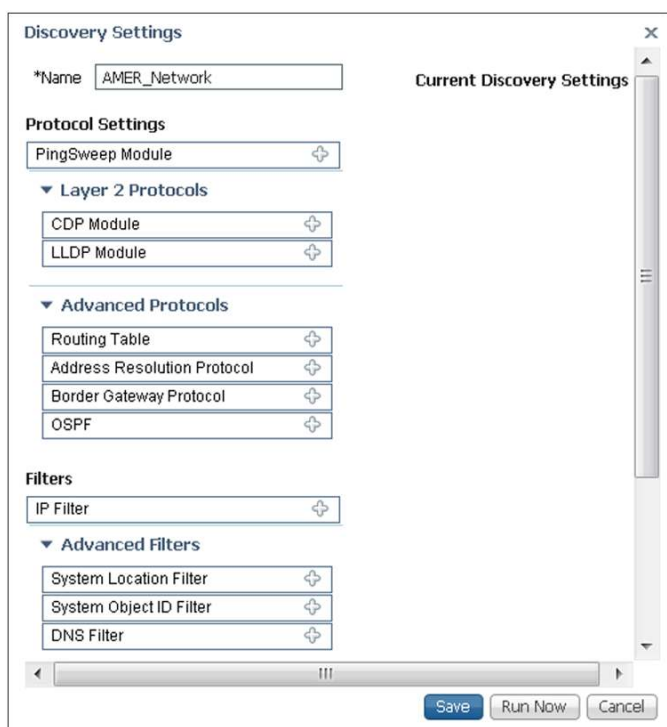
TIP: It is important that APs from your WCS server be added to your Cisco Prime Infrastructure server prior to importing maps, because APs on your WCS maps are also included during the export process. APs that have not been added to your Cisco Prime Infrastructure system, but are present on exported floor maps, result in errors that are displayed when you import those maps into Cisco Prime Infrastructure.

Discovering Your Network

Cisco Prime Infrastructure uses and enhances the discovery mechanisms that were used in Cisco Prime LMS 4.x. Protocols like ping, SNMP (v1, v2c, and v3), Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF) are used to discover the network. This section will focus on how best to configure the discovery profile once and to automate the discovery going forward.

Discover Devices

It is a very common practice to import the CSV file into the network management application and start managing the devices going forward. This is not a bad idea, but it leaves more chances for human error, especially if the spreadsheet is not updated with newly deployed devices in the network. With discovery, you always get the latest picture of your network.



The screenshot shows the 'Discovery Settings' dialog box. At the top, there is a field for '*Name' with the value 'AMER_Network'. To the right of this field is a tab labeled 'Current Discovery Settings'. Below the name field, there are several sections of settings:

- Protocol Settings:** A dropdown menu showing 'PingSweep Module'.
- Layer 2 Protocols:** A section with two checkboxes: 'CDP Module' and 'LLDP Module', both of which are checked.
- Advanced Protocols:** A section with four checkboxes: 'Routing Table', 'Address Resolution Protocol', 'Border Gateway Protocol', and 'OSPF', all of which are checked.
- Filters:** A dropdown menu showing 'IP Filter'.
- Advanced Filters:** A section with three checkboxes: 'System Location Filter', 'System Object ID Filter', and 'DNS Filter', all of which are checked.

At the bottom of the dialog box, there are three buttons: 'Save', 'Run Now', and 'Cancel'.

Create A New Discovery Profile

When we create the discovery profile, we are telling Cisco Prime Infrastructure which protocols we want to use from the ones mentioned above to discover the network. Each of them has its own pros and cons, but it's definitely necessary to have them all available at our discretion. Discovery can be easily accessed from the Getting Started Wizard when you log in for the first time or by navigating to **Operate > Discovery** (under Device Work Center). There are two options here: Quick Discovery and Discovery Settings. Quick Discovery allows you mainly to ping sweep your network followed by SNMP polling to get more details on the devices.

If you are planning to configure the discovery correctly the first time and reuse your configuration, start by clicking **Discovery Settings**. Now click **New** in the discovery settings modal pop-up. A window (as shown on left) will pop-up, where you can configure all the discovery settings will open. You will observe that the pop-up is broken down into three sections: Protocol Settings, Filters, Credential Settings, and Preferred Management IP (only 3 shown in figure above). You need to select at least one item from Protocol Settings, SNMP and Telnet/SSH from Credential Settings, and Preferred Management IP.

Start by giving the profile a suitable name. Depending on how many protocols you want to enable, start filling in the relevant information. Click on the “+” icon next to the Ping Sweep Module to open up more settings. You can add your subnets manually or use the Import CSV File button to import all your subnets from a simple CSV file. The CSV file needed for the import will have columns that correspond to the GUI, such as IP Address and Subnet Mask. Similarly you can fill in more protocols as well, but remember that the more protocols you add, the more time it will take to converge the discovery.

Seed Device	Hop Count
<input checked="" type="radio"/> 10.1.2.1	

TIP: If the majority of your devices are Cisco, or if LLDP is enabled on Cisco/non-Cisco devices, then using LLDP will converge the discovery faster. If the network has a mixture of multivendor network devices, ping sweep should help. Ping sweep will also help with doing a directed discovery, for example, on a 10.1.1.0 /24 network.

TIP: If Cisco Discovery Protocol information is desired in the Device Work Center, Cisco Discovery Protocol can be enabled in the discovery. It is not mandatory.

Configuring Cisco Discovery Protocol/LLDP

Configuring Cisco Discovery Protocol and LLDP are very similar in nature. The first check box enables the use of LLDP in the discovery. The second check box enables jumping the router (or Layer 3) boundaries. Cisco Discovery Protocol is a Layer 2 protocol, and if we want the discovery to continue all the way until there are no neighbors available, we need to use this option. Unlike ping sweep, the seed device for a Cisco Discovery Protocol/LLDP discovery is a single device from which the discovery should initiate. If the hop count is left blank, discovery will continue until end of CDP/LLDP neighbor is reached. You can add your subnets manually or use the Import CSV File button to import all of your Cisco Discovery Protocol/LLDP seeds from a simple CSV file. The CSV file needed for the import will have columns that correspond to the GUI, such as Seed Device IP Address and Hop Count.

Other protocols are very similar in nature. Some require the hop counts, while others like Border Gateway Protocol (BGP) and OSFP don't require hop counts.

Filtering

If you want to discover all of the subnets but would like to have a way to import information on certain devices based on their IP address, system location, type of device, or DNS, you can use filters to do just that.

TIP: If you are running discovery for the first time, pick a smaller range or hop count to begin with. Do not use filters in this discovery. Once the results are what you expect, go back and edit that profile to add filters as needed.

Credentials

Credentials are also an important part of the discovery. Please refer to the credential matrix from the Protocol Check section and enter the credentials appropriately. If this is not done, devices in the Device Work Center will error out with "Managing with Credential Errors." You can configure multiple community strings for the same network. This really helps to manage multiple devices without having to worry about which community is configured on what device.

The screenshot shows the 'Credential Settings' dialog box with the 'SnmpV2 Credential' tab selected. The 'Enable SnmpV2 Credential' checkbox is checked. Below it are 'Edit', 'Delete', and 'Add Row' buttons. A table with two columns, 'IP' and 'Read Commu...', contains one row with the IP '10.1.2.*' and a masked community string '*****'. At the bottom are 'Save' and 'Cancel' buttons.

For example, in the figure above, you could add another SNMP string for the 10.1.2.* network in addition to the one already configured.

The screenshot shows the 'Credential Settings' dialog box with the 'Telnet Credential' tab selected. The 'Enable Telnet Credential' checkbox is checked. Below it are 'Edit', 'Delete', and 'Add Row' buttons. A table with four columns: 'IP', 'User Name', 'Password', and 'Enable Passw...', contains one row with the IP '10.1.2.*', masked user '*****', masked password '*****', and masked enable password '*****'. At the bottom are 'Save' and 'Cancel' buttons.

The last thing to configure before we run discovery is the preferred management IP. Once the devices are discovered and added to the inventory, how do you want to manage them? Do you want to see the device list with DNS, loopback IP, or local hostname configured on the devices (aka sysName)? If DNS is not used on your network devices, go ahead and select sysName. If devices have a specific management VLAN and all the devices have loopback configured for that, it would be a good idea to use that. DNS is my last choice as the device names become very long and it clutters up the device selector.

Discover the Network

With Cisco Prime Infrastructure, you can now discover the wired and wireless network in just one discovery. When the discovery profile is saved, select the discovery profile and click the Run Now button as shown in the figure on the left. The results will be displayed on the same page as the discovery settings. You can refresh the job and watch the status of the discovery in real time.

Discovery Settings		
<input type="button" value="Run Now"/> <input type="button" value="Schedule"/> <input type="button" value="New"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/>		
Name	Date Created	Date Modified
<input type="radio"/> Lab1	2012-Aug-21 21:17:07	2012-Aug-21 21:17:07
<input checked="" type="radio"/> test1	2012-Sep-04 21:22:14	2012-Sep-05 09:20:04

Scheduling Ongoing Discovery

In addition to running discovery in real time, you can schedule discovery to run when you want it. Select the discovery profile name and click Schedule instead of Run Now. You will get a modal pop-up that looks like the figure on the right. Scheduling is extremely flexible in Cisco Prime Infrastructure. You can run every **x** minutes to **y** years.

Schedule Discovery

Job Name

My_Scheduled_Discovery

Start Time

☐ Now
☒ Date

09/12/2012 11:26 AM

(MM/dd/yyyy hh:mm AM/PM)

Recurrence

☐ None
☐ Minute
☐ Hourly
☒ Daily
☐ Weekly
☐ Monthly
☐ Yearly

Settings

Every 1 week(s)

☐ Sunday
☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday

End Time

☒ No End Date/Time
☐ Every 1 Times
☐ End at 09/12/2012 11:26 AM

(MM/dd/yyyy hh:mm AM/PM)

Validate Discovery

Now that we have discovered our wired/wireless network, how can we make sure we are archiving the entire inventory, configuration, and other relevant information? We can start with inventory, as that is where we will know whether Cisco Prime Infrastructure was having issues fetching inventory or configuration information.

Device Work Center

Navigate to **Operate > Device Work Center** to see the entire inventory that has been discovered. The left pane allows you to filter on devices based on the device types or user-defined group that we can create. The top portion of the Device Work Center allows you to see quick information on the device as shown in the figure above. Once you click the device's name, the bottom pane is populated with more detailed information. Tabs in the bottom pane can be changed to quickly access focused, detailed information as seen in the image below.

Device Group

Switches and Hubs

Cisco Catalyst 2960 Series

Cisco Catalyst 3500 Series

Cisco Catalyst 3560 Series

Cisco Catalyst 3560-E Series

Cisco Catalyst 3750 Series

Cisco Catalyst 4500 Series

Cisco Catalyst 4500-X Series

Device Group > Device Type > Switches and Hubs > Cisco Catalyst 3750 Series Switches

Cisco Catalyst 3750 Series Switches

Edit

Delete

Sync

Groups & Sites

Add Device

Bulk Import

Selected 1 | Total 10

Show All

Device Name	Reachability	IP Address	Device Type	Collection Status	Collection Detail	Collection Time	Software Version
LA-3750-SBR	Reachable	10.2.10.1	Cisco 3750 St...	Managed	Collection Status : G	September 12, 2...	12.2(58)SE1
LOH-3750-SBR	Reachable	10.11.10.3	Cisco 3750 St...	Managed	Collection Status : F	September 12, 2...	12.2(53)SE2
NY-3750-SBR.cis...	Reachable	10.4.10.1	Cisco 3750 St...	Managed with War...	Collection Status : F	September 12, 2...	12.2(58)SE1
RTP-3750-SBR	Reachable	10.1.10.1	Cisco 3750 St...	Managed	Collection Status : G	September 12, 2...	12.2(58)SE1
SF-3750-SBR	Reachable	10.3.10.1	Cisco 3750 St...	Managed	Collection Status : G	September 12, 2...	12.2(53)SE2
SIN-3750-SBR	Reachable	10.6.10.1	Cisco 3750 St...	Managed	Collection Status : G	September 12, 2...	15.0(1)SE

Device Details

Configuration

Configuration Archive

Image

Startup/Running Mismatch: Yes

Schedule Rollback

Schedule Archive

Schedule Override

Selected 0 | Total 5

Show All

Date	Created By	Description	Out of band
August 28, 2012 4:24:53 PM PDT	Syslog	Archived by syslog	Yes
August 28, 2012 3:29:24 PM PDT	Syslog	Archived by syslog	Yes
August 28, 2012 3:03:39 PM PDT	Syslog	Archived by syslog	Yes
August 28, 2012 2:40:55 PM PDT	Syslog	Archived by syslog	Yes
August 22, 2012 10:37:39 AM PDT	Inventory	Initial version	

Fixing Credential Errors

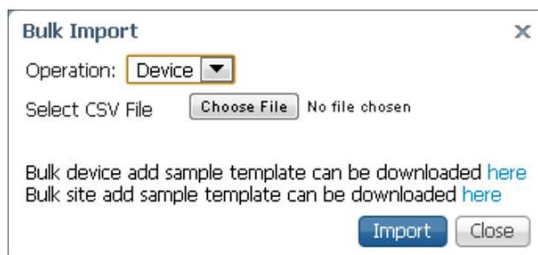
Most often you will find a few devices that don't have the SNMP strings or the CLI access that you thought they would have. You can either streamline or change the information on the devices, or if you have another set of credentials for a different subnet, you could add that to the CLI section of the discovery profile and rerun the

discovery. If you have a handful of changes, you can click the devices with a status of Managed with Warning and then click the Edit button to modify the credentials.

This version of Cisco Prime Infrastructure 1.3 does not have the capability of exporting the device list with credentials from the web interface, but this facility will be added in next release. At that point in time, you can export the device credentials, change them using a spreadsheet application, and import them back.

Importing Devices Manually

If you maintain a spreadsheet that has all the devices and would rather get started with that, you do have this option in Cisco Prime Infrastructure 1.3. If you go to **Operate > Device Work Center > Bulk Import**, you get an import pop-up as shown in the figure below.

A screenshot of the 'Bulk Import' dialog box in Cisco Prime Infrastructure. The dialog has a title bar with 'Bulk Import' and a close button (X). Inside, there is a label 'Operation:' followed by a dropdown menu showing 'Device'. Below that is a label 'Select CSV File' followed by a 'Choose File' button and the text 'No file chosen'. At the bottom, there are two lines of text: 'Bulk device add sample template can be downloaded [here](#)' and 'Bulk site add sample template can be downloaded [here](#)'. At the very bottom are 'Import' and 'Close' buttons.

TIP: Export the device template using the first “here” link. Use the exported CSV file to populate the device information. This will make sure your import goes through successfully.

Automating Branch Device Deployment

If you have a need to deploy devices in branches from time to time, automated branch deployment can really ease your Day-0 task by empowering you with zero-touch deployment. This is another way of automatically adding devices in Cisco Prime Infrastructure. We will talk about this method in detail in “Advance Configuration Topics.”

Deploying Wireless and Advanced Instrumentation

Cisco Prime Infrastructure can really simplify the dreaded task of deploying advance instrumentation like Application Visibility and Control (AVC), NetFlow, Next Generation Network Based Application Recognition (NBAR2), and much more. Cisco Prime Infrastructure uses converged configuration templates to achieve this task. This section will focus on instrumentation that will help visualize some of the common challenges in managing application responses within a corporation.

Deploy a WLAN Using a Configuration Template

Configuration groups are an easy way to group controllers logically. This feature provides a way to manage controllers with similar configurations. Templates can be extracted from existing controllers to provision new controllers or existing controllers with additional configuration parameters. Configuration groups can also be used to schedule configuration sets from being provisioned. Controller reboots can also be scheduled or cascaded depending on operational requirements. Mobility groups, dynamic channel assignment (DCA), and controller configuration auditing can also be managed using configuration groups.

Config Group Detail : 'Test-Config-Group'

Configure > Controller Config Groups > Config Group Detail

General **Controllers** Country/DCA Templates Apply/Schedule Audit Reboot Report

All Controllers				Group Controllers	
IP Address	Name	Config Group	Mobility Group Name	IP Address	Name
192.168.136.4	WLC-4400-1	none	eset		
192.168.136.4	SJ-WISM2-1	none	mobile-1		
192.168.136.4	WLC-2100-1	none	eset		
192.168.152.11	AMS-2504-WLC	none	AMS		

>>>
 (Add)
 <<<
 (Remove)

Save Selection Cancel

Configuration groups are used when grouping sites together for easier management (mobility groups, DCA, and regulatory domain settings) and for scheduling remote configuration changes. Configuration groups can be accessed from **Design > Wireless Configuration** (under Configuration) > **Controller Config Groups**.

- Adding controllers: Controllers in WCS are presented and can be moved over to the new configuration group.
- Applying templates: Discovered or already present templates can then be applied to the controller.
- Auditing: Make sure that template-based audit is selected in the audit settings and then audit the controllers in the group to make sure that they comply with policies.

NetFlow

NetFlow is an embedded instrumentation within Cisco IOS Software to characterize network operation. Visibility into the network is an indispensable tool for IT professionals. NetFlow gives network managers a detailed view of application flows on the network. Cisco Prime Infrastructure supports Traditional NetFlow (TNF) as well as Flexible NetFlow (FNF). A summarized view of what versions of NetFlow exist, their support, and their implied usage in Cisco Prime Infrastructure can be seen in the following two tables.

Flow Record Type	NetFlow Version	Cisco Prime Infrastructure Support	Template to Use	Technologies Used By
Traditional NetFlow (TNF)	Cisco (v5)	Cisco Prime Infrastructure 1.3	There is no template for this, but one can be created.	<ul style="list-style-type: none"> • Network traffic stats
Flexible NetFlow (FNF)	RFC 3954 (v9)	Cisco Prime Infrastructure 1.3	Collecting Traffic Statistics under OOTB (Out of the box) Folder	<ul style="list-style-type: none"> • PerfMon • Performance Agent (PA)
IPFix	RFC 5101 RFC 5102	Cisco Prime Infrastructure 2.0	Not available yet.	IPFix is a protocol developed by the IETF working group. The IETF Working group used NetFlow v9 as the basis for IPFix.

The following table shows further breakdown of NetFlow, and how NetFlow data is used for application visibility.

Features	Description	Export Format Support	Template to Be Used	Suggested Use
TNF	Basic NetFlow records	Version 5	Custom template needs to be created	Old platform that does not support Flexible NetFlow or IPFIX yet.
FNF	Flexible, extensible flow records. Report application from NBAR2.	Version 9 (IPFIX)	Traffic Statistics under OOTB Folder	<ul style="list-style-type: none"> For newer platforms such as <ul style="list-style-type: none"> ISR G2 ASR 1000 Report application visibility
PA	Application Response Time (ART)	Version 9 (IPFIX)	Need to develop	<ul style="list-style-type: none"> ART Transaction time Per application latency Response time (Available only on ISR G2)
PerfMon	Media Performance	Version 9 (IPFIX)	PerfMon template under OOTB Folder	<ul style="list-style-type: none"> Voice/video performance Jitter Packet loss

Using Configuration Templates to Enable NetFlow

Deploying TNF is relatively simple, but FNF can be challenging. Cisco Prime Infrastructure greatly simplifies managing NetFlow end to end. You can follow the design, deploy, operate, report model for NetFlow as well. You can design the NetFlow template by going to **Design > Configuration Templates > My Templates > OOTB > Collecting Traffic Statistics**. This will open the NetFlow v9 templates as shown in the figure above. You can fill in all the meta-data at the top of the template and save as a new template. The next step is to publish the template so that it becomes available for other members to deploy the template. Note that the default port for NetFlow for Cisco Prime Infrastructure 1.3 is 9991 and cannot be changed in this release.

TIP: [Samplicator](#) (Not tested nor supported by TAC) may be used to point all devices to send NetFlow to one place. Samplicator can then fork out NetFlow data to multiple Cisco Prime Infrastructure instances as desired.

Now that the template is published, the next task is to deploy the template so that we can configure devices to start sending NetFlow data to Cisco Prime Infrastructure. Go to **Deploy > Configuration Templates**, find **Collecting Traffic Statistics** in the list, and click **Deploy**. You will see the Template Deployment modal pop-up window (see figure below). Select the device or devices, fill in the values, and click **Apply** to accept the changes. You can fill in values for each device or you can use the export to/import from a spreadsheet option for quick data entry. Click the CLI Properties to see the CLI that is generated from the values provided. Finally, schedule your job to enable NetFlow on the devices.

Template Deployment- Prepare and schedule

Switches and Hubs

- Cisco Catalyst 4500 Series Swi Cisco Catalyst 4500 Series Switches
- Cisco Catalyst 3500 Series XL Cisco Catalyst 3500 Series XL Switches
- Cisco Catalyst 6500 Series Swi Cisco Catalyst 6500 Series Switches
- Cisco Catalyst 3750 Series Swi Cisco Catalyst 3750 Series Switches
- FL4-3750S-1 FL4-3750S-1 Switches and Hubs 10.15.10.1 Cisco

Value Assignment

Devices

Name

3750-PHY-1

Feature

CLI Preview

*Flow Exporter Name LONDON-BR

*IP Address 10.1.2.3

*Flow Exporter Port 9991

*Flow Monitor Name LON-MONITOR

*Interface GI1/0

Apply

Schedule

OK Cancel

Check Whether NetFlow Data Are Coming or Not

We have now enabled NetFlow on the devices, but how do we know whether or not Cisco Prime Infrastructure is receiving it? A quick way to tell is to go to **Design > Monitoring Templates** and see if there are multiple NetFlow instances for each unique NetFlow template. Normally you will see a template (as shown on below) as Flexible_NetFlow-nnnnnnnn (where nnnnnnnn is the random number mapped per template). Once you click that template, the right pane will show template details. The bottommost portion (see figure below), Exporting Devices, should tell us which device is using/sending the NetFlow for that template. The middle portion of the same template shows all the attributes sent in that template. You may also run a report by choosing **Report > Report Launch Pad > Raw NetFlow Reports** and selecting the same NetFlow template. Click **New** to generate a new report. Specify all the details and run the report to see if you are really getting any data from this device based on what was configured. All NetFlow-pertinent dashlets will also start populating automatically.

Exporting Devices

Template Parameters

Show All

Template ID	Device IP Address	Site
257	10.0.103.2	San Francisco Branch

Raw NetFlow

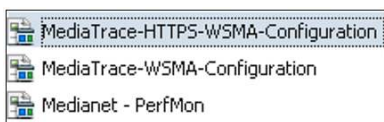
Netflow 25031097
Netflow 25037274
Netflow 25139001
Netflow 25468349
Netflow 25524022
Netflow 25814149
Netflow V1
Netflow V5
Netflow V7

Medianet


The Cisco architecture for medianet is an end-to-end IP architecture that enables pervasive and quality rich-media experiences. Medianet combines a smarter network to smarter endpoints with medianet technology embedded into network elements and endpoints. Cisco Prime Infrastructure simplifies the whole lifecycle for medianet from enablement to reporting.

Enabling Medianet

Enabling medianet does require using the CLI to configure some devices that support medianet. Cisco Prime Infrastructure has predefined templates for enabling medianet. Just as we enabled NetFlow, we can do the same thing for medianet. Navigate to **Design > Configuration Templates > My Templates > OOTB**. You will see three templates for medianet, as shown in the figure below.



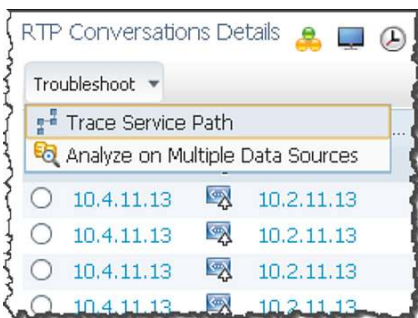
The only difference is that the first one uses HTTPS, while the second one uses regular HTTP. The last one is for enabling medianet PerfMon, which allows you to see the traffic that is flowing through a given interface. The steps for deploying the template remain the same as with any other CLI template. Note that the first two templates for enabling medianet do not have any variables.

 **TIP:** Make sure that a user is defined in the device with privilege level 15 for the Web Services Management Agent (WSMA) to work.

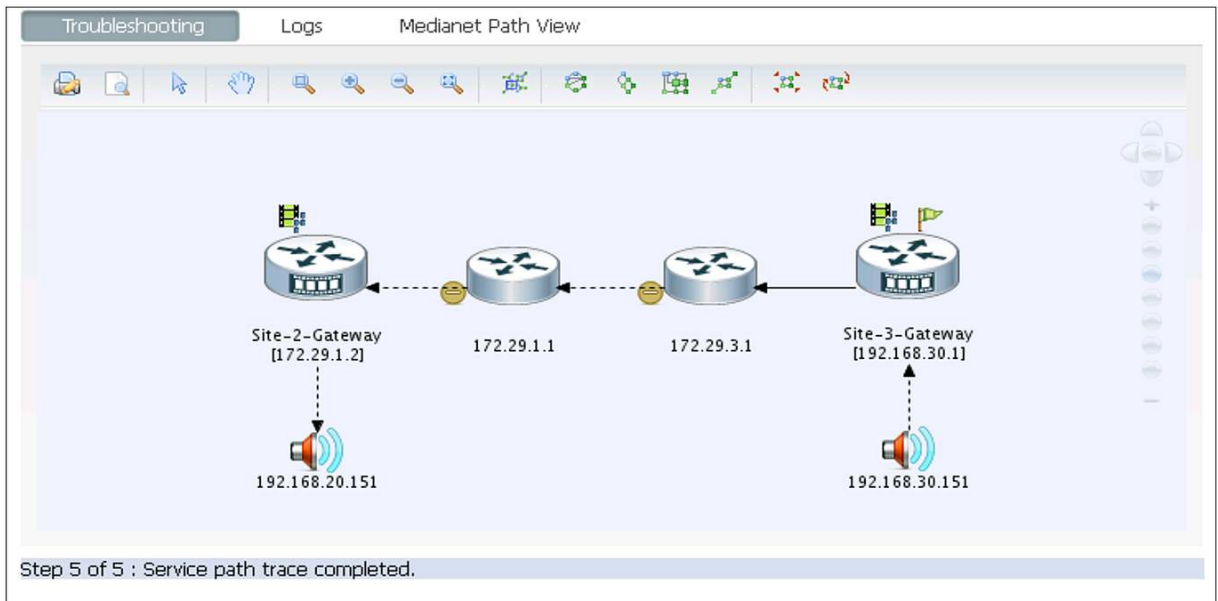
Check Whether Medianet Is Enabled

Once medianet is turned on, there are a few commands that can be executed on the CLI to see whether the devices can show the medianet data. Here are a few commands you can use on the devices:

```
show mediatrace session statistics
show mediatrace session data
```



Please refer to the [Troubleshooting Guide](#) for details on how to make sure medianet is properly operational. Once medianet is verified to be working, we can see the RTP conversation (see figure below) details dashlets showing sessions.



For troubleshooting, simply choose **Troubleshoot > Trace Service Path** in the same dashlet. This will launch another window where Mediatrace can be visually seen as figure above.

To see the active calls navigate to **Operations > Path Trace** under Operational Tools. You can then select the audio or video calls with jitter/packet loss for troubleshooting as shown in the figure below.

Application: RTP

RTP Streams

Trace Service Path Analyze Path Specify Session for Path Trace

Type	Source			Destination			Jitter (ms)	Packet Loss %	MOS
	IP Address	Site	User ID	IP Address	Site	User ID			
▶	10.15.11.10		Unknown	192.168.138...		Unknown	1.66	0	4.38
▶	10.3.11.42		Unknown	10.4.11.100		Unknown	846.3	5.53	0
▶	10.4.11.13		Unknown	10.2.11.13		Unknown	932.3	0	0
▶	10.3.11.41		Unknown	10.9.11.12		Unknown	0	0	0
▶	192.168.138...		Unknown	192.168.152...		ifields	2.19	0	0

Monitoring/Troubleshooting

Basic Monitoring

Cisco Prime Infrastructure provides a very easy and flexible model for monitoring your wired/wireless network. Cisco Prime Infrastructure allows you to define or “design” monitoring templates that dictate how and what you want to monitor. You can then turn on monitoring by deploying the monitoring template. The results are then shown in the form of dashboards, dashlets, and reports.

Basic Device Health

The Basic Device Health feature is turned on by default for all devices. This includes device monitoring of availability, CPU, memory, buffers, and environment. Basic Device Health is polled every 5 minutes by default, but you can customize this as well. The template is called Device Health - choose **Design > Monitoring Configuration > Features > Metrics > Device Health**. The parameters can be changed by clicking the polling value for that row as shown in the following figure.

<input type="checkbox"/> * Parameter	Description	Polling Frequency
<input type="checkbox"/> device availability	Device Availability	5 min
<input type="checkbox"/> cpuUtilization	CPU utilization	1 min
<input type="checkbox"/> memoryPoolUtilization	Memory Pool Utilization	5 min
<input type="checkbox"/> bufferMissPercent	Buffer Miss Percentage	15 min
<input type="checkbox"/> largestFreeBufferPercent	Largest Free Buffer Percentage	30 min
<input type="checkbox"/> envTemperature	Current Temperature in degrees Celsius	1 hour
		6 hour
		12 hour

TIP: Don't forget to save the template after making the changes. The template will need to be republished and redeployed if changes are made.

Interface Statistics

Interface Statistics are **not** enabled by default, as monitoring interfaces can get very tricky if not done correctly. Some business-critical device interfaces should be polled more often than others, so there is no one size fits all, when it comes to monitoring interfaces. Interface polling can be very quickly enabled by using a predefined monitoring template. You can navigate to **Design > Monitoring Configuration > Features > Metrics > Interface Health** (shown below). Follow the same methodology to change the polling interval as mentioned for Device Health. You can see how interface availability is changed to every minute.

<input type="checkbox"/> * Parameter	Description	Polling Frequency
<input type="checkbox"/> Interface Availability	Interface Availability	1 min
<input type="checkbox"/> ifInErrors	ifInErrors	5 min
<input type="checkbox"/> ifOutErrors	ifOutErrors	5 min
<input type="checkbox"/> ifInDiscards	ifInDiscards	5 min

Design Custom Monitoring Templates

Flexible monitoring templates enable users to customize how they monitor their network. You can create your own templates by navigating to **Design > Custom SNMP Templates** and selecting the MIB and the table as shown in figure on left. You can then see all the variables from the table. Select the ones you are interested in, and they will be now available for polling. If the MIB you are interested in is not available in the drop-down list, you can upload a new MIB by clicking Upload MIB on the same page. Once you save the page after selecting the object identifiers (OIDs), you should see a template created as shown in the figure below.

Custom SNMP Templates

Basic
Advanced

Name: 64BitQoS
MIB's: CISCO-CLASS-BASED-QOS-MIB
Table's: cbQosCMStatsTable

☐ cbQosCMPrePolicyPktOverflow
☐ cbQosCMPrePolicyByte
☐ cbQosCMPostPolicyByte
☐ cbQosCMDropPkt
☒ cbQosCMDropByte64
☐ cbQosCMNoBufDropPkt64

☐ cbQosCMPrePolicyPkt
☐ cbQosCMPrePolicyByte64
☒ cbQosCMPostPolicyByte64
☐ cbQosCMDropPkt64
☐ cbQosCMDropBitRate

☒ cbQosCMPrePolicyPkt64
☐ cbQosCMPrePolicyBitRate
☐ cbQosCMPostPolicyBitRate
☐ cbQosCMDropByteOverflow
☐ cbQosCMNoBufDropPktOverflow

☐ cbQosCMPrePolicyByteOverflow
☐ cbQosCMPostPolicyByteOverflow
☐ cbQosCMDropPktOverflow
☐ cbQosCMDropByte
☐ cbQosCMNoBufDropPkt

You can now create a poller from this template. If you now change the metadata and save this template, it will become a deployable monitoring poller and will be visible under My Templates. You are now ready to deploy the template to get monitoring started.

* Parameter	Description
cbQosCMDropByte64	
cbQosCMPPostPolicyByte64	
cbQosCMPPrePolicyPkt64	

Deploy Custom Monitoring Templates

In order to deploy the monitoring template just created, you can navigate to **Deploy > Monitoring Deployment > My Templates**. The default view in Cisco Prime Infrastructure 1.3 is Tasklet view. Change that to Table view to see how many devices are being polled using the template in question. Now locate your template, select it, and click **Deploy**. You will see a modal pop-up list as shown in the figure at the left. You can either select a device or devices or you can select the Device Groups option to select predefined or user-defined groups or even sites, as shown in the figure at left. Choose the appropriate group, and click **Submit**. Once back in Table view, you can see that devices are now assigned to the poller we chose in the previous step. This means that Cisco Prime Infrastructure will now be polling the devices based on what was designed in the template.

Name	Description
<input type="checkbox"/> Third Party Device	Third Party Device
<input type="checkbox"/> Cisco UCS Series	Cisco UCS Series
<input type="checkbox"/> Cisco Interfaces and Modules	Cisco Interfaces and Modules
<input type="checkbox"/> Third Party Access Point	Third Party Access Point
<input type="checkbox"/> Site Groups	Site Groups
<input type="checkbox"/> Los Angeles Branch	This is a site group
<input type="checkbox"/> System Campus	This is a site group
<input type="checkbox"/> San Francisco Branch	This is a site group
<input type="checkbox"/> San Jose Data Center	This is a site group
<input type="checkbox"/> Amsterdam Branch	This is a site group

Data Collection from NAM

In order for Cisco Prime Infrastructure to manage Network Analysis Module, it needs to have a minimum software version of 5.1.1 plus the latest patches available. We can then make sure that Cisco Prime Infrastructure is enabled to poll the NAM data. You can navigate to **Administration > Data Sources**. The top portion of the same page shows all the devices that are actively sending NetFlow data to Cisco Prime Infrastructure. The bottom pane of the page shows all the NAMs that have been discovered or added to the inventory.

▼ NAM Data Collector				
<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
<input type="checkbox"/>	Name	Type	Host IP Address	Data Usage in System
<input type="checkbox"/>	ACC-NAM2204.cisco.com	Cisco NAM 2204 Appliance	192.168.136.67	Enabled
<input type="checkbox"/>	Campus-NAM3.eset-cisco.com	Cisco Catalyst 6500 Series Network Analysis Mod	192.168.136.129	Enabled
<input type="checkbox"/>	DC-NAM2220.cisco.com	Cisco NAM 2220 Appliance	192.168.136.32	Enabled
<input type="checkbox"/>	RTP-NAM-SRE.cisco.com	Cisco SM-SRE Network Analysis Module	192.168.136.131	Enabled

Select the NAM that should be polled by Cisco Prime Infrastructure, and click **Enable** as shown in the figure below.

▼ Device Data Sources				
				Show All
Data Source	Type	Exporting Device	Status	Last 5 min Flow Record Rate
10.0.111.2-32443	NETFLOW	10.0.111.2	<input checked="" type="checkbox"/> Up	1861
10.0.101.2-32442	NETFLOW	10.0.101.2	<input checked="" type="checkbox"/> Up	243
10.0.109.2-32582	NETFLOW	10.0.109.2	<input checked="" type="checkbox"/> Up	17

Turning on Advanced Monitoring

Cisco Prime Infrastructure consumes a lot of information from various different sources. Some of the sources for data include NAM, NetFlow, NBAR, medianet, PerfMon, and Performance Agent. The following table depicts the sources of the data for the site dashlets as used by Cisco Prime Assurance:

Dashlet Category	Dashlet Name	NAM	Medianet	NetFlow	PA	NBAR2
Site	Application Usage Summary	y	y	y	y	y
	Top N Application Groups	y	y	y	y	y
	Top N Applications	y	y	y	y	y
	Top N Applications with Most Alarms	y	y	y	y	y
	Top N Clients (In and Out)	y	y	y	y	y
	Top N VLANs	y		Y	Y	
	Worst N RTP Streams by Packet Loss	y	y			
	Worst N Clients by Transaction Time	y			y	

The following table shows how the application-specific dashlets get populated in Cisco Prime Assurance:


Dashlet Category	Dashlet Name	NAM	Medianet	NetFlow	PA	NBAR2
Application	Application Configuration	y	y	y	y	y
	Application ART Analysis	y			y	
	App Server Performance	y			y	
	Application Traffic Analysis	y	y		y	y
	Top N Clients (In and Out)	y			y	
	Worst N Clients by Transaction Time	y			y	
	Worst N Sites by Transaction Time	y			y	
	KPI Metric Comparison	y	y		y	
	DSCP Classification	y		y		
	Number of Clients Over Time	y		y		
	Top Application Traffic Over Time	y		y		

Dashlet Category	Dashlet Name	NAM	Medianet	NetFlow	PA	NBAR2
	Top N Applications	y		y	y	
	Top N Clients (In and Out)	y		y	y	
	Average Packet Loss	y	y			
	Client Conversations	y		y		
	Client Traffic	y		y		
	IP Traffic Classification	y		y		
	Top N Applications	y		y		
	DSCP Classification	y		y		
	RTP Conversations Details	y	y			
	Top N RTP Streams	y	y			
	Voice Call Statistics	y	y			
	Worst N RTP Streams by Jitters	y	y			
	Worst N RTP Streams by MOS	y				
	Worst N Sites by MOS	y				
	Worst N Site to Site Connections by KPI	y	y		y	

NetFlow

Once we have verified that NetFlow is enabled on devices and directed to Cisco Prime Infrastructure, we are now ready to turn on monitoring for NetFlow. Just as for Device and Interface Health, all it takes is provisioning the appropriate monitoring template and deploying it. You can start out by going to **Design > Monitoring Configuration > Features > Flexible NetFlow**, choosing the templates based on what was discussed in an earlier NetFlow section, filling out the appropriate details, and saving the template. The template will be instantiated with the new name as specified in the header under My Templates.

You can then navigate to **Deploy > Monitoring Deployment**. Look for the template you just created. In this case it's called "RTP-Branch-NetFlows". Looking at the figure on right, Templates with an orange ball with a right arrow are already deployed, and the templates with a green ball with a right arrow are the ones that are still not deployed. Once the template is deployed, dashlets should start populating the data after a couple of polling cycles.

RTP-Branch-Netflows	
Description	
Test for DG	
Deployed No	
Status Inactive	
Last Deployed	
Voice Video Data Metrics (de...	
Description	
Voice Video Data Metrics (default)	
Deployed Yes	
Status Active	
Last Deployed 2012-08-21 09:06PM PDT	
View Recent	

WAN Optimization - aka Cisco Wide Area Application Services

Cisco Wide Area Application Services (WAAS) devices and software help you to ensure high-quality WAN end-user experiences across applications at multiple sites. You can refer to the following URL

[http://wwwin.cisco.com/dss/adbu/waas/collateral/Using NAM in a WAAS Deployment.pdf](http://wwwin.cisco.com/dss/adbu/waas/collateral/Using_NAM_in_a_WAAS_Deployment.pdf) for various scenarios for deploying WAAS in your network.

Once you have deployed your WAAS changes at candidate sites, you can navigate to **Operate > WAN Optimization** to validate the return on your optimization investment. Cisco Prime Infrastructure also allows you to monitor WAAS-optimized WAN traffic by navigating to **Operate > WAN Optimization > Multi-Segment Analysis**. Click the **Conversations** tab to see individual client/server sessions, or the **Site to Site** tab to see aggregated site traffic. Some of the key dashlets to help with WAAS monitoring are detailed in the following table:

Dashlet	Description
Transaction Time (Client Experience)	Graphs average client transaction times (in milliseconds) for the past 24 hours, with separate lines for optimized traffic and pass-through traffic (in which optimization is turned off). With optimization enabled, you should see a drop in the optimized traffic time when compared to the pass-through time.
Average Concurrent Connections (Optimized versus Pass-through)	Graphs the average number of concurrent client and pass-through connections over a specified time period.
Traffic Volume and Compression Ratio	Graphs the bandwidth reduction ratio between the number of bytes before compression and the number of bytes after compression.
Multisegment Network Time (Client LAN-WAN - Server LAN)	Graphs the network time between the multiple segments.
Average and Maximum Transaction Time	The time between the client request and the final response packet from the server. Transaction time will vary with client uses and application types, as well as with network latency. Transaction time is a key indicator in monitoring client experiences and detecting application performance problems.
Average Client Network Time	The network time between a client and the local switch or router. In WAAS monitoring, client network time from a Wide Area Application Engine (WAE) client data source represents the network round-trip time (RTT) between the client and its edge WAE, while client network time from the WAE server data source represents the WAN RTT (between the edge and core WAEs).
Average WAN Network Time	The time across the WAN segment (between the edge routers at the client and server locations).
Average Server Network Time	The network time between a server and NAM probing point. In WAAS monitoring, server network time from a server data source represents the network time between the server and its core WAE.
Average Server Response Time	The average time it takes an application server to respond to a request. This is the time between the client request arriving at the server and the first response packet being returned by the server. Increases in the server response time usually indicate problems with application server resources, such as the CPU, memory, disk, or I/O.
Traffic Volume	The volume of bytes per second in each of the client, WAN, and server segments.
Average and Maximum Transaction Time	The time between the client request and the final response packet from the server. Transaction time will vary with client uses and application types, as well as with network latency. Transaction time is a key indicator in monitoring client experiences and detecting application performance problems.

Monitor/Troubleshoot a Wireless Network

RRM/Clean air

RF profiles and groups are supported in NCS version 1.1 for both RF profile creation templates and AP group templates. If you use NCS 1.1 to create the RF profiles through the creation of templates, this gives the administrator a simple way to create and apply templates consistently to groups of controllers. The process flow is the same as was previously discussed in the controller feature set with some minor but important differences.

The process is the same as previously discussed in that you first create RF profiles, and then you apply the profiles through the AP groups. There are differences in how this is done from NCS and in the use of templates for deployment across the network.

Build RF Profile

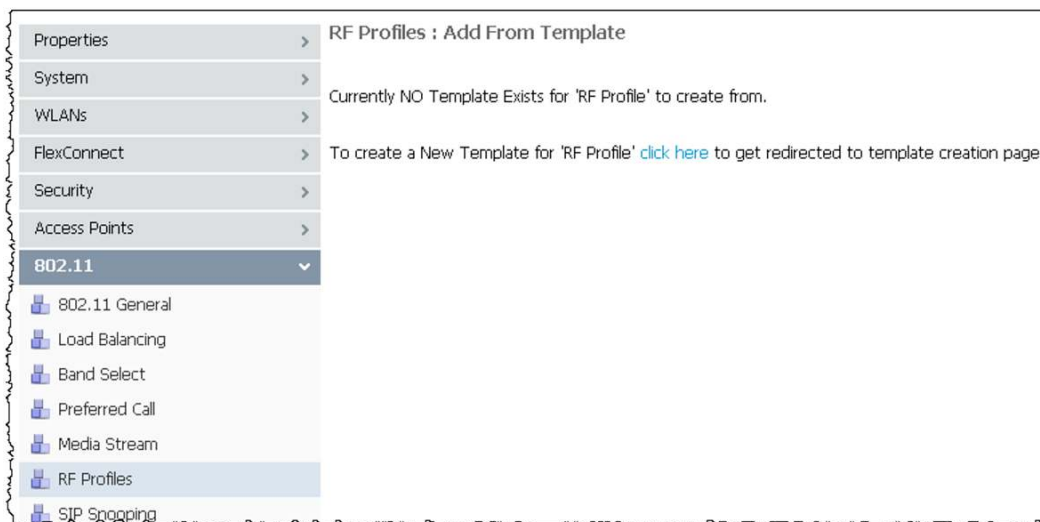
With Cisco Prime Infrastructure there are two ways that you can approach building or managing an RF profile. Choose **Configure > Controllers**, then click the IP address of the controller and choose **802.11 > RF Profiles** in order to access profiles for an individual controller.

Figure below displays all the RF profiles currently present on the chosen controller and allows you to make changes to profiles or AP group assignments. The same limitation as with the controller GUI is in effect in regard to a profile that is currently applied to an AP group. You have to disable the network or unassign the RF profile from the AP group.



When you create a new profile, Cisco Prime Infrastructure prompts you to choose an existing template. If this is the first time it is being accessed, you are directed to the Template Creation dialogue for an 802.11 controller template.

You may also navigate to **Configure > Controller Template Launch Pad > 802.11 > RF Profiles** (see figure below) in order to go to the controller template launch pad directly.



In both cases, a new RF profile is created in Cisco Prime Infrastructure through the use of a template. This is a preferred method, since it allows the administrator to use the workflow of Cisco Prime Infrastructure and apply templates and configurations to all or select groups of controllers and reduce configuration errors and mismatches.

Complete these steps:

1. In order to create an RF profile template, choose **Add Templates** from the pull-down menu at the top right of the screen as shown in the figure below.



2. Configuration of the template/settings is almost identical with the addition of a template name. Make this descriptive for easy recognition in the future. Change settings as needed or required and choose **Save** as seen in figure below.

Note: If you choose a threshold value for Transmit Power Control Version 2 (TPCv2) and it is not the chosen TPC algorithm for the RF group, then this value is ignored.

TIP: A simple setting to change for validation is the minimum TPC power. The minimum power can be raised if you choose a dBm value that is more than the current power level assigned by Radio Resource Management (RRM). This helps to validate the RF profiles operation.

3. Once you click **Save** the options at the bottom of the screen change as shown in the following figure:

Choose **Apply to Controllers** and the controller dialogue box appears to display the list of controllers managed by this NCS server as shown in the figure below.

4. From figure on right, Select **Save Config to Flash** box, then select the controller that you wish to have the profile available on, and click on **OK**.

IP Address	Controller Name
171.69.217.67	WCS-5508-sim1

5. You can see the controller template results as shown in figure below:

Controller Template 'BldgO-RF-Profile' > Template Results

Configure > Controller Template Launch Pad > 802.11 > RF Profiles > Controller Template 'BldgO-RF-Profile' > Template Results

IP Address	Controller Name	Operation Status	Reason
171.69.217.67	WCS-5508-sim1	Success	-

☐ View Save Config / Reboot Results

6. Now when you view the RF profiles screen, you can see the new template created as shown in figure below.

System > RF Profiles Controller Templates

Configure > Controller Template Launch Pad > 802.11 > RF Profiles

Template Name	Profile Name	Description	Radio Type	Applied To Controllers	Applied To Virtual Domains
BldgO-RF-Profile	BldgO-RF-Profile	Default 802.11a Template	802.11a	0	0

2012-Sep-27, 21:16:57 UTC

The previous steps can be repeated in order to create and apply additional templates as required, for example, for 802.11b.

Apply RF Profiles to AP Groups

As with the WLC configuration for RF profiles, newly created profiles can be applied to a controller through the use of AP groups they are assigned to. In order to do this, either a previously saved AP group VLANs template or a newly created template can be used.

Choose **Configure > Controller Template Launch Pad** and choose **AP Group** as shown in figure below.

System > Controller Template Launch Pad

Configure > Controller Template Launch Pad

System	General	New
SNMP Community	SNMP Community	New
Network Time Protocol	Network Time Protocol	New
User Roles	User Roles	New
AP Username Password	AP Username Password	New
AP 802.1X Supplicant Cr...	AP 802.1X Supplicant Credentials	New
Global CDP Configuration	Global CDP Configuration	New
DHCP	DHCP	New
Dynamic Interface	Dynamic Interface	New
Interface Groups	Interface Groups	New
QoS Profiles	QoS Profiles	
AP Timers	AP Timers	
Traffic Stream Metrics QoS	Traffic Stream Metrics QoS	
WLANs	WLAN Configuration	New
FlexConnect		
Security	AP Group	New

In order to create a new template, choose **New** and fill in the required information. See figure below.

System > New Controller Template
Configure > Controller Template Launch Pad > WLANs > AP Group > New Controller Template

WLANs > Name: PI_HQ_Deploy
Description (Optional):

WLAN Profiles RF Profiles Venue Group

Each AP Group can contain up to 16 WLAN Profiles.

WLAN Profile Name	Interface / Interface Group (G)	NAC Override	Edit
IFM	management	<input type="checkbox"/>	
Emulation	virtual	<input type="checkbox"/>	

Add Remove

Choose the **RF Profiles** tab in order to add RF profiles as shown in figure (below).

System > New Controller Template
Configure > Controller Template Launch Pad > WLANs > AP Group > New Controller Template

WLANs > Name: PI_HQ_Deploy
Description (Optional):

WLAN Profiles RF Profiles Venue Group

802.11a Radio BldgO-RF-Profile
802.11b/g Radio none

Create new RF profile.

In Cisco Prime Infrastructure 1.3, you can choose the **Venue Group** tab in order to add venue information as well. (See figure above)

System > New Controller Template
Configure > Controller Template Launch Pad > WLANs > AP Group > New Controller Template

WLANs > Name: PI_HQ_Deploy
Description (Optional):

WLAN Profiles RF Profiles Venue Group

Venue Config

Venue Group: Business
Venue Type: Bank

Operator Class

81	83	84	112	113	115	116	117	118
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
119	120	121	122	123	124	125	126	127
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Multiple Venue List

Multiple Venue List

Delete Add Row

Venue Language	Venue Name
<input checked="" type="checkbox"/> ENG	California

If you save the template, a warning message may appear. As stated in the previous message, the change of the interface that the assigned WLAN uses disrupts the VLAN mappings for FlexConnect APs applied in this group. Ensure that the interface is the same before you proceed.

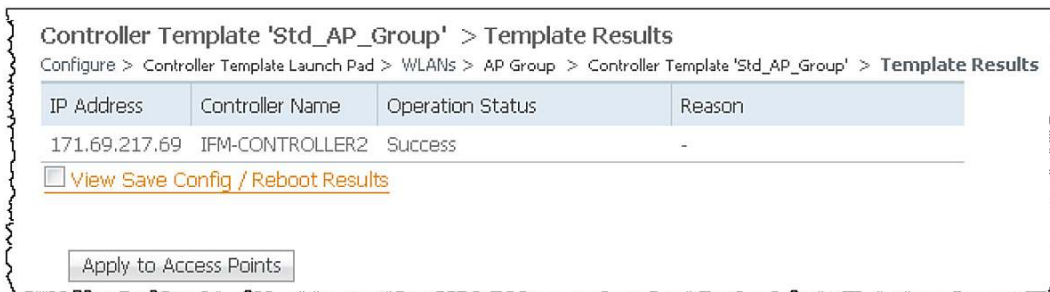
Once you choose OK, the dialogue is replaced with more options. Choose the **Apply to Controllers** option as shown in the following figure.



Choose the controllers to which the template needs to be applied as shown in figure below.



Cisco Prime Infrastructure responds with operational status (see figure below) on whether the template was successfully applied to the selected controllers.



If the template was not pushed successfully, NCS provides a message that states the reason for the failure. In this example, the RF profile that is applied to the group is not present on one of the controllers to which the template was applied.

Apply the RF profile again, specifically to that controller, and then reapply the AP group in order to generate a successful message.

Once the AP group has been deployed with the RF profiles applied (click the **Apply to Access Points** button), only access points attached to the controllers where the AP group was deployed successfully are available to select from.

Note: Until this point, no real changes were made to the RF infrastructure, but this changes when APs that contain new RF profiles are moved into the group. When an AP is moved into or out of an AP group, the AP reboots to reflect the new configuration.

Choose the APs you want to add to the AP group and choose OK. A warning message appears. NCS displays the status of the change.

Monitor/Troubleshoot Clients and Users

Client Visibility

In NCS 1.0, both wired and wireless monitoring and troubleshooting have been integrated with identity services. Integration between wired/wireless network management has been achieved through three network elements:

- Cisco Wireless LAN Controllers
- Cisco Catalyst® Switch security features: AAA, RADIUS, 802.1x and MAC authentication, MAC notification traps (nonidentity clients), syslog (identity clients only)
- Cisco Identity Services Engine (ISE)

All clients - wired and wireless - are displayed in the Clients and Users page (Monitor > Clients and Users).

Wired clients display AP name as N/A. Switch port information is provided in interfaces column as shown in figure below.

MAC Address	IP Address	IP Type	AP IP Address	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface
00:21:5c:01:b8:6f	192.168.152.38	Dual-Stack	192.168.152.14	jfields		Intel	AMS-2504-WLC	Root Area	13	Associated	vlan 13
00:26:b0:94:1b:6c	192.168.152.37	Dual-Stack	192.168.152.14	jfields		Apple	AMS-2504-WLC	Root Area	13	Associated	vlan 13
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	N/A	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6

Wireless Clients

In order to launch the client troubleshooting tool, click the button to the left of the client list item. Once the client is selected, click the Troubleshoot icon in the toolbar, as shown in the following figure:



The following window is displayed for the client:

Client Troubleshooting [Go back](#)

Properties

General

User Name: **cbala**

IP Address: **171.70.241.40**

MAC Address: **c8:b0:c8:df:4c:6a**

Vendor: **Apple**

Endpoint Type: **Unknown**

Client Type: **Regular**

Media Type: **Lightweight**

Mobility Status: **Local**

Hostname: **dhcp-171-70-241-40.cisco.com**

E2E: **Not Supported**

802.11u Capable: **No**

Session

Controller Name: **sjc14-wl-c2**

AP Name: **SJC14-418-AP4**

AP IP Address: **171.71.133.42**

AP Type: **Cisco AP**

AP Base Radio MAC: **64:d9:89:42:4c:40**

Anchor Controller: **Data Not Available**

802.11 State: **Associated**

Association ID: **43**

Port: **2**

Interface: **corp1**

SSID: **blizzard**

Profile Name: **blizzard**

Protocol: **802.11n(5GHz)**

VLAN ID: **260**

AP Mode: **local**

Data Switching: **Unknown**

Authentication: **Unknown**

Security

Security Policy Type: **WPA2**

EAP Type: **PEAP**

On Network: **Yes**

802.11 Authentication: **Open System**

Encryption Cipher: **CCMP (AES)**

SNMP NAC State: **Access**

Radius NAC State: **RUN**

AAA Override ACL Name: **none**

AAA Override ACL Applied Status: **N/A**

Redirect URL: **none**

ACL Name: **none**

ACL Applied Status: **N/A**

FlexConnect Local Authentication: **No**

Policy Manager State: **RUN**

Authenticating ISE: **Data Not Available**

Authorization Profile Name: **Data Not Available**

Posture Status: **Unknown**

TrustSec Security Group: **Data Not Available**

Windows AD Domain: **Data Not Available**

Troubleshoot

802.11 Association: **✓**

802.1X Authentication: **✓**

IP Address Assignment: **✓**

Successful Association: **✓**

Problem

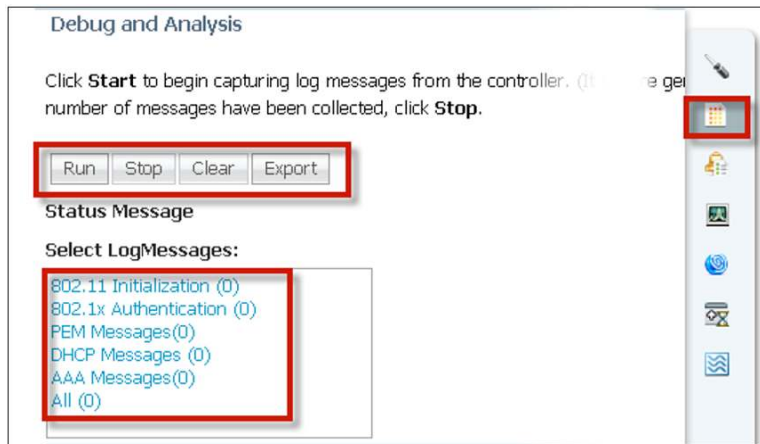
No issues found with client connectivity

Recommendation

No recommended actions

- Search Cisco Support Community
- Open or Update a service request

Log messages can be retrieved from the controller with the use of the Log Analysis tool, as shown in the following figure:



Refer to the [Policy Enforcement Module \(PEM\)](#) for more information on the PEM state.

The Event History tool provides users with event messages from clients and APs, as shown in the following figure:



Test Analysis Tool (CCXv5 Clients)

CCXv5 clients are client devices that support Cisco Compatible Extensions version 5 (CCXv5). You can now have troubleshooting capabilities for these clients in the Test Analysis section.

The screenshot shows the 'Client Troubleshooting' interface with a 'Test Analysis' section. It includes a list of diagnostic tests on the left, input fields for 'Input1' and 'Input2' in the center, and a table of test results on the right. The 'Start' button is highlighted with a red box.

Select	Diagnostic Test
<input type="checkbox"/>	DHCP
<input type="checkbox"/>	IP Connectivity
<input type="checkbox"/>	DNS Ping
<input type="checkbox"/>	DNS Resolution
<input type="checkbox"/>	802.11 Association
<input type="checkbox"/>	802.1x Authentication
<input type="checkbox"/>	Profile Redirect

Start Stop Frame

Input1

Name to resolve:

AP name:

Client Profile Number:

Input2

Profile:

Status	Results
Not initiated	None
Not initiated	None
Not initiated	None
Not initiated	None
Not initiated	None
Not initiated	None
Not initiated	None

Results

No results available.

Wired Clients

Cisco Prime Infrastructure 1.3 provides integrated management of wired and wireless devices/clients. Cisco Prime Infrastructure 1.3 also provides monitoring and troubleshooting for wired and wireless clients. SNMP is used to discover clients and collect client data. ISE is polled periodically to collect client statistics and other attributes to populate related dashboard components and reports.

If ISE is added to the systems and devices are authenticating to it, the Client Details page displays additional details labeled as Security within the Client Troubleshooting, as shown in the following figure:

The screenshot shows the 'Client Troubleshooting' interface with a 'Client Details' page. It includes a 'Properties' section on the left, a 'Session' section in the center, and a 'Security' section on the right. The 'Security' section is highlighted with a red box.

Client Troubleshooting Go back

Properties

General

User Name **jfields**

IP Address **192.168.152.37**

MAC Address **00:26:b0:94:1b:6c**

Vendor **Apple**

Endpoint Type **Apple-Device**

Client Type **Regular**

Media Type **Lightweight**

Mobility Status **Local**

Hostname **Data Not Available**

E2E **Not Supported**

802.11u Capable **No**

Session

Controller Name **AMS-2504-WLC**

AP Name **NMTG-AP3500-2**

AP IP Address **192.168.152.14**

AP Type **Cisco AP**

AP Base Radio MAC **04:c5:a4:f2:3f:60**

Anchor Controller **Data Not Available**

802.11 State **Associated**

Association ID **1**

Port **1**

Interface **vlan 13**

SSID **AMS-DOT1X**

Profile Name **AMS-dot1x**

Protocol **802.11g**

VLAN ID **13**

AP Mode **local**

Data Switching **Unknown**

Authentication **Unknown**

Security

Security Policy Type **WPA2**

EAP Type **PEAP**

On Network **Yes**

802.11 Authentication **Open System**

Encryption Cipher **CCMP (AES)**

SNMP NAC State **Access**

Radius NAC State **RUN**

AAA Override ACL Name **none**

AAA Override ACL Applied Status **N/A**

Redirect URL **none**

ACL Name **none**

ACL Applied Status **N/A**

FlexConnect Local Authentication **No**

Policy Manager State **RUN**

Authenticating ISE **eset-ise-1**

Authorization Profile Name **Default-Corporate-Policy**

Posture Status **Not Applicable**

TrustSec Security Group **Data Not Available**

Windows AD Domain **eset.cisco.com**

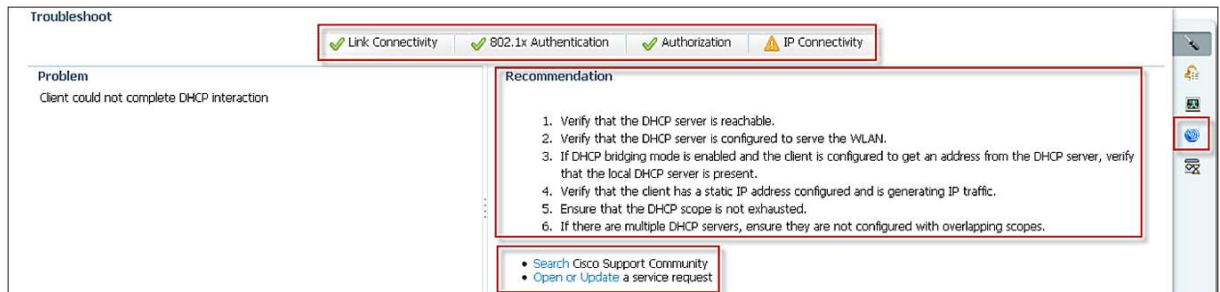
In order to navigate to **Operation > Clients and Users**, select a client, and click the Troubleshoot icon on the tools menu at the top of the page, as shown in the following figure:

The screenshot shows the 'Clients and Users' tools menu. It includes a 'Troubleshoot' icon (a wrench and screwdriver) which is highlighted with a red box, and other icons for 'Test', 'Disable', 'Remove', 'More', 'Track Clients', and 'Identify Unknown Users'.

Clients and Users

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

This takes the user to the page shown in the screen shot below. In this example, the client device has link connectivity, but failed IP connectivity.



On the right side of the screen, there is a tool bar with these items, all related to troubleshooting:

- Client Troubleshooting Tool
- Log Analysis
- Event History
- Context Aware History

Event History provides messages related to connectivity events for this client. In this example, the client failed to successfully authenticate. Date/time is provided to assist the network administrator in troubleshooting this client.

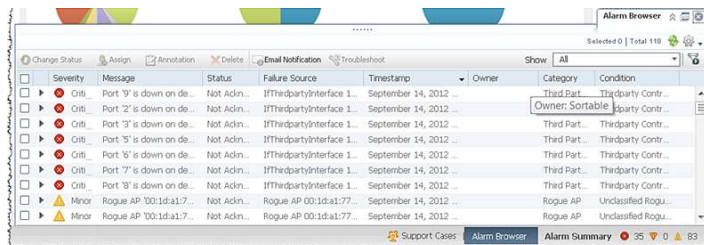
ISE provides authentication records to NCS through the REST API. Network administrators can choose a time period for retrieving authentication records from ISE. In the example in the following figure, the authentication record indicates that the user was not found in the ISE database.



Alarms and Events

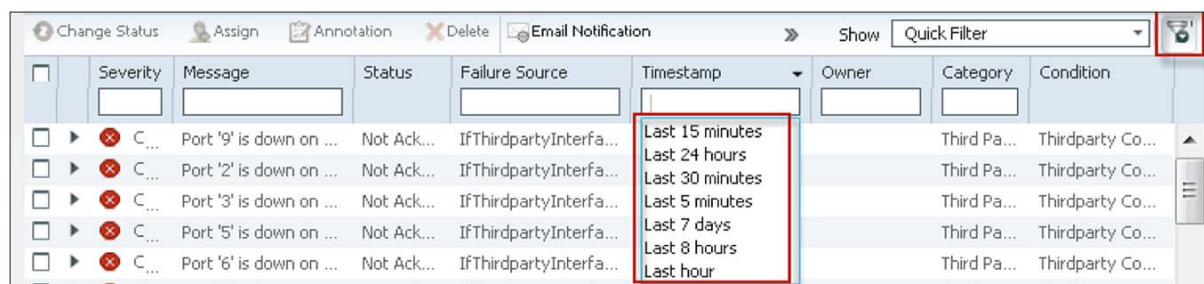
Alarms and events provide a single page view of all alarms and events for wired and wireless infrastructure. Persistent alarm summary and alarm browser are displayed at the bottom right of the screen (figure on right) regardless of what screen the user is on. Next to it is Alarm Browser view that shows all the alerts based on severity and device types as shown in the figure below.





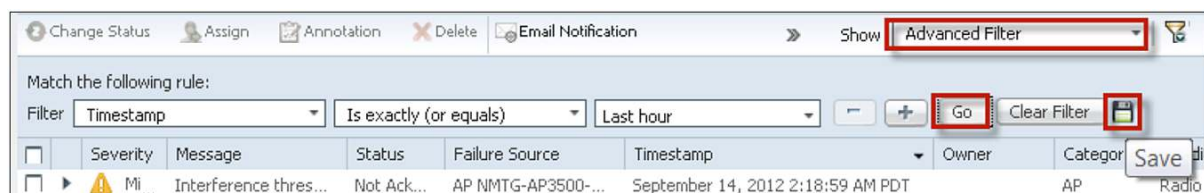
Quick Filter

Almost all of the tables in Cisco Prime Infrastructure have a quick filter widget. This quickly allows users to filter through the table, especially when there are many rows involved. This is very useful with alarms and events or clients and users. The following figure shows how quickly correct alarms can be filtered with this.



Advanced Filter

The Advanced Filter, as the name implies, allows user to filter on the content with complex rules. The following figure shows the Advanced Filter being used with more complex rules. These filters can be saved for one-click use the next time they are needed.

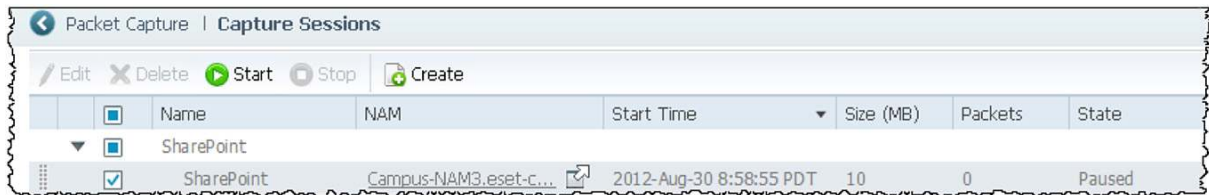


Trigger Packet Capture from Cisco Prime Infrastructure

Cisco Prime Infrastructure provides a very flexible solution for capturing packets throughout your network. You can either manually trigger a packet capture or automatically specify the capture based on some advanced parameters, so that it will be triggered once a threshold level is breached. In both of these solutions, packets can be captured locally on the NAM or they can be stitched from multiple NAMs and stored in Cisco Prime Infrastructure.

Manual Packet Capture from Cisco Prime Infrastructure

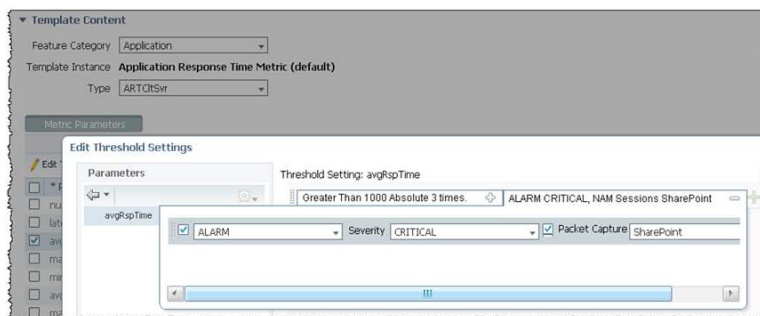
In order to do an ad hoc packet capture, you can navigate to **Operate > Packet Capture** (under Operational Tools) > **Capture Sessions**. If you are coming to this page for the first time, you may not have any capture profiles set up. In order to create a new profile, click **Create** and fill in all the criteria for capturing a particular traffic. If you have a need to capture a particular type of traffic all the time, it may a good idea to proactively create those profiles and test them out before automating them, as will be shown in the next section.



Once the profile is defined, you can test it out by clicking **Start**, as shown in the preceding figure. See if the packets are captured correctly. You can then use these profiles for automatically capturing packets.

Automating Packet Capture Using Cisco Prime Infrastructure

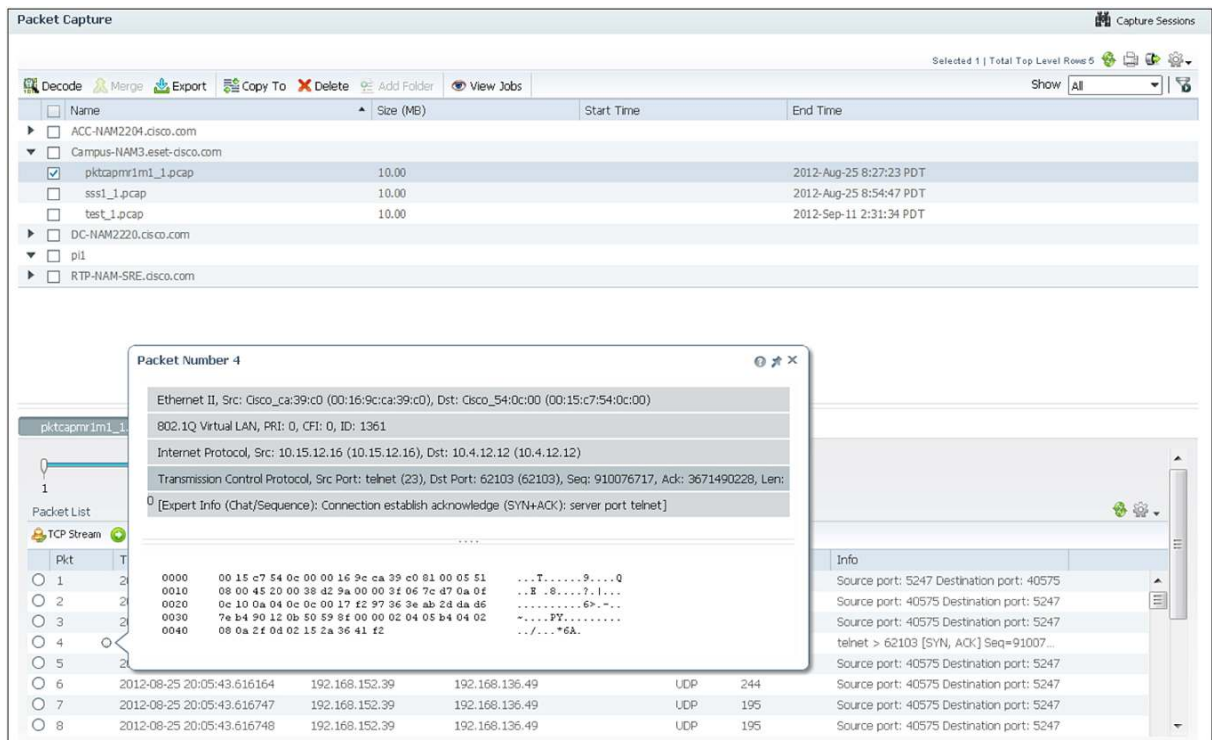
There are times when you want to capture packets based on a trigger. There is no way to find out ahead of time when the trigger will happen. For example, if you are trying to meet the SLA for AvgRespTime for an application, you may want to start the packet capture if the response time exceeds the predefined time. You can easily achieve this by combining threshold and packet capture in Cisco Prime Infrastructure. Navigate to **Design > Monitoring Configuration > Features > Thresholds**. When you click a threshold template, you can create a new instance from it. Besides the header information, you can select thresholds based on your interest from Traffic Analysis, Application, Voice/Video Signaling, Voice/Video Data, Interface Health, Device Health, and NAM Health. It would be a good idea to explore these options and see what types of trigger points each of them has. Once you select the category for capture, you can then select the subcategory. All the trigger points can then be seen. In order to change any of them, simply select that row and edit the threshold as shown in the image above. You can see (figure below) that we have chosen to alert and start capturing Sharepoint traffic if the AvgRespTime exceeds the default value.



Decoding Packet Capture Using Cisco Prime Infrastructure

Once the packets are captured, there are two options to decode the capture. The easiest way is to select the packet capture session and click Decode from the Packet Capture homepage (**Operate > Packet Capture**). The capture decode is shown in a pop-up window, which makes it extremely easy to evaluate each and every packet as shown in the figure below.

You could also click the Export button and the .pcap file will be downloaded directly on the client PC. This is useful if you need to perform advance troubleshooting on the capture decode. There is a dimmed Merge button between the Decode button and the Export button, which can be used to merge the .pcap files if more than one file is selected.



TIP: if the capture file is not very large (that is, not on the order of GB), it makes sense to decode it in Cisco Prime Infrastructure instead of jumping over to the NAM. Otherwise, you should use NAM instead of Cisco Prime Infrastructure for decoding very large capture files.

Miscellaneous Multi-NAM Capabilities Within Cisco Prime Infrastructure

Cisco Prime Infrastructure can serve as a central manager of managers (MoM) if multiple NAMs are deployed in the network. Some of the functionality that Cisco Prime Infrastructure can help with includes:

- Centralized monitoring of NAM Health
- Deploying configurations to multiple NAMs using the CLI configuration templates
- Upgrading NAMs using software image management capabilities
- Using one-click packet capture from multiple NAMs based on a capture policy
- Proactively capturing packets using threshold breaches

All of these allow users to use Cisco Prime Infrastructure to effectively manage the NAMs, thus making it a very good and stable data source for application visibility.

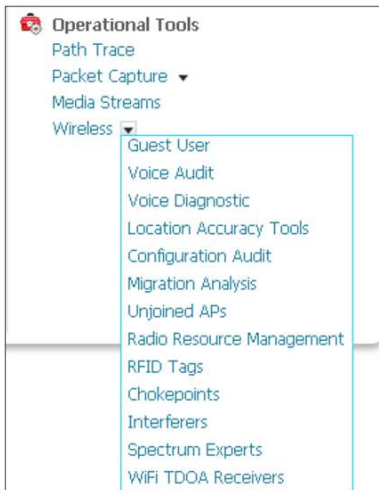
Remediate Issues

Remediate Wireless Issues

The following tools available within Cisco Prime Infrastructure may be used in order to remediate wireless issues:

- Cisco CleanAir®
- Client Troubleshooting
- AP Troubleshooting
- Audit Tool

- Security Dashboard
- Switchport Tracing (SPT)
- Apart from these key tools, you can find more tools by navigating to Operate > Wireless (under Operational Tools).
- Contextual device 360-degree views for easy access to assorted tools:
 - Ping
 - TraceRoute
 - Cisco Discovery Protocol Neighbors
 - WLAN and SSID information
 - Active AP and client count



Remediate Wired Issues

The following tools within Cisco Prime Infrastructure can be used to remediate wired issues:

- Wired Client Troubleshooting
- Ad Hoc and Automated Packet Capture
- Device Work Center
- Contextual device 360-degree views for easy access to assorted tools:
 - Ping
 - TraceRoute
 - Cisco Discovery Protocol Neighbors
 - Config Diffs
 - Inventory Details
 - Network Audits
 - Support Forums



Optimize

Use Cisco Prime Infrastructure to Optimize the Operation of Your Converged Network

There are several tools available within Cisco Prime Infrastructure to optimize your network.

Some of the tools that help optimize wireless infrastructure would be:

- Wireless Network Performance (RRM)
- Wired Performance (WAN bandwidth)
- Reports

Dashboard Customization


Cisco Prime Infrastructure uses the latest dashboard, which uses the latest technology of CSS3, HTML5, as well as AJAX with some charts. All of these allow for easy customization and visualization of data. There are two main ways of customizing the dashboards:

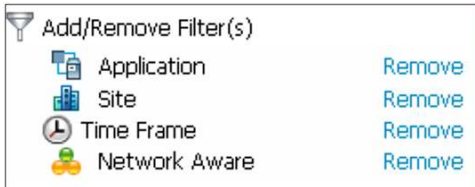
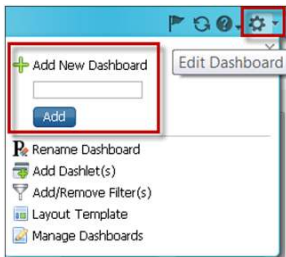
- Adding your own dashboard in addition to the ones provided
- Adding/moving dashlets (aka portlets) from one dashboard to another

First navigate to one of the four existing dashboards as shown in the figure below:

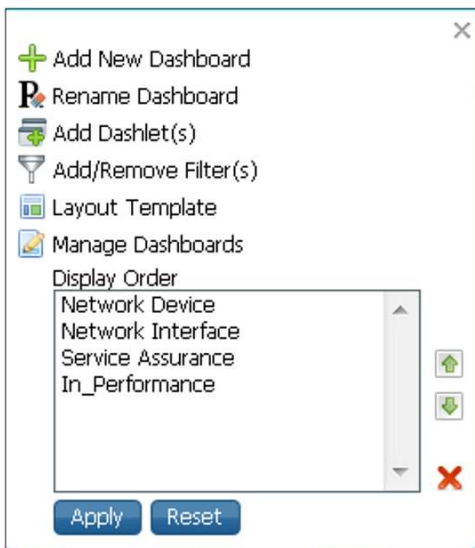


You can easily add a new dashboard by going to the top right of the screen and clicking the Edit Dashboard

() icon. You should see a new pop-up as shown in the following figure. Depending on where you were in the menu when you clicked the gear icon, a new dashboard will be created under that tree. Type in a suitable name for the dashboard, and click the Add button to create a new dashboard. A new tab is reflected immediately. If you created a tab by mistake, you can simply go to Manage Dashboards as shown in figure at the left and delete the newly created dashboard, and then re-create a new one under the appropriate dashboard.

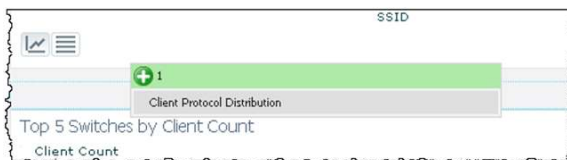


Note that Add/Remove Filter(s) applies only to the default dashboards and not for the custom dashboards. By default all of these filters will be populated for the default dashboards.



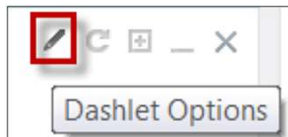
The next step is to populate the new dashboard that you created with content. This is done by adding dashlets to it. There are about 50 preconfigured templates that you can use for various dashboards.

A new dashlet can be added by going to the dashboard where you want it to show up and clicking Add Dashlet(s) from the Edit Dashboard menu. Once you see the list of dashlets, you can simply drag and drop the desired dashlet onto the dashboard. You should see a green bar as a confirmation that the dashlet will stay there, as shown in figure below.

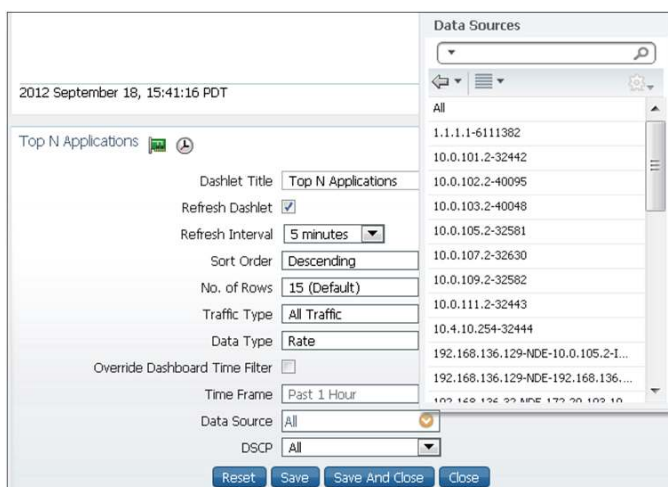


Customizing the Dashlet Content

We can not only customize the dashboard but also the content within the dashlets. At times, you may want to know the rates instead of the volume, or you may want information coming from NetFlow instead of NAM or vice versa. You can configure the dashlet to show just that. First, make sure the needed dashlet already exists in the dashboard. If not, you will need to create it as shown in the previous section. Now click Dashlet Options, as shown in the following figure.



This will expose all of the configurations that can be tweaked for a given dashlet as shown in the figure at the right. You may now use the pull-down menu to select and configure as needed. Some key interesting things to note are data type, traffic type, data sources, and differentiated services code point (DSCP). Each dashlet will have its configuration parameters. Once you are done, click Save and Close to return to the default data view.

A screenshot of the 'Dashlet Options' configuration window for 'Top N Applications'. The window is titled '2012 September 18, 15:41:16 PDT'. It contains several configuration fields: 'Dashlet Title' (Top N Applications), 'Refresh Dashlet' (checked), 'Refresh Interval' (5 minutes), 'Sort Order' (Descending), 'No. of Rows' (15 (Default)), 'Traffic Type' (All Traffic), 'Data Type' (Rate), 'Override Dashboard Time Filter' (unchecked), 'Time Frame' (Past 1 Hour), 'Data Source' (All), and 'DSCP' (All). At the bottom are buttons for 'Reset', 'Save', 'Save And Close', and 'Close'. On the right side, there is a 'Data Sources' list with a search bar and a list of IP addresses and network ranges.

Advance Configuration Topics

Identity Services Engine Integration

Cisco ISE is a next-generation identity and policy-based network access platform that helps enable enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. See the figure above. Cisco Prime Infrastructure manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, Cisco Prime Infrastructure collects additional information about these clients from the ISE and provides all relevant client information to Cisco Prime Infrastructure to be visible in a single console.

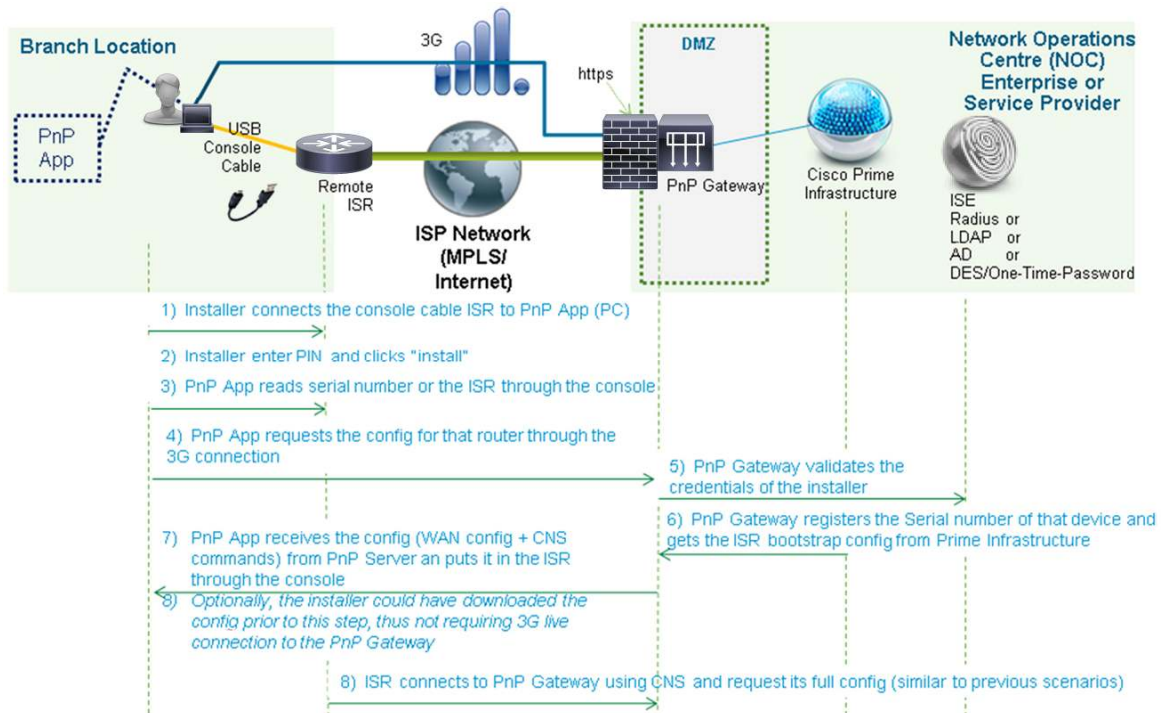
Cisco Prime Infrastructure can be integrated with ISE by navigating to **Design > External Management Servers** (under Management Tools) > **ISE Servers**. You can add a new ISE server by selecting Add Identity Services Engine as shown in the figure above. You will then be prompted for some basic ISE connectivity information (see the figure below). Once that is entered, the ISE server is then added to the list. Most of the remaining configuration will need to be done on the ISE itself.

TIP: ISE has a locking mechanism if the password is entered incorrectly three times in a row. It is extremely important to use the correct credentials when integrating within Cisco Prime Infrastructure; otherwise the ISE web interface will be locked out. Users will then need to log in through the ISE CLI to unlock the web interface.

See [“Understanding the Cisco ISE Network Deployment”](#) for detailed ISE configuration tasks that are needed to populate the data consumed by Cisco Prime Infrastructure (the steps are the same as with NCS 1.1/ISE 1.x integration).

Automated Deployment

Automated deployment is a new feature within Cisco Prime Infrastructure 1.3 that eases the pain of deploying new branch routers or switches. Normally when a device is provisioned in a new branch or remote site, it needs to be prepared for provisioning. Some network engineers prefer to stage the device completely and ship it to the end location, while others prefer to do a partial staging of the device so that it can come online once it's deployed in the end location. Management systems can then be used to push the full configuration. In both cases, a lot of manual configuration is needed, and it amounts to big delays in deploying a new branch or site. Automated deployment could be used for places where quick and zero-touch deployments are desired. If a nontechnical staff is deploying the device in a remote branch, this feature will definitely prove to be useful. The following image gives us a good overview of the deployment process:



The three main components within the automated deployment profile are:

- Bootstrap configuration
- Desired device configuration
- Desired Cisco IOS Software image

Bootstrap Configuration

This is the configuration that is needed within the device in order to get the full-blown working configuration. Some users may recall that the Cisco Networking Services Configuration Engine also worked the same way. A sample bootstrap configuration is shown below:

```
ip host abcd.ef.com 192.168.1.163
ip host abcd 192.168.1.163
cns trusted-server all-agents abcd.ef.com
cns trusted-server all-agents abcd
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
cns event abcd.ef.com 11013 keepalive 120 2 reconnect-time 60
cns exec 80
cns image server http://abcd.ef.com /cns/HttpMsgDispatcher status
http://abcd.ef.com /cns/HttpMsgDispatcher
cns config partial abcd.ef.com 80
cns config initial abcd.ef.com 80
```

More examples of the bootstrap configuration can be found at

http://www.cisco.com/en/US/partner/docs/net_mgmt/prime/infrastructure/1.2/user/guide/create_pnp.html.

There are four bootstrapping options available for automated deployment within Cisco Prime Infrastructure. There are no CLI skills needed for any of these options.

1. Using the Cisco Prime Automated Deployment application (available for PC/iPhone/iPad): Installer connects LAN/WAN cables and a USB console cable and a laptop/iPhone/iPad application to bootstrap the ISR router at the end location in a branch/site. This options works well if multiple devices are to be deployed.
2. Portable USB drives may also be used to bootstrap the device: Installer at the remote site connects LAN/WAN cables and a USB stick to the new device to be deployed at that site. This option is available for ISR routers with Cisco Virtual Office zero-touch deployment capabilities.
3. Using Cisco Integrated Customized Services, which loads a custom factory configuration on the ISR, is available for all ISR routers. Installer only connects LAN/WAN cables at the site.
4. Using Cisco Configuration Professional (CCP) Express is available for all ISR routers only.

Bootstrap configuration is needed for the device to talk to the automated deployment gateway to download the designed/desired configuration and image. In the next release of Cisco Prime Infrastructure (2.0), the gateway will be included within Cisco Prime Infrastructure itself, so there will be no need to install a separate gateway application (as with Cisco Prime Infrastructure 1.3).

Desired Device Configuration

The desired device configuration is the configuration that is intended to be running on the device after the device has been successfully deployed. This configuration should contain components such as SNMP, SSH/Telnet, ACLs, and syslog that will enable Cisco Prime Infrastructure to effectively manage this device when it comes online.


Desired Cisco IOS Software Image





This is the Cisco IOS Software image that is desired to be running on the device after successful deployment of the device.

Creating the Bootstrap and Device Configuration Template

Before creating an automated deployment template, we need to have the templates ready for bootstrap and the initial configuration of the device. In order to create a new bootstrap configuration template, navigate to **Design > Configuration Templates > CLI Template > CLI** and fill in all the details in the Template Basic section. In the next section, Validation Criteria, users can specify what device family type and what Cisco IOS Software version are applicable for this template. Type or paste the CLI in the CLI Content area. Let's look at how to convert a simple line with two values into a variable. We will look at the first line of the bootstrap configuration:

```
ip host abcd.ef.com 192.168.1.163
```

Once the preceding line is pasted into the CLI content area, select the value **abcd.ef.com**, which we want to convert to a variable. Once the value is selected, you can then click the Manage Variable icon () on the right. This will create a new variable as shown in the following figure:

Add Variable					
					
	Name	Type	Description	Display Label	Required
	abcd.ef.com				false

Select the row, and click **Edit**. You can now give a meaningful name to the value so that the user deploying the template will know what it means. The following image shows the same row after editing:

Name	Type	Description	Display Label	Required
fqdn_hostname	String	FQDN Host	Full Hostname	<input checked="" type="checkbox"/>

Save the changes, and click **Add** at the bottom to replace our original value abcd.ef.com with **\$fqdn_hostname**. You can now click **Form View** to get a feel for how the template will appear when you deploying it. See the following figure:

Template Detail
 CLI Content
 ip host \$fqdn_hostname 192.168.1.163

Template Detail
 Form View
 *Full Hostname

Similarly you can take each of the values that need to be converted and make them into variables. Once you are done, you can click **Save As New Template** and create a new bootstrap template out of it. The final template could look something like the following:

My Templates > BN Demo

PnP_Bootstrap

Template Basic
 *Name PnP_Bootstrap
 Description Template for Automated Deployr
 Author tshah
 Feature Category CLI

Validation Criteria
 *Device Type Routers
 OS Version

Template Detail
 CLI Content

```

ip host$fqdn_hostname $host_ip_address
ip host $hostname $host_ip_address
cns trusted-server all-agents $fqdn_hostname
cns trusted-server all-agents $hostname
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
cns event $fqdn_hostname 11013 keepalive 120 2 reconnect-time 60
cns exec 80
cns image server http://$fqdn_hostname /cns/HttpMsgDispatcher status http://$fqdn_hostname /cns/HttpMsgDispatcher
cns config partial $fqdn_hostname 80
cns config initial $fqdn_hostname 80

```

This will be used in the next section when creating a new automated deployment template. This procedure can be used for creating any new template.

Create Automated Deployment Templates

In order to create a new template for automated deployment, navigate to **Design > Automated Deployment Profiles > PnP Profile** (selected by default). You can now fill in the Profile Basic, Validation Criteria, and Profile Detail sections. The filled out template should look like the one shown below:

The screenshot shows the 'PnP Profiles' configuration page for a profile named 'PnP 3750 Switch Deploy'. The page is divided into three main sections: Profile Basic, Validation Criteria, and Profile Detail. The Profile Basic section includes fields for Name (PnP 3750 Switch Deploy), Description (Auto deployment of a new 3750), and Author (root). The Validation Criteria section includes a dropdown for Device Type (Cisco Catalyst 3750-E Seri...). The Profile Detail section includes dropdowns for Bootstrap Template (PnP_Bootstrap), Software Image (c3750-ipserviceslnk9-tar....), Image Location (Flash:), and Configuration Template (NTP). At the bottom, there are buttons for Save, Save as New PnP Profile, Cancel, UnPublish, and Deploy.

Now save the template. You can also click **Publish** and then **Deploy** if you plan on deploying the template right away.

Deploying the Automated Deployment Template

Once published, the template can also be deployed by navigating to **Deploy > Automated Deployment Profiles**. Select the recently created template and click **Deploy**, as shown in the following figure:

The screenshot shows the 'Automated Deployment Profiles' page. On the left, there is a tree view under 'Automated Deployment' showing 'PnP Profiles' and 'PnP 3750 Switch Deploy'. On the right, the details for 'PnP 3750 Switch Deploy' are shown, including the description 'Auto deployment of a ...' and the published date '2012-Aug-28 10:39:37 PDT'. At the bottom right, there are buttons for 'Detail', 'History', and 'Deploy' (highlighted with a red box).

Once you click Deploy, you can see all the devices that are now filtered out based on our Validation Criteria in the template. Click **Add** to add the device that is to be provisioned using automated deployment. The following figure shows a sample filled-out form for the modal pop-up that appears after you click Add.

PnP PreProvisioning Details [X]

*Name Description

Device Selection Parameters

Device Id ⓘ Type **Switches and Hubs/Cisco Catalyst 3750-E Series Switches**

Profile Parameters

▼ Configuration Template Properties

*Peer key number

*Authentication Key number

*MD5 Number

*Peer IP Address

▼ Image Properties

Image Location ⓘ

Erase Flash ☐

Continue On Image Failure ☐

Activate Image ☒

Device Management Parameters

▼ Device Management Parameters

IP Address

▼ SNMP Parameters

Version Timeout (sec) Retries

*Community

▼ CLI Parameters

Protocol

UserName Password Confirm Password

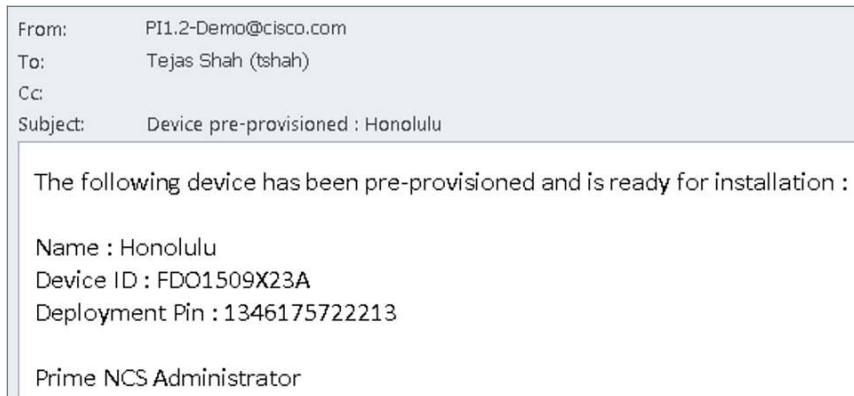
Enable Password Confirm Enable Password Timeout (sec)

[OK] [Cancel]

Click **OK** to save the new device to be provisioned in the network. You can now see the device ID, which is the serial number for the device as show in figure below.

Device Provisioning Profiles				
Add Edit Delete Export Bootstrap TFTP Email Bootstrap Show All				
<input type="checkbox"/> Name	Description	Device Type	Device Id	
<input checked="" type="checkbox"/> Honolulu		Switches and Hubs/Ci...	FDO1509X23A	

You can now either send the email using the bootstrap configuration or email the PIN directly. You will get an email as shown the figure below. This PIN can then be used to pull the bootstrap directly from the PnP gateway server.



Deploying Devices Using Automated Deployment Templates

The easiest way to deploy the bootstrap configuration is by using the Automated Deployment Application as shown in figure on right. You need to connect the laptop to the router using the console cable, and just input the PIN number in the Cisco Deployment Application as shown in the following image.



The application will then configure the router with the basic bootstrap configuration. Once the device reboots, it will connect to the automated deployment gateway and download the actual device configuration and the image that it needs to run.

References

Prime Infrastructure 1.3 Links

- Cisco Prime Infrastructure 1.3 - Quick Start Guide
http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.3/quickstart/guide/cpi_qsg_1_3.html
- Cisco Prime Infrastructure 1.3 Release Notes:
http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.3/release/notes/cpi_rn_13.html
- Supported Devices in 1.3
http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.3/supported/devices/cpi13_supported_devices.xlsx

-
- Cisco Prime Infrastructure 1.3.1 update (1.3.0.20 Update 1 Patch)
<http://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=284652876&softwareid=284272933> > PI_1_3_0_20-Update.1.12.tar.gz

Cisco Product Pages

- Cisco Prime Infrastructure <http://www.cisco.com/go/primeinfrastructure>
- Cisco Identity Security Engine (ISE) <http://www.cisco.com/go/ise>
- Cisco Prime Network Analysis Module (NAM) <http://www.cisco.com/go/nam>
- Cisco Application Visibility and Control <http://www.cisco.com/go/avc>
- Product Downloads http://www.cisco.com/cisco/web/support/index.html#~shp_download

Ordering and Licensing

- Cisco Ordering Tools <http://www.cisco.com/go/ordering>.
- Ordering and Licensing Guide [Cisco Prime Infrastructure 1.x Ordering and Licensing Guide](#)
- Product Evaluation <http://www.cisco.com/go/nmsevals>

Related Deployment Guides

- Wireless Deployment Guide (NCS)
http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bba943.shtml
- ISE Deployment Guide http://www.cisco.com/en/US/docs/security/ise/1.0/install_guide/ise10_deploy.pdf
- MSE Deployment Guide
http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml
- AVC Deployment Guide (Wireless)
http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bed910.shtml



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)